

Sensibler Umgang mit persönlichen Daten

Datenschutz geht zur Schule

Arbeitsblätter

klicksafe wird kofinanziert von der Europäischen Union

Datenschutz geht zur Schule
BvD e.V.
DATENSCHUTZ GESTALTEN

DATEV STIFTUNG Zukunft

klicksafe.de
Mehr Sicherheit im Internet durch Medienkompetenz

Titel:
Datenschutz geht zur Schule
Sensibler Umgang mit persönlichen Daten.
Arbeitsblätter

Herausgeber:
Katrin Eggert, BvD e. V.
Ralf Heimburger, Mitglied im AK Schule, BvD e. V.
Rudi Kramer, Sprecher der Initiative „Datenschutz geht zur Schule", BvD e. V.
Frank Spaeing, stellv. Sprecher der Initiative
„Datenschutz geht zur Schule", BvD e. V.
Riko Pieper, stellv. Sprecher der Initiative „Datenschutz geht zur Schule", BvD e. V.

Initiative „Datenschutz geht zur Schule" des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.
in Zusammenarbeit mit klicksafe und Unterstützung der DATEV-Stiftung Zukunft

3. überarbeitete Auflage November 2018

Projektunterstützung:
DATEV-Stiftung Zukunft

Kooperationspartner:
Die in diesem Handbuch zusammengestellten Arbeitsmaterialien entstammen zum größten Teil aus Publikationen der EU-Initiative klicksafe, die der Initiative „Datenschutz geht zur Schule" zur Verfügung gestellt wurden. klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.

Koordinator klicksafe: Peter Behrens, LMK

klicksafe wird von der Europäischen Union kofinanziert
http://ec.europa.eu/saferinternet

Die alleinige Verantwortung für diese Veröffentlichung liegt beim Herausgeber.

Die Europäische Union haftet nicht für die Verwendung der darin enthaltenen Informationen.

Die in diesem Arbeitsmaterial verwendeten klicksafe-Handbücher und deren Autoren werden im Folgenden aufgeführt:

Always on, Mobile Medien – Neue Herausforderungen
Stefanie Rack (klicksafe), Fabian Sauer (Handysektor, mecodia)

Das klicksafe-Lehrerhandbuch KnowHow für junge User
Marco Fileccia, Birgit Kimmel, Stefanie Rack, Isabell Tatsch, Friederike Groschup

Ethik macht klick – Werte-Navi fürs digitale Leben
Prof. Dr. Petra Grimm, Karla Neef, Michael Waltinger – Institut für Digitale Ethik (IDE)/Hochschule der Medien (HdM),
Birgit Kimmel und Stefanie Rack – klicksafe

Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web
Stefanie Rack und Marco Fileccia sowie der Arbeitskreis „Datenschutz und Bildung" der Datenschutzbeauftragten des Bundes und der Länder

Let's talk about Porno! Jugendsexualität, Internet und Pornographie
Birgit Kimmel und Stefanie Rack – klicksafe
Constantin Schnell und Franziska Hahn – Landesmedienzentrum Baden-Württemberg (LMZ)
Johann Hartl – pro familia Landesverband Bayern e. V.

Nicht alles, was geht, ist auch erlaubt! Downloaden, tauschen, online stellen – Urheberrecht im Alltag
Dr. Till Kreutzer, Stefanie Rack, Marco Fileccia, Birgit Kimmel

Safer Smartphone – Sicherheit und Schutz für das Handy
Stefanie Rack (klicksafe), Fabian Sauer (Handysektor, mecodia)

Wie finde ich, was ich suche? Suchmaschinen kompetent nutzen
Stefanie Rack, Birgit Kimmel, Franziska Hahn, Marco Fileccia – klicksafe
Carola Rienth und Dr. Arnd Haller – Google Germany GmbH
Gregor Schwarz und Otto Vollmers – Freiwillige Selbstkontrolle Multimedia (FSM)
Dr. Friederike Siller, Anke Meinders, Cornelia Margraf – fragFINN e. V.

Selfies, Sexting, Selbstdarstellung
Stefanie Rack (klicksafe)
Fabian Sauer (Handysektor, mecodia)

Datensatz – Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind
Steffen Haschler (Bildungsprojekt „Chaos macht Schule",
Chaos Computer Club Mannheim) unter Mitarbeit von
Benjamin Schlüter (Bildungsprojekt „Chaos macht Schule",
Chaos Computer Club Berlin) und
Stefanie Rack (klicksafe)
Verantwortlich: Birgit Kimmel (Pädagogische Leitung klicksafe)

Arbeitsblätter „Daten unter Artenschutz ", „Bedrohliche Drohnen?"
Stefanie Rack (klicksafe)

Der Datenschutz Medienpreis (DAME) des BvD stellt jährlich eine Übersicht aller eingereichten Wettbewerbsbeiträge zusammen und stellt somit eine umfangreiche Plattform für Filme und Videoclips rund um das Thema Datenschutz zur Verfügung.
https://www.bvdnet.de/dame/

Es wird darauf verwiesen, dass alle Angaben in diesem Buch trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Herausgeber und der Autoren ausgeschlossen ist.



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung-Nicht kommerziell 4.0 International Lizenz, d. h. die nichtkommerzielle Nutzung und Verbreitung ist unter Angabe der Quelle klicksafe und der Webseite www.klicksafe.de erlaubt. Sollen über die genannte Lizenz hinausgehende Erlaubnisse gewährt werden, können Einzelabsprachen mit klicksafe getroffen werden. Wenden Sie sich dazu bitte an info@klicksafe.de.

Weitere Informationen unter:
https://creativecommons.org/licenses/by-nc/4.0/

Hinweis:
Männliche/weibliche Form: Die auf den meisten Seiten verwendete männliche Form impliziert selbstverständlich die weibliche Form. Auf die Verwendung beider Geschlechtsformen wird lediglich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

Layout und Umschlaggestaltung:
Designgruppe Fanz & Neumayer, Ludwigshafen und Heidelberg

Datenschutz geht zur Schule

Sensibler Umgang mit persönlichen Daten
Arbeitsblätter

Unterlagen erstellt durch Initiative „Datenschutz geht zur Schule“
des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.
in Zusammenarbeit mit klicksafe.

Herausgeber:
Katrin Eggert, BvD e. V.
Ralf Heimburger, Mitglied im AK Schule, BvD e. V.
Rudi Kramer, Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.
Riko Pieper, stellv. Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.
Frank Spaeing, stellv. Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.

Datenschutz geht zur Schule
BvD e.V.
DATENSCHUTZ GESTALTEN

DATEV STIFTUNG Zukunft

klicksafe.de

Grußwort Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Die Wahrnehmung der Anforderungen des Datenschutzes hat durch Fehlinformationen, Missverständnisse und unzureichende Klarheit bei der Einführung der Datenschutz-Grundverordnung gelitten. Umso wichtiger ist es, wenn schon frühzeitig in der Schule die Grundlagen eines verantwortungsvollen Umgangs mit personenbezogenen Daten behandelt werden. Die Einsatzszenarien moderner IT-Technologie wandeln sich immer schneller und der Erfolg ihres Einsatzes hängt immer mehr von der Kenntnis der Nutzer über technische und rechtliche Zusammenhänge ab, welche die Grundlage eines vertrauensvollen Umgangs bilden.

Die betrieblichen Datenschutzbeauftragten bekommen immer wieder im Rahmen ihrer Sensibilisierungsmaßnahmen zum rechtskonformen Umgang mit Daten und Informationen gespiegelt, dass zwar ein Bewusstsein vorhanden ist, aber konkrete Handlungsanweisungen fehlen. Initiativen von anderer Seite an Schulen zielten in den letzten Jahren auf die Abwehr sicherheitstechnischer Risiken oder die Gewinnung von Nachwuchskräften in der IT ab. Umso erfreulicher ist es, dass zunehmend auch die Vermittlung von Datenschutzkenntnissen Einzug in die Lehrpläne hält. Dies kommt dem Ansatz der Initiative „Datenschutz geht zur Schule" des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. sehr entgegen, sollen dadurch doch den Schülerinnen und Schülern klare und einfache Verhaltensregeln für den sensiblen Umgang mit persönlichen Daten von ihnen oder anderer im Netz näher gebracht werden.

Der Erfolg der ersten Auflage dieses Lehrer-Handouts in 2016 und die stete Nachfrage nach diesem „best of" einiger Lehrmaterialien des Kooperationspartners klicksafe bestärkten uns, das Lehrer-Handout zu überarbeiten. Dabei konnten wir für die Umsetzung wieder von der großzügigen Förderung der DATEV Stiftung Zukunft profitieren, die die Initiative seit 2015 unterstützt.

Dieses Handout kann eine vertiefe Befassung mit den Themen durch Lehrerinnen und Lehrer nicht ersetzen, soll diese aber in die Lage bringen, im Unterricht passende Materialien für die Vermittlung der Grundlagen einsetzen zu können. Es ergänzt die im Rahmen von „Datenschutz geht zur Schule" behandelten Fragenstellungen und kann aber auch ohne die Vorträge genutzt werden.

Ganz herzlich bedanken wir uns an dieser Stelle bei all den ehrenamtlichen Dozentinnen und Dozenten der Initiative „Datenschutz geht zur Schule", die sich zu diesem Thema engagieren. Die großen gesellschaftlichen Veränderungen, die durch die Digitalisierung gefördert werden, können nur dann erfolgreich bewältigt werden, wenn allen Beteiligten die erforderlichen Kenntnisse der Grundlagen und der Vermeidung von Risiken vermittelt werden und bekannt sind.

Wir freuen uns, dabei mitwirken zu dürfen!



Rudi Kramer
Sprecher der Initiative „Datenschutz geht zur Schule"
des BvD e. V.

Grußwort DATEV-Stiftung Zukunft

Erinnern Sie sich an den 25.05.2018? Vermutlich nicht unbedingt. Abhängig davon, in welchem Bundesland Sie Ihren Berufsstand vertreten, war jener Freitag im Mai diesen Jahres vermutlich ein ganz normaler Unterrichtstag oder Sie haben den letzten Tag der Pfingstferien mit der Vorbereitung auf den Schlussspurt des Schuljahres 2017/2018 verbracht. Für öffentliche Einrichtungen, aber auch für Unternehmer und Unternehmen jeder Größe, die unseren EU-Wirtschaftsraum gestalten, war der 25.05.2018 allerdings eine Art „Reset". Die EU-Datenschutz-Grundverordnung (DSGVO) war ab eben jenen 25.05.2018 rechtmäßig anzuwenden. Allgemein formuliert, regelt die DSGVO die rechtmäßige Verarbeitung personenbezogener Daten im gesamten EU-Raum. Über deren Umfang, Inhalt und die Auswirkungen dieser Verordnung bestand vor und besteht nach dem 25.05.2018 breite Unsicherheit in öffentlichen Einrichtungen, im privaten Umfeld, und auch in der Wirtschaft. Auch heute – mehrere Monate nach der Durchsetzung der DSGVO – dominieren Unsicherheit, Halbwissen und Nervosität im Umgang mit der 11 Kapitel schweren Verordnung.

Sehr wahrscheinlich waren auch Sie als Privatperson direkt betroffen. Vielleicht erinnern Sie sich an die zahlreichen E-Mails, die Sie bis kurz vor dem Stichtag erhalten haben. Amazon, Zalando und tausende andere Onlinehändler haben von ihren Bestandskunden eine Bestätigung zur künftigen Datenverarbeitung eingeholt und über Neuigkeiten in den AGBs informiert. Wie erging es Ihnen persönlich bei jenen E-Mails? Waren Sie vielleicht auch etwas verwundert, welche Firmen offenbar Ihre E-Mailadresse immer noch besitzen und deshalb mit Ihnen in Kontakt getreten sind?

Die Einführung der DSGVO hat aber für noch viel größere Unsicherheiten auch im nichtwirtschaftlichen Bereich gesorgt. Privatpersonen, die über Jahre in ihrer Freizeit Online-Foren betrieben haben, entschlossen sich, den Betrieb einzustellen. Zu groß war die Unsicherheit, Daten von Communitymitgliedern (wie bspw. die IP-Adresse) künftig streng nach der DSGVO verarbeiten zu müssen. Aus der gleichen Nervosität heraus wurden auch übergreifende WhatsApp Chat-Gruppen von privaten Betreibern geschlossen. Und auch das jüngste Beispiel aus der überregionalen Presse zeigt, dass bei der DSGVO weiter Unklarheit herrscht. Ein Mieter aus Wien möchte seinen Namen nicht auf dem Klingelschild des Mietshauses sehen und verweist auf die DSGVO. Die Stadtverwaltung gibt ihm Recht, der Vermieter erwägt nun, an ca. 2000 Immobilien alle Namensschilder abzumontieren.

An jenen Beispielen wird deutlich, wie Unklarheit, Unsicherheit und vor allem unzureichende Kenntnisse über rechtliche Anforderungen den Alltag beeinflussen. Als DATEV-Stiftung Zukunft ist es uns ein besonderes Anliegen, Wissensvermittlung zu den Themen Datenschutz und IT-Sicherheit auf allen Niveaustufen des Deutschen Qualkifikationsrahmens fest zu verankern. Die Arbeit der Initiative „Datenschutz geht zur Schule" des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. war eines der ersten Projekte, das von der DATEV-Stiftung Zukunft gefördert wurde und wir freuen uns, auch an der Ihnen vorliegenden 3. überarbeiteten Auflage mitgewirkt zu haben. Die Anpassungen an die neue DSGVO sowie die inhaltliche Aktualisierung einiger Kapitel geben uns die Zuversicht, dass sich auch diese Ausgabe als ein nützliches Arbeitsmittel für die praxisnahe Wissensvermittlung der Themen „Datenschutz" und „IT-Sicherheit" bewährt.



Eckhardt Schwarzer
Vorstandsvorsitzender
der DATEV-Stiftung Zukunft



Dr. Markus Algner
Vorstand der
DATEV-Stiftung Zukunft



Julia Bangerth
Vorstand
der DATEV-Stiftung Zukunft

Vorwort

Die Unterteilung in Online und Offline ist inzwischen fast schon obsolet: Das Internet ist fest in unseren Alltag eingebunden und gerade für Kinder und Jugendliche ist dessen Nutzung ein selbstverständliches Grundbedürfnis in fast allen Lebenslagen. „Always On" so lautet auch der Titel eines unserer klicksafe-Materialien. Wir sind fast immer und für fast alles im Netz unterwegs, die Vielfalt unserer Online-Nutzung sowie die sich dauernd wandelnde Medienlandschaft bringen dabei zahlreiche neue Herausforderungen für ein gelingendes Leben in der digitalen Welt mit sich.

Worauf sollte man bei der Nutzung von Kommunikationsdiensten achten? Über welche urheberrechtlichen Grundlagen sollten Internetnutzer verfügen? Wie verhalte ich mich, wenn ich im Internet belästigt werde? Welche Normen und Werte wünschen wir uns im Netz? Wie schützt man seine Privatsphäre? Wer sammelt alles Daten und was passiert mit den Spuren, die wir im Netz hinterlassen? Fragen wie diese spiegeln die Bandbreite der Themen, mit denen wir uns von klicksafe seit Jahren auseinandersetzen.

Dem Thema Datenschutz kommt dabei eine große Rolle zu: Nicht nur Nachrichtendienste, auch Medienanbieter sammeln eine Vielzahl an Nutzerinformationen und werten diese auch aus. Unter dem Stichwort BIG DATA ist dieses Phänomen derzeit in aller Munde. Doch wo, wie und vor allem welche Daten erfasst werden, ist für den Durchschnitts-Nutzer zunächst häufig eher abstrakt und intransparent. Die neue Datenschutzgrundverordnung (DSGVO) hat Vieles neu geregelt, aber auch Fragen aufgeworfen. Unter www.klicksafe.de/dsgvo können Sie sich über die komplexen Änderungen informieren. Mit Arbeitsmaterialien rund um das Thema Datenschutz setzten wir darauf, das Thema für Jugendliche interessant und zugänglich zu machen und die Idee vom „informierten Nutzer" voranzutreiben.

Ein zentraler Aspekt des Auftrages von klicksafe ist die Information und Schulung von Multiplikatorinnen und Multiplikatoren, die sich ebenso wie wir für das Thema Internetsicherheit engagieren. Es freut und ehrt uns deswegen sehr, dass unsere Arbeitsmaterialien einen solchen Anklang finden, dass sie die Grundlage des Lehrerhandouts der Initiative „Datenschutz geht zur Schule" bilden. In engem Austausch mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. wurde in den letzten Monaten eine Selektion bestehender klicksafe-Materialien getroffen, die vom klicksafe-Lehrerhandbuch „Knowhow für junge User" über die Module „Ich bin öffentlich ganz privat" und „Nicht alles, was geht, ist auch erlaubt" bis hin zu „Ethik macht klick" reicht. Mit dieser Auswahl an Themen hoffen wir, die verschiedensten Aspekte rund um das Thema Datenschutz im Internet multiperspektivisch abzudecken.

Durch die Aufbereitung von leicht verständlichen Hintergrundinformationen und konkreten Praxisprojekten möchten wir Ihnen leicht handhabbare Arbeitsmaterialien zur Verfügung stellen, die Sie mit wenig Aufwand in Ihrem Arbeitsalltag einsetzen können.

Wir bedanken uns bei den ehrenamtlichen Dozentinnen und Dozenten der Initiative „Datenschutz geht zur Schule", die Kinder und Jugendliche im bewussten Umgang mit persönlichen Daten sensibilisieren.

Für die verantwortungsvolle Aufgabe, Schülerinnen und Schüler für den Datenschutz sowie einen kritischen Umgang mit digitalen Medien zu sensibilisieren, wünschen wir Ihnen viel Erfolg.

Ihr klicksafe-Team

Die Kapitel des Handbuchs
Das Handbuch ist in acht „Kapitel" unterteilt. Jedes Kapitel enthält verschiedene Bausteine zu einzelnen Themen. Jedes Kapitel kann unabhängig von den anderen im Unterricht eingesetzt werden.

Sachinformationen
Ausführliche Sachinformationen zu den Themen finden Sie jeweils in Linksammlungen, die Sie bei Interesse zur Vertiefung hinzuziehen können.

Linkliste
Aufgeführt sind ausschließlich Links zum jeweiligen Kapitel sowie den von uns zur Thematik geprüften und als qualitativ besonders hochwertig erachteten Seiten und Portalen. Dies gilt auch für die Links auf den Arbeitsblättern der Schülerinnen und Schüler. Wir erheben also keinen Anspruch auf Vollständigkeit; Qualität ging uns hier vor Quantität.

Methodisch-didaktische Tabelle
Der methodisch-didaktische Informationsteil gibt Ihnen einen tabellarischen Überblick über Planungsaspekte der Unterrichtsstunde/Unterrichtseinheit und soll Ihnen eine schnelle und effiziente Planung ermöglichen. Hier finden Sie:

- Kompetenzen
- Methoden: Damit schnell überblickt werden kann, welche Materialien benötigt werden. Viele Methoden orientieren sich am Konzept des „Kooperativen Lernens".
- Material: Damit Sie wissen, welche Vorbereitungen Sie treffen müssen (z. B. Filmmaterial downloaden).
- Zeitaufwand (in Minuten)
- Benötigte Zugänge: Wir haben großen Wert darauf gelegt, mehrere Unterrichtseinheiten auch ohne die Möglichkeit einer PC Benutzung oder/und eines Internetzugangs zu konzipieren, um diese auch im „PC-freien" Unterricht einsetzen zu können.
- Hinweise für die Durchführung

Arbeitsblätter
Die Arbeitsblätter sind nach drei Schwierigkeitsgraden konzipiert.

 4.–6. Klasse = einfach

 7.–8. Klasse = mittel

 ab 9. Klasse = schwer

Entscheiden Sie aufgrund des Leistungsstandes Ihrer Klasse, welche Arbeitsblätter Sie in welcher Klassenstufe einsetzen.

In diesem Buch werden viele relevante Themen des Jugendmedienschutzes ausführlich behandelt. Jeder Baustein, z. T. auch jedes Kapitel ist so aufgebaut, dass Sie auch nur ein Thema herausnehmen und sich die Inhalte aneignen können, um sie anschließend in Ihrem Unterricht umzusetzen.

Symbole

Überschaubare Informationseinheiten werden mit einem Infokasten, der mit einem Dreieck eingeleitet wird, hervorgehoben:

Tipp: *Facebook bietet z. B. die Funktion* ***Meine Seite für Andere:*** *Das eigene Profil kann aus der Perspektive eines beliebigen anderen Nutzers betrachtet werden. So weiß man, welche Infos den anderen Nutzern zugänglich sind und kann gegebenenfalls Einstellungen anpassen.*

Ein persönlicher Tipp der AutorInnen, Tipps zur inhaltlichen Weiterbeschäftigung mit dem Thema oder Durchführungshinweise werden mit einem Handsymbol eingeleitet:

Aus der Praxis
Selbstverständlich steht in der Schule die kritische Auseinandersetzung mit Computerspielen im Vordergrund. Nicht minder wichtig ist es aber für den Lehrer, sich auf die Welt der Computerspiele einzulassen. Möglich ist das bspw. in sog. LAN-Partys – Computerspiele-Events – für Lehrer und Eltern.

Rechtliche Regelungen und Hintergründe finden sich in einem solchen Kasten:

Der § 202a StGB bezüglich des Ausspähens von Daten besagt:
„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. “

Beschreibungen zur Durchführung einer Methode, wie bspw. die Methode Partnerinterview befinden sich in Kästen mit dem Schraubenschlüssel:

Methode „Partnerinterview”
Zu zweit mit Partner A und Partner B. Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt mit den Worten „Habe ich dich richtig verstanden, dass …?”. Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler einbauen, die der andere finden muss!

Links auf Webseiten für weitere Informationen, zur Vertiefung und Recherche befinden sich in Kästen mit dem Maussymbol:

In der JIM-Studie findest Du viele interessante Ergebnisse zur Mediennutzung Jugendlicher: **www.mpfs.de**

Für Informationen, Tipps oder alternative Vorschläge:

„Jeder, der denkt, das Internet sei anonym, der glaubt auch, er werde im Kaufhaus nicht gefilmt” – so oder so ähnlich könnte man böswillig sagen, wenn Täter von Cyber-Mobbing sich sicher fühlen. Bei jedem Zugriff auf das Internet werden die Verbindungsdaten beim Provider gespeichert. Es ist also leicht herauszufinden, wer wann und wo im Internet unterwegs war. Und bei einer möglichen Straftat darf ein Richter diese Verbindungsdaten kontrollieren.

Für Zusatzaufgaben/Hausaufgaben:

Zusatzaufgabe/Hausaufgabe:
Für die Schüler ist „PowerPoint-Karaoke“ eine sehr gute Möglichkeit, spontanes und kreatives Präsentieren zu üben. Sie lernen außerdem auf spielerische Weise die Suche nach bestimmten Dateiformaten.

Eine Einführung

Wie die erste Auflage richtet sich das Lehrerhandout primär an alle Lehrerinnen und Lehrer, die begleitend an Vorträgen der Initiative „Datenschutz geht zur Schule" teilgenommen haben und die in den Vorträgen behandelten Themen in ihrem Unterricht vertiefen wollen.

Auch hier durften wir wieder in Zusammenarbeit mit klicksafe Themen und Arbeitsblätter der verschiedenen Publikationen, die auf klicksafe angeboten werden, ausgewählt, um möglichst zu allen Inhalten, die in einem Vortrag angesprochen werden können, Arbeitsblätter zu bieten und ggf. auch weiterführende oder vertiefende Informationen. Soweit möglich wurden die Inhalte auf Anpassungsbedarf durch die Datenschutz-Grundverordnung (DSGVO) geprüft und dieser umgesetzt. Die Schnelllebigkeit europäischer bzw. bundesdeutscher Gesetzgebung sowie die Kulturhoheit der Länder sorgen dafür, dass einige Aussagen nicht jedes Detail der rechtlichen Betrachtung in aller Tiefe berücksichtigen können.

Unsere Erfahrungen mit und die Nachfrage nach der ersten Auflage zeigten: Auch ohne den Vortrag von „Datenschutz geht zur Schule" gehört zu haben, besteht ein erfreulich hohes Interesse von Pädagogen, die sich mit den Themen Datenschutz und Medienkompetenz auseinandersetzen wollen und dafür passend thematische Arbeitsblätter suchen und auf das Lehrer-Handout zurückgegriffen haben. Für die dritte Auflage haben wir in Abstimmung mit klicksafe bewusst auf das Thema Cybermobbing verzichtet, da es sich nur am Rande mit der rechtmäßigen Datennutzung befasst. Hinweise und Arbeitsblätter dazu sind weiterhin in der als pdf weiterhin verfügbaren 2. Auflage sowie bei den Materialien von klicksafe enthalten. Für den genutzten Platz wurde dafür die Thematik der Selbstdarstellung im Netz erweitert und ein Bereich zu Drohnen eingeführt.

Die Arbeitsblätter werden in der Regel in unterschiedlichen Schwierigkeitsgraden angeboten, um der Tatsache Rechnung zu tragen, dass die Thematiken in unterschiedlichen Jahrgangsstufen behandelt werden können, von der 5. Klasse bis zur Berufsschulen gibt.

Sie finden diese (immer in aktueller Version) unter dem folgenden Link:

https://www.bvdnet.de/datenschutz-geht-zur-schule/lehrerhandout/

Bei den Arbeitsblättern haben wir immer versucht, unterschiedliche Schwierigkeitsgrade anzubieten, um der Tatsache Rechnung zu tragen, dass es einmal Vorträge für jüngere Schülerinnen und Schülern und einmal welche für Schüler der höheren Klassen bzw. von Berufsschulen gibt. Sie sollten also jeweils passend zu Ihrer Klasse Materialien finden können.

Kapitel 1 | Datenschutz, Big Data und Profiling

1_1 Datenschutz / Big Data . . . 13
1_2 Datenschutz – Arbeitsblätter . . . 31
1_3 Datensatz, Datenschatz – Arbeitsblätter . . . 47
1_4 Daten unter Artenschutz – Arbeitsblatt . . . 70

Kapitel 2 | Mobiles Internet und das Internet der Dinge

2_1 Handy / Smartphone / Tablet – Arbeitsblätter . . . 75
2_2 WhatsApp & Co – Arbeitsblätter . . . 103
2_3 Internet der Dinge – Arbeitsblätter . . . 105

Kapitel 3 | Soziale Netzwerke in Schule und Arbeit

3_1 Soziale Netzwerke – Arbeitsblätter . . . 121
3_2 Arbeit und Schule – Arbeitsblätter . . . 134

Kapitel 4 | Das Recht am eigenen Bild

4_1 Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter . . . 151

Kapitel 5 | Passwortschutz und PC Sicherheit

5_1 Internet – Arbeitsblätter . . . 191
5_2 PC-Sicherheit – Arbeitsblätter . . . 230
5_3 Passwörter – Arbeitsblätter . . . 239

Kapitel 6 | Cybertreffen, Sexting und Selfie

6_1 Cybertreffen – Arbeitsblätter . . . 247
6_2 Sexting – Arbeitsblätter . . . 251
6_3 Selbstdarstellung im Netz – Arbeitsblätter . . . 264

Kapitel 7 | Freizeit – Gaming und Drohnen

7_1 Gaming – Arbeitsblätter . . . 299
7_2 Bedrohliche Drohnen? – Arbeitsblatt . . . 304

Kapitel 8 | Lehrer und Datenschutz

8_1 Lehrer und Datenschutz – Arbeitsblätter . . . 309
8_2 Materialsammlung Klicksafe . . . 321

1|1 Datenschutz / Big Data
1|2 Datenschutz
1|3 Datensatz, Datenschatz
1|4 Daten unter Artenschutz

1

Datenschutz, Big Data und Profiling



Übersicht der Bausteine:

- **Datenschutz / Big Data**
- **Datenschutz** | **Arbeitsblätter**
- **Datensatz, Datenschatz** | **Arbeitsblätter**
- **Daten unter Artenschutz** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Ethik macht klick – Werte-Navi fürs digitale Leben
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf



klicksafe to go
Datensatz – Datenschatz
Warum Datenschutz und Sicherheit wichtig sind
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf

1 Datenschutz, Big Data und Profiling



1_1 Datenschutz/Big Data
1_2 Datenschutz – Arbeitsblätter
1_3 Datensatz, Datenschatz – Arbeitsblätter
1_4 Daten unter Artenschutz

Einleitung



„Die Verteidigung des Privaten ist der erste Schritt zur Rettung der Freiheit."
Wolfgang Sofsky, *2009, S. 18*

Die Existenz einer Privatsphäre* wurde lange Zeit von der Gesellschaft als selbstverständlich vorausgesetzt. Dabei ist sie historisch gesehen ein junges Privileg. Erst gegen Ende des 18. und im Laufe des 19. Jahrhunderts erhielt der Schutz der Privatsphäre infolge der bürgerlichen Emanzipation und der Ausbildung moderner Nationalstaaten einen hohen Wert.

Heute scheint es allerdings nicht mehr gut um die Privatsphäre und ihren Wert zu stehen. Der Grund: Die Digitalisierung der Gesellschaft hat tiefgreifende und unumkehrbare Veränderungen mit sich gebracht. Die umfassende Nutzung von digitalen Technologien und deren fortschreitende Durchdringung unserer Lebenswelt hat auch Auswirkungen auf unsere Privatsphäre. Spätestens seit den Enthüllungen Edward Snowdens im Juni 2013 ist bekannt, dass unsere persönlichen digitalen Daten gespeichert, gehandelt und ausgewertet werden – nicht nur von Geheimdiensten, sondern auch von einer Vielzahl von Unternehmen.

In Technologiekreisen wird sogar schon das Ende der Privatsphäre postuliert: Die sogenannte Post-Privacy-Bewegung ist davon überzeugt, dass die Privatsphäre ein Auslaufmodell ist, und setzt auf vollständige Transparenz. Datenschutz sei aufgrund der globalen Struktur des Internets, in der nationale Gesetzgebung nicht greife, und der „Kommunikationsbedürfnisse, Neugierden und Bequemlichkeiten (...) der Nutzer(innen)"[1] nicht umsetzbar.

Und fragt man Jugendliche und junge Erwachsene nach dem Begriff „Privatsphäre", wissen sie oft nicht recht, was sie sich darunter vorstellen sollen: „Bei Nennung des Stichworts ‚Privatsphäre' im Internet assoziieren Jugendliche und junge Erwachsene vor allem Privatsphäre-Einstellungen in Online-Communitys – insbesondere Einstellungen bei Facebook. Sie denken dabei somit vor allem an technische Optionen, die aktiviert oder deaktiviert werden können. Folglich besteht sogar die Möglichkeit, ‚seine Privatsphäre auszuschalten'."[2]

Es ist daher notwendig, den Wert der Privatsphäre noch einmal zu hinterfragen: Was ist das eigentlich, und wozu ist sie gut? Bei der Privatsphäre handelt es sich nicht um einen abstrakten Begriff, sondern um einen wichtigen Bestandteil unseres Lebens. Den wenigsten von uns ist allerdings bewusst, was es bedeuten würde, auf Privatheit zu verzichten. Insofern ist Privatheit vergleichbar mit der Gesundheit: Erst wenn sie fehlt, weiß man sie wirklich zu schätzen. Um seine Daten – und damit die eigene Privatsphäre – zu schützen, muss man sich also zuerst bewusst machen, welchen Wert die Privatsphäre für unser Menschsein und unsere Identität hat.

* Im Folgenden werden die Begriffe „Privatsphäre", „Privatheit" und „Privacy" synonym verwendet.

1 Vertrauen ist gut, Privatsphäre ist besser

Sensibilisierung für die Bedeutung von Privatheit

Es existiert keine allgemeingültige Definition des „Privaten". Bei der Privatsphäre handelt es sich vielmehr um eine Idee, die historisch, kulturell und situationsspezifisch Veränderungen unterworfen ist.

1.1 Was ist eigentlich privat?

Reflexionsfragen: *Was verstehe ich unter „privat/öffentlich"? Was ist für mich „privat" und was ist „öffentlich"?*

Begriffsbestimmung
„Privat" leitet sich vom lateinischen Begriff „privatus" ab, der in der Übersetzung „(der Herrschaft) beraubt, gesondert, für sich stehend" bedeutet und damit die Trennung von der öffentlichen Sphäre meint – vor allem vom Staat. Im alltäglichen Sprachgebrauch spiegelt sich das wider, indem „privat" meist in Opposition zu „öffentlich" verwendet wird.

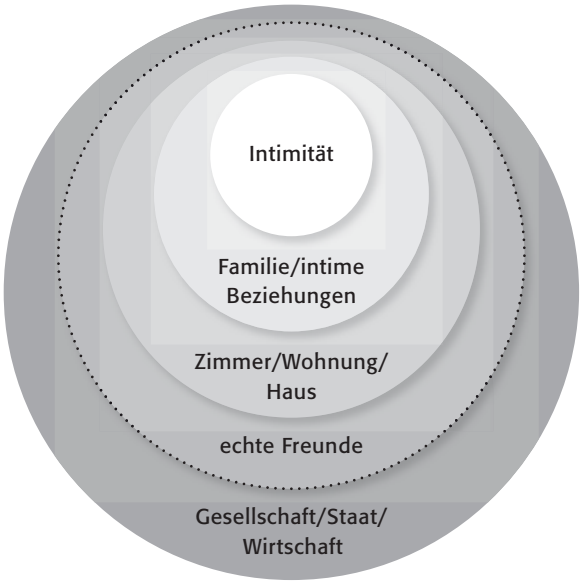


Abb. 4: „Räumliche" Privatsphäre

Doch so eindeutig, wie es scheint, ist diese Trennung nicht. Sofern es sich um die Privatsphäre von Personen handelt, kann sie nicht nur Räumen oder Orten zugeschrieben werden, sondern auch „Handlungen, Situationen, (mentalen) Zuständen (...) und Gegenständen"[3]. In **räumlicher** Hinsicht kann man sich die Verwendungsweisen von „öffentlich" und „privat" vorstellen wie die Schichten einer Zwiebel: Im Innersten liegt der Bereich der persönlichen Intimität und Privatheit, z. B. in Form eines Tagebuchs. Die zweite Schicht ist die des klassischen Privatbereichs: die Familie oder andere intime Beziehungen. Repräsentiert wird die Privatsphäre meist durch private Räume wie die eigene Wohnung oder das Haus (vgl. Abb. 4). Demgegenüber bildet die Öffentlichkeit das gesellschaftliche und staatliche Außen.

Bezogen auf **Handlungen oder Entscheidungen** kann man aber auch in der Öffentlichkeit „privat" sein: Ob ich zu einer Demonstration oder in die Kirche gehe, ist ebenso meine Privatsache wie das Gespräch, das ich mit einem Freund im Café führe, oder die Wahl der Kleidung, die ich in der Öffentlichkeit trage. **Private Informationen** können z. B. meine politische Einstellung oder meine Meinung über eine Person sein, aber auch Daten zu meiner Gesundheit oder das Wissen darüber, mit wem ich zusammenlebe.

*„Privat" nennen wir also sowohl **Räume**, **Handlungen** und **Verhaltensweisen** sowie **bestimmte Informationen**.*

„Privat" ist jedoch nicht gleichzusetzen mit „geheim". Privates kann geheim sein, muss es aber nicht – wie die Kleidung einer Person in der Öffentlichkeit. Umgekehrt muss Geheimes – wie etwa Staatsgeheimnisse – nicht zwangsläufig privat sein. Zudem ist „privat" nicht dasselbe wie „intim": Intimität ist ein Kernbereich des Privaten, aber nicht identisch mit ihm. Privatheit umfasst einen größeren Bereich.

1.2 Hier kann ich ich sein

Formen und Funktionen der Privatheit

Reflexionsfrage: *Welche Formen und Funktionen hat die Privatsphäre?*

Der Politologe und Jurist Alan F. Westin (1967) hat vier Formen des Privaten beschrieben:

- **Für-sich-Sein (Solitude):** beschreibt die Situation des Individuums, in dem es für sich alleine ist und damit frei von der Wahrnehmung bzw. Beobachtung durch andere.
- **Intimität (Intimacy)** bezieht sich auf die Situation in einer Liebesbeziehung oder einer kleinen Gruppe von Freunden oder der Familie, in der sich die Beteiligten im gegenseitigen Vertrauen einander öffnen können.
- **Anonymität (Anonymity)** meint die Freiheit, in der Öffentlichkeit nicht identifiziert und somit nicht beobachtet oder kontrolliert zu werden.
- **Zurückhaltung (Reserve)** – als die unterschwelligste Form von Privatsphäre – bezieht sich auf die geistige und körperliche Zurückhaltung gegenüber anderen, wie sie sich z. B. in Anstandsformen ausdrückt, wenn Menschen auf engem Raum (wie einem Fahrstuhl) aufeinandertreffen.

Im Zusammenleben haben sich eine Reihe unterschiedlicher Mechanismen zur Regulation der Privatsphäre entwickelt, die von kulturellen Normen (z. B. Anstandsregeln) über die räumliche Gestaltung der Umgebung (z. B. Architektur) bis zu nonverbalen (z. B. Kleidung) und verbalen Verhaltensweisen reichen. Die einzelnen Regulationsmechanismen können sich von Kultur zu Kultur unterscheiden.

Der optimale Grad an Privatheit wird nicht durch die größtmögliche Abgrenzung von anderen (Einsamkeit oder Isolation) erreicht, sondern ist ein dynamischer Prozess, der je nach individueller Konstitution und Situation variiert. Die beiden Pole, zwischen denen der Einzelne das für sich ideale Maß an Privatsphäre aushandelt, sind das individuelle Bedürfnis nach sozialer Interaktion einerseits und dem nach Privatsphäre andererseits.

Für Westin hat die Privatheit zudem vier zentrale Funktionen, die auch heute noch gültig sind (vgl. Abb. 5).

Die Privatsphäre bietet also einen geschützten Raum, in dem wir unabhängig von Beeinflussungen anderer agieren können – und damit authentisch und selbstbestimmt die sein können, die wir sein wollen. Hier können wir ohne Zwänge frei nachdenken, uns ausprobieren und uns unsere Meinung bilden.

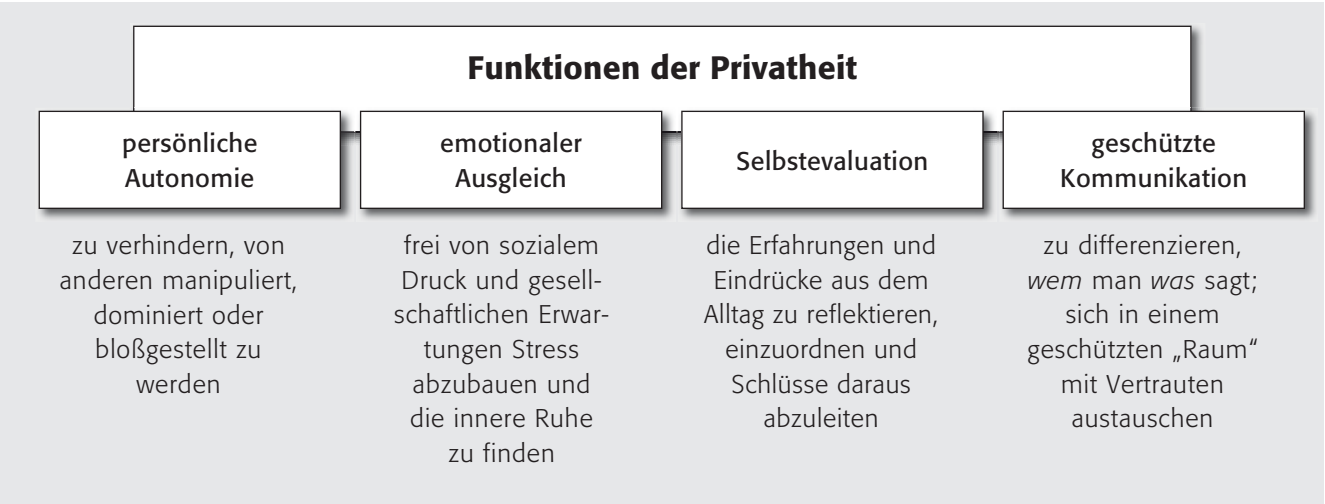


Abb. 5: Funktionen der Privatheit

1.3 Machen wir uns freiwillig zum gläsernen Menschen?

Privatsphäre im digitalen Zeitalter

Reflexionsfragen: *Welche Veränderungen haben sich seit der Einführung des Social Web für die Privatsphäre ergeben? Welche Nachteile können für mich durch die Preisgabe privater Informationen entstehen?*

Private Details werden nicht erst seit der Einführung des Web 2.0 (Social Web) in der Öffentlichkeit thematisiert. Früher jedoch war der Zugang zur Öffentlichkeit nur über Medieninstitutionen wie Verlage, Fernsehsender oder Radioanstalten möglich. Im Web 2.0 kann nun jeder mitmachen und ein Millionenpublikum erreichen. Die Rahmenbedingungen für die Privatsphäre haben sich damit gravierend verändert: Niemals zuvor war die potenzielle Verfügbarkeit von privaten Informationen größer, da die Voraussetzung für die Teilhabe am Social Web die Preisgabe von persönlichen Daten ist.

Anders als bei der verbalen Face-to-Face-Kommunikation werden die preisgegebenen Informationen im Netz veröffentlicht und liegen in digitaler Form vor. Sie sind damit nicht mehr flüchtig, sondern **beständig** und **langfristig verfügbar**. Diese privaten Informationen sind mithilfe von Suchmaschinen **auffindbar** und auf diese Weise auch **zusammenführbar**; sie lassen sich **beliebig vervielfältigen** und **aus ihrem ursprünglichen Kontext lösen** und in einen anderen übertragen.[4]

Die **fehlende soziale, räumliche und zeitliche Abgrenzung** des Social Web erschwert die Aufrechterhaltung der verschiedenen sozialen Kontexte: Der Nutzer kann kaum einschätzen, wie viele Personen seine persönlichen Informationen einsehen können und wer sie sind – Freunde und Familie oder Bekannte, Kollegen oder gar Fremde. Selbst bei strikter Nutzung der Privatsphäre-Einstellungen in Online-Netzwerken und/oder der Festlegung verschiedener Empfängergruppen in WhatsApp können Daten dupliziert und an unerwünschte Empfänger weitergeleitet werden. Diese unerwünschte Öffentlichkeit kann zu einem großen Problem werden: Oft sagen wir unseren Eltern nicht das, was wir einem Freund erzählen, oder unserem Chef nicht, was wir unserer Familie preisgeben. In unterschiedlichen Kontexten sind wir unterschiedliche Menschen. Wir brauchen diese verschiedenen sozialen Rollen.

Das Privacy-Paradox

Obwohl seit einigen Jahren insbesondere Kinder und Jugendliche sensibilisiert werden, dass man im Netz vorsichtig sein soll mit der Preisgabe persönlicher Informationen, und die NSA-Affäre das Thema Datenschutz zusätzlich in das öffentliche Bewusstsein katapultiert hat,[5] existiert nach wie vor das sogenannte Privacy-Paradox[6]. Damit wird das Phänomen beschrieben, dass die Nutzer den Schutz ihrer Privatsphäre zwar generell für wichtig halten, dies aber nicht unbedingt auf ihr Handeln übertragen. So belegt auch eine aktuelle Studie zum Datenschutzverhalten bei der Nutzung von Apps: „Trotz des eindeutigen Sicherheitsbewusstseins gibt es immer noch eine eindeutige Diskrepanz zum tatsächlichen Nutzerverhalten, wenn es um beliebte Social Apps wie Facebook oder WhatsApp geht. Denn mit 51% ist über die Hälfte der Befragten aufgrund von Datenschutzgründen nicht bereit, auf diese Apps zu verzichten."[7] Auch bei Suchmaschinen ändern die wenigsten ihre Gewohnheiten: In Deutschland nutzen mehr als neunzig Prozent Google, trotz aller Kritik an den Datenschutzpraktiken des Unternehmens. Alternative Suchmaschinen sind kaum bekannt.

Es gibt einige mögliche Erklärungen für dieses paradoxe Verhalten: So könnte mangelndes Wissen über vorhandene Schutztechniken oder Probleme im Umgang mit diesen die Ursache sein. Oder aber das genaue Gegenteil: Eine digital sozialisierte Generation glaubt, „die digitale Selbstdarstellung unter Kontrolle



zu haben. Dass man also das komplexe Gesamtbild, das man von sich digital mosaikhaft zusammensetzt, steuern könne."[8] Ein wesentliches Motiv könnte auch die starke Gewöhnung an den Komfort der digitalen Dienste und Geräte sein, die bis hin zur Abhängigkeit gehen kann. Vielleicht existiert aber auch grundsätzlich ein mangelndes Bewusstsein gegenüber den Folgen der digitalen Datenpreisgabe, weil die Probleme zu komplex sind, um sie einer größeren Öffentlichkeit verständlich zu machen?[9]

„Ich habe doch nichts zu verbergen."

Sehr beliebt ist das Argument, man habe ja nichts zu verbergen und daher auch nichts zu befürchten. Doch das ist ein Irrtum. Es kann jedem schaden, wenn bestimmte private Informationen – wie z. B. über eine schwere Krankheit – öffentlich werden. Es wird gerne übersehen oder vergessen, „dass Daten kein feststehendes, objektives und immer richtiges Bild vermitteln, sondern verarbeitet, verknüpft und verwertet werden und dabei immer neue Informationen ergeben. Das Bild, das andere so von einer Person gewinnen, kann ganz anders aussehen als das Bild, das die betroffene Person selbst für korrekt hält. Außerdem ist vielen möglicherweise zu wenig bewusst, dass sie auch unschuldig ins Visier der Sicherheitsbehörden geraten können. Sie meinen, Überwachungsmaßnahmen träfen nur andere, etwa Terroristen."[10]

Mein Ich gehört mir:
Kontrolle über die eigene Identität

Um seine Privatsphäre in einer digitalen und vernetzten Welt zu schützen, muss man die Kontrolle über seine privaten Daten behalten. Beate Rösslers Definition beschreibt das sehr treffend: „(…) als privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas' kontrollieren kann."[11]



Privatheit ist zu verstehen „in dem Sinn, dass ich Kontrolle darüber habe, wer welchen ‚Wissenszugang' zu mir hat, also wer welche (relevanten) Daten über mich weiß; und in dem Sinn, dass ich Kontrolle darüber habe, welche Personen ‚Zugang' oder ‚Zutritt' in Form von Mitsprache- oder Eingriffsmöglichkeiten haben bei Entscheidungen, die für mich relevant sind".
***Beate Rössler,** 2001, S. 24*

Diese Form der Kontrolle ist nicht nur räumlich, sondern vor allem metaphorisch zu verstehen.
Ich entscheide selbstbestimmt darüber, wer was wann und in welchem Zusammenhang über mich weiß. Oder, wie es Steffan Heuer und Pernille Tranberg ausdrücken:





„Wer seine Privatsphäre schützen will, muss die Kontrolle über möglichst viele Bestandteile seiner Identität behaupten. Wir sind die Summe der Dinge, die uns beschreiben – unsere Eigenschaften, unsere Vorlieben und Abneigungen, unsere Leidenschaften, unsere Gene, Gesichtsprofile, Netzhautscans, Sprachmuster, unser Freundeskreis, unser Surfverhalten im Web und sogar die Art, wie wir gehen (…)."
***Steffan Heuer & Pernille Tranberg,** 2013, S. 23*

2 Nichts zu suchen, aber viel zu finden

Erkennen der Mechanismen von Datenpreisgabe und Datensammlung

Reflexionsfrage: *Wer erhebt und verarbeitet private Daten und gibt sie gegebenenfalls weiter?*

2.1 Jäger und Sammler
Datenspuren im Netz

Die Daten, die wir freiwillig in den sozialen Medien preisgeben, sind nur ein Teil der Datenspuren, die wir überall hinterlassen. Diese Datenspuren werden von verschiedenen – vor allem kommerziellen – Datensammlern aufgezeichnet, ausgewertet, verwendet und/oder weitergegeben. „Diese Datensammlung (...), die neben der Verbreitung von selbst (mehr oder weniger bewusst) freigegebenen (Profil-)Informationen eine potenziell weitreichendere Dimension hat, wenn es um Fragen von Identität, komplex aggregiertem Wissen über eine Person, Bewegungsprofile u.v.m. geht, stellt das **weitaus wirkmächtigere Problem** im Kontext des Datenschutzes dar."[12] Wenn unser Verhalten im Netz permanent verfolgt, aufgezeichnet und ausgewertet wird, verkehrt sich das Internet als vermeintliches Instrument der Freiheit, der Teilhabe und der Transparenz in sein Gegenteil: zum Instrument der Überwachung.

Dass die allgegenwärtige Datensammlung eher noch unterschätzt wird, zeigt auch eine aktuelle Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI): „Wenn von Öffentlichkeit die Rede ist, denken Jugendliche und junge Erwachsene nicht an eine mögliche Überwachung durch Staaten, ein Mitlesen und Datensammeln von Unternehmen oder anderen institutionalisierten Speicherungsverfahren, sondern in erster Linie an ihre Peergroup und damit an die Reputation innerhalb ihres Netzwerks."[13] Ihnen ist in der Regel aber bewusst, dass ihre Online-Aktivitäten verfolgt und die Erkenntnisse daraus für personalisierte Werbung genutzt werden. Dagegen haben sie kaum Vorbehalte, im Gegenteil: Sie sehen darin eher einen praktischen Nutzen.[14]

Eine Sensibilisierung für die Situationen und Umstände, in denen wir Datenspuren hinterlassen und in denen Daten gesammelt werden, ist eine notwendige Voraussetzung, um die daraus resultierende Gefahr für die eigene Privatsphäre einschätzen zu können. Beispielhaft gibt folgende Tabelle eine Übersicht über Datensammler in den digitalen Räumen, der analogen Welt und der vernetzten Umwelt (dem Internet der Dinge; vgl. Abb. 6).

Digitaler Raum	Analoger Raum	Vernetzte Umwelt/Internet der Dinge
• Soziale Medien • Suchmaschinen • Surfen (Cookies) • Online-Shopping • Apps • Cloud-Computing • Smartphone/Tablet • E-Book-Lesegeräte • ….	• Staatliche Stellen (Polizei, Finanzbehörden, Geheimdienste) • Verbindungsdaten (Telefon, SMS) • Ausweispapiere • Kundenkarten • Kreditkarten • Gesundheitskarte • Video-Überwachung • Navigationsgeräte • Mautstationen • Flugdaten • ….	• Vernetztes Zuhause (Smart Home) • Self-Tracking Devices (z. B. Fitness-Armband) • Vernetztes Auto • Smarte Kleidung • ….

Abb. 6: Datensammler

Über jeden von uns werden mehr Daten gesammelt und gespeichert als je zuvor, auch weil wir selbst und unsere digitale Umgebung immer mehr Daten hinterlassen. Vor allem das Internet hat die Sammlung persönlicher Daten erleichtert, sie billiger und nutzbarer gemacht. Man kann herausfinden, welche Hobbys wir haben, in wen wir uns verlieben werden, wie wir politisch denken, ob wir uns demnächst scheiden lassen, Kinder bekommen oder krank werden. Dieses Wissen, das mittels Algorithmen auch aus den scheinbar harmlosesten Angaben gewonnen wird, bedroht unsere Privatsphäre.

Video aus der Sendung Quarks & Co: „Die tägliche Datenspur: Wie das digitale Ich entsteht": ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-digitalesich100.html***

Wir stehen inzwischen unter ständiger Beobachtung – auch wenn wir uns nicht im Internet bewegen. Jede Zahlung mit der Kreditkarte, jede Flugbuchung im Reisebüro, jedes Handy hinterlässt Datenspuren. Auch wenn wir selbst nicht Mitglied bei Facebook sind, weiß Facebook aus den Adressbüchern seiner Mitglieder etwas über uns – und kann so auch Profile über die soziale Vernetzung von Menschen anlegen, die gar kein Facebook-Konto haben. Und über immer intelligentere Endgeräte – z. B. eine Videoüberwachung, die mit einer Mustererkennung für Gesichter, Sprache und Verhalten gekoppelt ist, oder durch RFID-Chips (Internet der Dinge) – können Daten aus unserem analogen Leben ins Digitale übertragen werden.

„Internet der Dinge" *bezeichnet die Vernetzung von Gegenständen des Alltagsgebrauchs über das Internet, damit diese selbstständig miteinander kommunizieren können. Dazu müssen sie beispielsweise über IP-Adressen eindeutig identifizierbar sein. Diese Objekte sammeln, speichern und verarbeiten Informationen, z. B. über eine Person oder eine Umgebung. Ihre Programmierbarkeit, ihr Speichervermögen, ihre Sensoren und ihre Kommunikationstechnik befähigen sie, online und autark Informationen auszutauschen. Dadurch erledigen sie verschiedene Aufgaben für den Nutzer und können so unterschiedlichste Lebensbereiche des Menschen optimieren.*

2.2 Eine verhängnisvolle Affäre?



Heute versteht man unter dem Begriff ***Big Data*** *vor allem „die auf der Grundlage gewaltiger Speicher- und Auswertungskapazitäten mögliche* ***Datenanalyse*** *zur Gewinnung neuer Erkenntnisse".* ***Thilo Weichert,*** *2013*

Big Data

Big Data steht als Sammelbegriff für die riesigen Datenmengen, die überall entstehen und mit herkömmlichen Speicherungs- und Analysewerkzeugen nicht zu bewältigen sind. Das war der Anlass zur Entwicklung von Werkzeugen wie Google Map-Reduce oder Hadoop von Yahoo, mit denen gewaltige Datenmengen verarbeitet werden können – auch dann, wenn sie nicht bereits in Datenbanken, sondern unstrukturiert vorliegen, wie es bei allen Texten, Bildern und Videos aus sozialen Medien der Fall ist. Die Internetkonzerne haben diese Programme entwickelt, da sie selbst über die größten Datenmengen verfügen und ein finanzielles Interesse daran haben, die von ihnen gesammelten Daten kommerziell zu verwerten.[15] Experten des Weltwirtschaftsforums in Davos haben 2011 personenbezogene Daten als „das Öl von heute" bezeichnet.[16] Im digitalen Zeitalter werden „**alle** Daten als wertvoll betrachtet (...), und zwar aus sich selbst heraus"[17]: Sie sind inzwischen zum Kerngeschäft vieler Unternehmen geworden.

Video zu „Big Data" von der Landesanstalt für Medien NRW (LfM): ***http://www.youtube.com/watch?v=otWN5o1C2Bc***

Über eine intelligente Auswertung gigantischer Datenmengen und die Kombination von Daten aus verschiedenen Quellen können weitreichende Schlussfolgerungen gezogen werden. Es lassen sich statistische Trends oder Muster, Gesetzmäßigkeiten oder Korrelationen zwischen einzelnen Merkmalen erkennen. Auf diese Weise werden beispielweise mit Hilfe von Korrelationen bei der Auswertung von Vergangenheit und Gegenwart Zukunftsprognosen erstellt. Solche Vorhersagen sind aus vielfältigen Gründen äußerst interessant für Unternehmen, Organisationen und Staaten: Mit ihnen lassen sich Gefahren frühzeitig erkennen, Risiken minimieren, Zeit sparen und Gewinne machen. Sie können aber auch dazu dienen, Kontrolle und Macht auszuüben.

Es wird also Nutzen aus Informationen gezogen, die möglicherweise für etwas ganz anderes gesammelt wurden und erst einmal scheinbar wertloses Material waren, bis sie durch Analyse, Verknüpfung oder Reorganisation in wertvolle Daten umgewandelt wurden.[18] Die Daten verlieren dabei nicht an Wert und können immer wieder für andere Zwecke wiederverwendet werden.

Video (Quarks & Co): „Partnersuche 2.0: Wie aus Big Data Big Business wird“ ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-partnersuche100.html***

3 Das Ende der Privatsphäre?

Auseinandersetzung mit den Risiken von Big Data

Reflexionsfrage: *Was kann mit – freiwillig oder unfreiwillig – preisgegebenen privaten Informationen geschehen?*

Personenbezogene Daten werden vor allem mit den Methoden **Tracking** und **Scoring** ausgewertet. Beide dienen dazu, eine Vorhersage über zukünftiges Verhalten zu ermöglichen, indem Profile einer Person oder einer Gruppe erstellt werden – über Interessen, Konsum, Aufenthaltsorte, Sozialkontakte, Kreditwürdigkeit, Verhalten oder Gesundheit.

3.1 „Zeige mir, wo Du klickst, und ich sage Dir, wer Du bist.“

Tracking
Beim Tracking wird das Verhalten einer Person anhand einer bestimmten Eigenschaft verfolgt. Schon ein eingeschaltetes Handy – es muss kein Smartphone sein – und die dabei entstehenden Metadaten wie Empfänger, Dauer, Anzahl der Gespräche oder Aufenthaltsort genügen, um ein detailliertes Profil und damit Einblicke in das Privatleben eines Einzelnen zu erhalten. Es ist also gar nicht notwendig, den Inhalt einer Kommunikation auszuwerten.

Im Internet bedeutet Tracking, dass unser Surf-, Nutzungs- und Konsumverhalten beobachtet wird. Für das Sammeln von Informationen auf den Webseiten werden Cookies eingesetzt. Diese kleinen Dateien verfolgen uns im gesamten Web und dienen in erster Linie Werbe- und Marketingzwecken. Jeder Nutzer erhält dabei eine ID-Nummer, über die er immer wieder erkannt wird. Der Besuch einer Webseite löst im Durchschnitt 56 Tracking-Vorgänge aus, die zu 40 Prozent von großen Werbenetzwerken ausgehen. Ziel ist es, dem Nutzer unmittelbar beim Aufruf einer Webseite eine auf ihn zugeschnittene Werbung zeigen zu können. Dazu laufen im Hintergrund Online-Auktionen ab, bei denen automatisierte Systeme in Millisekunden Werbung für Webseiten verkaufen.[19]

Nun könnte man sagen: „Prima, das ist doch toll, wenn ich auf meine Interessen zugeschnittene Werbung erhalte.“ Oder: „Die Werbung beachte ich doch gar nicht, was soll’s.“ Das greift jedoch zu kurz. Denn unser Surfverhalten sagt viel über uns und unser Leben aus:

über unsere Interessen, Sorgen, Vorlieben oder Gedanken. „Zeige mir, wo Du klickst, und ich sage Dir, wer Du bist."[20] Eine französische Studie[21], die das Surfverhalten von fast 370.000 Internetnutzern ausgewertet hat, zeigt, dass sehr viele Nutzer schon nach dem Besuch von vier Webseiten von spezieller Software automatisch identifiziert werden können, weil 69 Prozent von uns eine einzigartige, unverwechselbare Surf-Historie besitzen, die wie ein Fingerabdruck ist. Wenn man sich vor Tracking nicht schützt, ist Anonymität – und somit der Schutz der Privatsphäre – beim Surfen im Netz nicht möglich.

Wird überdies das Tracking aus der Onlinewelt mit dem Tracking aus der „realen" Welt (z. B. über Kreditkarten, Kundenkarten oder Bonusprogramme) verbunden, werden die Kenntnisse über jeden Einzelnen und somit auch die Manipulationsmöglichkeiten immer umfangreicher. Die Qualität der Analysen und der Vorhersagen steht und fällt mit der Menge und der Qualität der Rohdaten, die einem Individuum zugeordnet werden können – und der Algorithmen, die diese Daten auswerten.



*Video: Quarks & Co zeigt die von Charles Duhigg recherchierte Geschichte über die Schwangerschaftsprognosen von TARGET: „Kassenbon als Schwangerschaftstest", **http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-talk-kassenbon100.html***

3.2 Big Brother is scoring you

Scoring

Beim Scoring erfolgt die zahlenmäßige Bewertung einer Eigenschaft einer Person durch die mathematisch-statistische Analyse von Erfahrungswerten aus der Vergangenheit, um ihr zukünftiges Verhalten vorherzusagen. Das bedeutet, einer Person wird ein individueller Scorewert als Ausdruck eines bestimmten für sie vorhergesagten Verhaltens zugeordnet. Scoring basiert dabei auf der Annahme, dass bei Vorliegen bestimmter vergleichbarer Merkmale **anderer Personen** ein ähnliches Verhalten vorausgesagt werden kann. So kann es auf der Basis schon weniger Daten zu einer Person – wie der Adresse – zu Risikoeinschätzungen kommen. Diese Einschätzung kann sich auf ganz verschiedene Bereiche menschlichen Verhaltens beziehen: auf die zukünftige Arbeitsleistung, auf die Vorhersage kriminellen Verhaltens oder zur Prognose des Gesundheitszustands. Am häufigsten und bekanntesten ist das Scoring hinsichtlich der Wahrscheinlichkeit, mit der eine Person eine Rechnung zahlen oder einen Kredit zurückzahlen wird, wie es zum Beispiel die Schufa macht.

Heute stehen neben den Informationen der Auskunfteien weit mehr Quellen zur Verfügung, um individuelle Risikoprofile und somit individuelle Preise für Kunden zu erstellen. So wertet etwa der Versicherer Axa Global Direct nach eigenen Angaben ca. 50 Variablen aus, um daraus die individuelle Prämie zu ermitteln – darunter Browser-Cookies, das Einkaufsverhalten oder Party-Einträge bei Facebook.[22]

3.3 Die Vermessung des Menschen

Profilbildung und Klassifizierung

Auf der Basis unserer Daten werden wir also vermessen, bewertet und klassifiziert oder es werden ganze Profile von uns erstellt. Man kann uns in gute und schlechte Kunden einteilen, uns individuelle Preise oder Prämien abverlangen, uns für kreditwürdig oder nicht halten, unsere Bedürfnisse und Verhaltensweisen prognostizieren und uns eine Versicherung verweigern oder zu schlechteren Konditionen anbieten. Darüber hinaus lassen sich aus unseren Daten auch politische und religiöse Einstellungen, gesundheitliche Verhältnisse, die sexuelle Ausrichtung, selbst Gefühle und Stimmungen ableiten. Daraus ergeben sich für die Unternehmen und Organisationen, die diese Daten besitzen, umfassende Möglichkeiten zur **Manipulation, Diskriminierung, sozialen Kontrolle** und **Überwachung**. Für uns selbst bedeutet das im Umkehrschluss eine **Einschränkung unserer Entscheidungs- und Handlungsfreiheit**.

Was, wenn ein potenzieller Arbeitgeber sich nicht mehr die Mühe macht, jemanden persönlich kennenzulernen, weil er über Facebook scheinbar schon alles für ihn Relevante über die Person erfahren hat? Dass viele Arbeitgeber sich die Facebook-Profile ihrer Bewerber anschauen, ist nicht neu. Nun hat eine Studie[23] jedoch gezeigt, dass die aus Facebook-Profilen gewonnenen Daten die Leistungsfähigkeit von Bewerbern präziser vorhersagen konnten als klassische Eignungs-Tests. Genauso ist denkbar, dass Tweets einem Personalchef Einblick in die Persönlichkeit des Bewerbers geben: Anhand dessen Ausdrucksweise, der Art der Ansprache und der Themen kann analysiert werden, ob er labil, extrovertiert, offen für Neues, verträglich oder gewissenhaft ist. Kommt es dann noch auf den persönlichen Eindruck an?

Viele von uns tragen selbst dazu bei, dass Profilbildung und Klassifizierung immer perfekter werden. Sie geben freiwillig wertvolle und sehr persönliche Daten von sich preis: ihre Fitness- und Vitaldaten, wie zurückgelegte Schritte oder Entfernungen, Geschwindigkeit, Herzfrequenz, Körpertemperatur, Kalorienverbrauch, Ruhephasen etc. Mit Sensoren ausgestattete Armbänder oder Schuhe, sogenannte Fitness-Tracker, und die dazu passenden Apps für das Smartphone sind für viele Hobby-Sportler Teil ihres täglichen Lebens geworden. Vielen macht es Spaß, sich so mit anderen zu messen und Resonanz für die eigenen Aktivitäten von ihren Wettbewerbern oder Freunden zu bekommen. Sie finden es nicht ungewöhnlich, ihre sportlichen Ergebnisse mit dem Rest der Welt zu teilen. Die aufgezeichneten Daten könnten aber auch unser gesamtes Gesundheitssystem verändern – wenn die gesundheitliche Dauererhebung künftig zur Norm werden würde, um die Krankenkassen zu entlasten.



3.4 Wir wissen, wer du bist!

Die „Big Four" Apple, Google, Facebook und Amazon

Vier große Konzerne aus den USA dominieren das Internet-Geschäft: Apple, Google, Facebook und Amazon. Obwohl ihre Angebote international sind, sehen sich die vier als amerikanische Unternehmen. Dies hängt auch damit zusammen, dass mit dem Thema Verbraucher- und Datenschutz in den USA lockerer umgegangen wird. Das strengere europäische Verbraucher- und Datenschutzrecht ist deshalb nur sehr schwer durchzusetzen.

Mehr als 800 Millionen Menschen nutzen regelmäßig Facebook. Mittlerweile gehören dem Unternehmen auch weitere Dienste wie WhatsApp oder Instagram. Der Erfolg von Facebook basiert auf dem sogenannten Social Graph: Er zeigt an, mit wem man befreundet ist, welche Musik man mag, welche Artikel man gelesen hat, wo man sich gerade befindet, wohin man gerne in Urlaub fährt oder – „Gefällt mir!" – was man gerade im Internet interessant findet. Werbekampagnen von Drittanbietern können bei Facebook dank dieser Informationen gezielt auf den einzelnen Nutzer zugeschnitten werden. Was das Unternehmen darüber hinaus mit den Nutzerdaten macht, bleibt weitgehend intransparent. Allerdings schloss Amazon vor nicht allzu langer Zeit einen Vertrag mit Facebook ab, um sein Kaufempfehlungssystem mit Hilfe des Social Graphs zu optimieren.[24]

„Wir wissen, wo du bist. Wir wissen, wo du warst. Wir können mehr oder weniger wissen, was du gerade denkst." Das hat nicht der Chef eines Geheimdienstes oder ein Diktator gesagt, sondern der Verwaltungsratschef von Google, Eric Schmidt.[25] Google weiß sehr viel über seine Nutzer, nicht nur aufgrund seiner Quasi-Monopol-Stellung im Suchmaschinenmarkt (siebzig Prozent Weltmarktanteil). Google ist zudem Eigentümer von YouTube, der größten Videoplattform, von Android, dem wichtigsten Betriebssystem für mobile Geräte (und bald in Spielekonsolen, Fernsehern, Autos und Kameras), von Chrome, dem inzwischen größten Browser, und von Gmail, dem weltweit meistgenutzten E-Mail-Dienst, bei dem sämtliche E-Mails von Google automatisiert durchsucht werden. Die Marktführerschaft in all diesen Bereichen führt zu einer unglaublichen Machtfülle, wie es Eric Schmidt selbst in seinem Buch „Die Vernetzung der Welt"[26] bestätigt:
Google kann seit der Änderung seiner Datenschutzbestimmungen im März 2012 – gegen die europäische Datenschützer vorgehen – die Daten seiner Nutzer quer über all seine Dienste auswerten und so einen umfassenden Wissensstand über alle Lebensbereiche aufbauen. Auf Kritik daran entgegnet Google, dass es das alles nur mit Erlaubnis der Nutzer tue. Das ist insofern problematisch, da die Nutzer meist nicht wissen (können), welche Daten sie preisgeben und was damit zukünftig geschieht. Selbst wenn ich Google-Produkte nicht nutze, kann Google Informationen und Daten über mich sammeln – über Dritte, die Gmail, eine Google-Kontaktliste oder den Google-Kalender nutzen. Damit wird das Grundrecht auf informationelle Selbstbestimmung ausgehebelt.



„Wir sind überzeugt, dass Portale wie Google, Facebook, Amazon und Apple weitaus mächtiger sind, als die meisten Menschen ahnen. Ihre Macht beruht auf der Fähigkeit, exponentiell zu wachsen. Mit Ausnahme von biologischen Viren gibt es nichts, was sich mit derartiger Geschwindigkeit, Effizienz und Aggressivität ausbreitet wie diese Technologieplattformen, und dies verleiht auch ihren Machern, Eigentümern und Nutzern neue Macht."
***Eric Schmidt,** 2013*

Video: LfM Digitalkompakt „Apple. Google. Facebook. Amazon." ***https://www.youtube.com/watch?v=h2hiuzTjegg***

4 Mein Leben gehört mir!

Reflexion über die Folgen der Verletzung der Privatsphäre



Reflexionsfrage: *Welche Folgen können sich aus der gewollten oder ungewollten Preisgabe persönlicher Daten ergeben?*

Die Risiken für die Privatsphäre, die sich durch die Digitalisierung ergeben, lassen sich in zwei Bereiche aufteilen:

1. Verletzungsmöglichkeiten, die sich auf Basis des von mir oder durch andere über mich im Netz Veröffentlichten ergeben – und daher meist von unmittelbaren Kommunikationspartnern oder von denen ausgehen, die Zugang zu diesen Daten haben (s. 4.1).
2. Verletzungsrisiken durch die unkontrollierbare Verwendung von privaten Daten durch kommerzielle Datensammler (s. 4.2).

4.1 Kein Recht auf Vergessen?

Schädigung durch die Preisgabe privater Informationen

Die individuellen Verletzungsrisiken in den Sozialen Medien basieren vor allem auf der Verzerrung und der unkontrollierten Weitergabe von Informationen von oder über uns. Es kann durch diesen Missbrauch zu Mobbing, Stalking, Identitätsdiebstahl, Beleidigungen, peinlichen Bloßstellungen oder ernsten Reputationsschäden (die z. B. die Karriere behindern) kommen sowie zu Chancenminimierung (z. B. bezüglich eines Jobs) oder Diskriminierungen (z. B. aufgrund äußerlicher Merkmale).

Wenn Menschen Einblicke in privates Handeln und Denken erhalten, denen man selbst diese Einblicke nicht gewähren würde, wird die eigene Privatsphäre ausgehöhlt. Andere erhalten die Möglichkeit, uns zu beobachten und auf Basis der Informationen Beurteilungen zu treffen und diese zu verbreiten – egal, ob sie uns kennen oder nicht. Es ist kaum möglich, unter diesen Bedingungen die eigene Selbstdarstellung zu steuern und zu kontrollieren, also selbst darüber zu bestimmen, wie man sich definiert und darstellt.

Dabei sollte die Deutungshoheit über das eigene Leben bei jedem selbst liegen. Der Schutz vor der unkontrollierbaren Verwendung privater Informationen – also der Schutz der Privatsphäre – ist eine notwendige Voraussetzung für die Ausbildung einer Identität, die es mir erlaubt, ein mündiges und selbstbestimmtes Leben zu führen.

Dazu gehört auch, selbst bestimmen zu dürfen, welche biografischen Ereignisse man Anderen zur moralischen Beurteilung zugänglich machen möchte – also frei zu entscheiden, welche Lebensentwürfe, Rollen und Werte als die „richtigen" erkannt werden. Dies lässt sich als Recht auf „Lebensexperimente"[27] beschreiben. Aufgrund der typischen Merkmale von Daten – Langlebigkeit, Durchsuchbarkeit, Reproduzierbarkeit und Klassifizierbarkeit – ist es jedoch möglich, Vergangenes und Gegenwärtiges zu synchronisieren. Sich persönlich zu entwickeln heißt, auch Fehler zu machen und entscheiden zu dürfen, ob diese anderen zur Beurteilung offenbart oder verheimlicht werden sollen. Gerade in der Jugendphase ist es wichtig, seine Grenzen auszuloten, sich zu orientieren und Rollen auszuprobieren. Was Jugendliche in dieser Phase äußern und beispielsweise auf ihre Profilseite stellen, kann möglicherweise schon kurz darauf nicht mehr ihrer Lebensauffassung und ihrem Wertesystem entsprechen. Menschen das Recht zu nehmen, selbst zu entscheiden, was vergessen werden und was in Erinnerung bleiben soll, heißt, sie in ihrer Identitätsbildung zu behindern.

4.2 Think big: Big Data, Big Power, Big Business

Die Verletzung der Privatsphäre durch Big Data

Die Auswirkungen der Verletzung der Privatsphäre durch Big Data lassen sich mit drei Schlagworten charakterisieren und zusammenfassen: **Big Data, Big Business, Big Power** bzw. **Klassifizierung, Kommerzialisierung** und **Überwachung.**

Ein digitales Double nimmt unseren Platz ein

Klassifizierung
Die Klassifizierung durch Big Data, also die Einteilung in Gruppen und/oder die Zuordnung eines Scores – z. B. bei Kreditauskunfteien oder Versicherungen – bedeutet eine Entpersonalisierung und Konformisierung des Einzelnen. Für die Beurteilung meines Verhaltens ist dabei vor allem das Verhalten sehr vieler Anderer entscheidend, die sich hinsichtlich bestimmter Merkmale ähnlich oder gleich verhalten, die aber dennoch von ihrer Persönlichkeit her nur wenig mit mir gemein haben können.

Menschen werden also aufgrund ihrer durch Big Data vorhergesagten Neigungen beurteilt – und nicht aufgrund ihres tatsächlichen Verhaltens. Damit wird die Chance eingeschränkt, sich anders zu verhalten als vorhergesagt und die Zukunft selbst zu gestalten. Da die Vorhersage auf unseren vergangenen Handlungen beruht, werden diese nicht vergessen: Wir können unserer eigenen Vergangenheit nicht entkommen. Die Verhaltensvorhersagen durch Big Data gefährden also insbesondere unsere Handlungs- und Entscheidungsfreiheit als Subjekt.

Darüber hinaus ist es problematisch, dass aus unseren Datenspuren und Dateneingaben ein digitales Ich geformt wird, dessen genaue Gestalt wir selbst gar nicht kennen können. Dieses „Digitale Double" ist mit unserer eigenen Person nicht identisch – aber es ist das, was Wirtschaftsunternehmen und Sicherheitsbehörden von uns kennen. „Dieser ‚persönliche' Datenzwilling hat für den Originalmenschen etwas zutiefst Unheimliches, und zwar nicht nur deshalb, weil man ihn nicht sieht, sondern weil er zugleich aus Eigenem wie auch aus Fremdem besteht. Sein ‚Datenkörper' verdankt sich der lebendigen Ausgangsperson und ihren Suchbewegungen; doch sein ‚Charakter' und seine ‚Seele' werden von der Internetindustrie definiert – von fremden Blicken, fremden Interessen, fremden Profilern."[28] Was bleibt noch vom Menschen, wenn er ausschließlich anhand von Daten beurteilt wird? Die digitale Datenerfassung kann die Komplexität moralischer Einstellungen und menschlicher Handlungen nicht erfassen, und dem, was eine Person tatsächlich ausmacht, unmöglich gerecht werden.[29]

Zieht man dazu noch in Betracht, dass die zugrunde gelegten Daten fehlerhaft oder von schlechter Qualität sein können, dass sie falsch analysiert oder irreführend verwendet werden und dass wir nicht die Möglichkeit haben, sie zu korrigieren, wird es ganz gruselig.

„Du bist das Produkt!"



„Du bist nicht der Kunde der Internet-Konzerne, du bist ihr Produkt."
***Jaron Lanier,** 2014*

Kommerzialisierung
Unsere sämtlichen Daten werden für Werbekunden ausgewertet, so dass wir in Wirklichkeit mit dem detaillierten Einblick in unser Verhalten, unsere Präferenzen und Interessen bezahlen – also letztlich mit unserer Identität. Wir zahlen einen hohen Preis für die vermeintliche Gratis-Kultur im Netz.

Ein großer Teil unseres Handelns spielt sich im Social Web ab. Es sollte uns also beunruhigen, dass unsere privaten Handlungen und Äußerungen permanent kommerziellen Interessen unterworfen werden und die Internetkonzerne inzwischen eine große Rolle in unserem Leben spielen. Und es sollte uns bewusst sein, dass wir im Zusammenhang mit den Praktiken der Internetkonzerne nicht über Technik debattieren, wie es Evgeny Morozov betont.[30]



„Ich bin kein Technikkritiker. Ich kritisiere die Monopolisierung von Macht durch Technik – und unseren naiven Umgang damit."
***Evgeny Morozov,** 2014*

Dass wir rein rechtlich der Nutzung unserer Daten per AGB selbst zustimmen, verdeutlicht das Dilemma. Denn: Ohne Zustimmung keine Nutzung eines Dienstes. Dabei kann der Nutzer aber in den seltensten Fällen die Folgen seiner Zustimmung abschätzen, selbst wenn er nicht grundsätzlich gegen eine kommerzielle Verwendung der Daten ist. Häufig stehen die genauen Zwecke der Datenverwendung zum Zeitpunkt der Erhebung noch nicht fest, oder es ergeben sich neue Zwecke für eine Wiederverwendung. Oder aber die AGB

werden geändert – und damit grundsätzlich die Spielregeln für die Verwendung. Was passiert in diesem Fall mit den Daten, die zuvor unter anderen Bedingungen erfasst wurden?

Die Diktatur der Algorithmen

Überwachung
Fast niemand weiß, welche Daten über ihn im Umlauf sind und welche Schlussfolgerungen aus ihnen gezogen werden. Big Data ermöglicht eine umfassende und permanente Beobachtung sowie die Dokumentation und Auswertung des Online-Verhaltens – und kann damit die persönliche Freiheit jedes Einzelnen einschränken. Das Argument, wer nichts zu verbergen hat, habe auch nichts zu befürchten, stellt alle unter Generalverdacht. Denn das „Wesen der Freiheit ist doch gerade, dass ich nicht verpflichtet bin, all das preiszugeben, was ich tue, dass ich das Recht auf Diskretion und, ja, sogar Geheimnisse habe, dass ich selbst bestimmen kann, was ich von mir preisgebe. Das individuelle Recht darauf macht eine Demokratie aus. Nur Diktaturen wollen (...) den gläsernen Bürger."[31]

Die Tatsache der ständigen Datenerfassung kann Menschen dazu veranlassen, sich in ihrem Verhalten einzuschränken, um nicht aufzufallen. Das wurde bereits im Volkszählungsurteil festgehalten: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen." Sich nur stromlinienförmig zu verhalten, die eigene Meinung zu verschweigen oder gar den Kontakt zu Menschen zu unterbinden, die sich politisch kritisch äußern, hätte fatale Folgen für eine auf Meinungsfreiheit und Autonomie begründete Demokratie. Damit würde im digitalen Zeitalter eine selbstzensorische Schweigespirale in Gang gesetzt.

Auch eine **Anonymisierung** der Daten scheint kein ausreichender Schutz zu sein, da Big Data mit mehr und vielfältigeren Daten die Re-Identifikation anonymisierter Datenbestände ermöglicht. Auch die harmlosesten Angaben können die Identität eines Menschen enthüllen, wenn jemand nur ausreichend viele Daten gesammelt hat.[32]

4.3 Die Rückkehr zur Autonomie

Ein neues Paradigma?
Korrelationen, die für Bewertungen und Vorhersagen genutzt werden, scheinen das neue Diktum zu sein, das paradigmatisch für die Wissensgenerierung im digitalen Zeitalter steht. Für Alexander Filipović ist damit eine ethische Problematik verbunden: „Im Wesentlichen scheint mir dabei bedeutsam, dass wir je mehr wir auf die Kraft von Big Data vertrauen, immer mehr auf Korrelationen vertrauen, statt auf Theorien, auf sozial abgestimmte und ausgehandelte Erkenntnisinteressen und auf für wahr befundene Gründe. Korrelationen sind an sich nicht schlecht, etwa funktionieren Übersetzungsprogramme auf der Basis von Korrelationen viel besser als auf der Basis von grammatischen Regeln. Aber wenn es darum geht, Vorhersagen über Phänomene, etwa über das Verhalten von Menschen zu machen, und dafür sind Big-Data-Analysen geeignet, dann rechnen wir damit systematisch Handlungsfreiheit und Autonomie aus dem menschlichen Verhalten heraus."[33]




„Solche Ansätze sind die Anfänge, denen man wehren muss, denn sie führen direkt (...) zu einer Welt, in der Entscheidungsfreiheit und freier Wille nicht mehr existieren, in der unser moralischer Kompass durch Vorhersagealgorithmen ersetzt worden ist und in der der Einzelne dem Willen des Kollektivs schutzlos ausgesetzt ist.
So eingesetzt, droht Big Data uns buchstäblich zu Gefangenen von Wahrscheinlichkeiten zu machen."
Viktor Mayer-Schönberger & Kenneth Cukier, *2013, S. 206*

6 Privatheit als Menschenrecht

Ein Ethos der Privatheit entwickeln

Reflexionsfragen: *Warum ist Privatsphäre gut, wünschens- oder schützenswert? Was hat das mit der Entwicklung eines autonomen und freien Subjekts zu tun?*

Wenngleich es zahlreiche Indizien für eine Krise der Privatheit gibt, besteht in den Theorien des Privaten weitgehend Konsens darüber, Privatheit als instrumentellen Wert und kulturelle Errungenschaft einzustufen, da sie eng mit dem modernen Menschenbild eines autonomen, freien und gleichberechtigten Subjekts verbunden ist. So meint der Informationsethiker Kuhlen, dass trotz vorhandener Relativierungstendenzen der Wert der Privatheit weiterhin sehr hoch einzuschätzen ist: Er zählt sie gar zu den Menschenrechten.



„Privatheit gehört zweifellos zu den Menschenrechten, zum kodifizierten Bestand der grundlegenden Rechte und Freiheiten aller Menschen. Auch wenn Privatheit ohne den Zusammenhang von westlichen Wert-, Wirtschafts- und Demokratievorstellungen nicht vorstellbar ist, erhebt Privatheit heute auch einen universalen Anspruch. Dieser wird auch gegenüber radikal veränderten medialen Rahmenbedingungen verteidigt, in erster Linie über das Prinzip der informationellen Selbstbestimmung, juristisch umgesetzt als Anspruch auf Datenschutz. (...) Jedoch sind auch Tendenzen unverkennbar, dass durch freiwilligen Verzicht auf Privatheit, sei es wegen erhoffter ökonomischer Vorteile, aus Einsicht in den vermeintlichen Wert der Sicherheit oder einfach aus Gleichgültigkeit oder Unwissenheit, der hohe Wertstatus von Privatheit relativiert wird."
Rainer Kuhlen, *2004, S. 193 f.*

Für Rössler (2001) und viele andere[35] stellt die Privatheit einen instrumentellen Wert dar, der notwendige Voraussetzung für und Ausdruck von **Autonomie** ist. Wenn es zu einer Relativierung der Privatheit käme, würde dies nach Rösslers Einschätzung auch das Fundament unserer Demokratie treffen: „Dies trifft dann nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist."[36]

In einer liberal-demokratischen Gesellschaft wie Deutschland spiegelt sich die Bedeutung der Privatsphäre auch in der Gesetzgebung wider. Begründet wird das Recht auf informationelle Selbstbestimmung damit, dass durch die Bedingungen der modernen Datenverarbeitung die **Selbstbestimmung bei der freien Entfaltung der Persönlichkeit** gefährdet werde. Wer nicht wisse oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und bevorratet werden, werde aus Vorsicht sein Verhalten anpassen. Man nennt dies „Chilling Effects": vorauseilendes, selbstbeschränkendes Handeln aus Angst vor möglichen Folgen. Dies beeinträchtigt nicht nur die **individuelle Handlungsfreiheit**, sondern auch das **Gemeinwohl**, da ein freiheitlich-demokratisches Gemeinwesen der Mitwirkung seiner Bürger bedarf, ohne dass diese Angst vor Überwachungsmaßnahmen oder späteren Nachteilen haben müssen. Auch in der Gesetzgebung zeigt sich also der enge Zusammenhang zwischen Daten- bzw. Privatsphärenschutz und Demokratie.

Menschen werden bei der Datensammlung auf der Basis von Korrelationen als Digitales Double klassifiziert – mit der Folge, dass ihnen bestimmte Angebote und Optionen unterbreitet oder auch vorenthalten werden. Die Nutzer werden dabei nicht als Individuen erfasst, sondern als ein Daten-Puzzle, das quantifizierbar und kapitalisierbar ist. Hinzu kommt eine **Informationsasymmetrie** zwischen Nutzer und Datensammler: Weder wissen die Nutzer, welche Daten in und aus welchem Kontext genutzt werden, noch ist ihnen der

Algorithmus bekannt, mittels dessen sie klassifiziert werden (**Intransparenz**). Die von den Nutzern oftmals freiwillig gegebenen (oder auch von den Anbietern geforderten) privaten Daten werden zu einem Digitalen Double korreliert und auf der Grundlage intransparenter Formeln „interpretiert".

Aus ethischer Sicht stellt sich die Frage, ob die Objektivierung und Kapitalisierung des Menschen als Digitales Double mit dem Würdekonzept des Menschen vereinbar ist. Für Kant steht „**Würde**" in Gegensatz zu „Preis": Während Dinge einen Preis haben und ausgetauscht werden können, hat der Mensch einen Wert, der über jeden Preis erhaben ist.[37]



„Im Reich der Zwecke hat alles entweder einen Preis oder eine Würde. Was einen Preis hat, an dessen Stelle kann auch etwas anderes, als Äquivalent, gesetzt werden; was dagegen über allen Preis erhaben ist, mithin kein Äquivalent verstattet, das hat eine Würde."
Immanuel Kant, *1786/1999, S. 61*

7 Was können wir tun?

Persönliche, politische und instrumentelle Handlungsoptionen

Reflexionsfragen: *Wie können Menschen vorgehen, die ihre Privatsphäre schützen wollen? Was sollte von der Politik und den Unternehmen unternommen werden?*

Um eine Balance zwischen den Errungenschaften der Digitalisierung und dem Schutz der Privatsphäre zu ermöglichen, möchten wir als ethische Handlungsempfehlung ein Vier-Punkte-Programm vorschlagen (s. 7.1–7.4).

7.1 Digitale Selbstverteidigung

Das Verständnis für die Bedeutung der Privatsphäre und ihre Wertschätzung ist im Bildungssystem und im öffentlichen Diskurs nachhaltig zu verankern. Dabei sollte die häufig geäußerte Meinung „Ich habe ja nichts zu verbergen" als hoch riskant geoutet werden. In summa können folgende Fähigkeiten für eine digitale **Privatheitskompetenz** stehen:

- die Reflexionsfähigkeit, warum private Daten als schützenswert einzustufen sind **(ethische Kompetenz),**
- das Wissen, wer private Daten zu welchem Zweck erhebt, verarbeitet und weitergibt **(strukturelle Kompetenz),**
- die Abschätzung der Folgen, die sich aus der Veröffentlichung privater Daten ergeben können **(Risikokompetenz),**
- das Wissen über Datenschutzrichtlinien und mögliche Schutzmaßnahmen **(rechtliche und technische Kompetenz)**.

Die ersten Schritte digitaler Selbstverteidigung: Privatsphäre-Einstellungen in Netzwerken konsequent nutzen, Browserverlauf und Cookies dauerhaft löschen, statt Google eine der in den Niederlanden ansässigen Suchmaschinen StartPage oder Ixquick verwenden, statt Gmail verschlüsselte E-Mail-Dienste nutzen (z. B. von Telekom oder United Internet), WhatsApp gegen den Messenger Threema eintauschen und den Datenzugriff von kostenlosen Apps verweigern.

Quarks & Co-Video: „Sichere Daten: Tipps zum Datenschutz im Netz" ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-tippszumdatenschutz100.html***

7.2 Politisches Engagement

Digitale Selbstverteidigung reicht alleine nicht aus, um den großen Datensammlern die Stirn zu bieten. Die durch den Missbrauch privater Daten und das blinde Vertrauen in Algorithmen aufgeworfenen ethischen Fragen machen deutlich, dass es sich hier nicht um eine Technikdebatte, sondern um eine gesellschaftliche Debatte handelt. Es sind die Bürger, die entscheiden müssen, ob sie ihr gesamtes Leben Effizienzkriterien unterordnen, ständig beobachtet und sekundengenau analysiert werden und ob sie ihr Verhalten von Softwareprogrammen bestimmen lassen wollen. Das kann sich in politischem Engagement und politischer Partizipation (Demonstrationen, Petitionen, Bürgerrechtsbewegungen) äußern. So gilt seit Mai 2018 die neue EU-Datenschutzgrundverordnung (DSGVO). Diese Datenschutz-Grundverordnung zeigt auch US-amerikanischen Unternehmen wie Google oder Facebook Grenzen auf, denn sie gibt allen EU-Einwohnern das Recht, Einblick in die über sie erhobenen Daten zu erhalten und diese auf Wunsch dauerhaft löschen zu lassen – das sogenannte „Recht auf Vergessenwerden". Außerdem enthält sie eine verschärfte Rechenschaftspflicht für sämtliche Verarbeiter personenbezogener Daten.[39]

7.3 Big-Data-Kodex

Grundsätzlich sind Datensätze weder gut noch schlecht. Angesichts der derzeitigen Entwicklung der digitalen Vernetzungs-, Sicherheits- und Überwachungstechnologien ist allerdings erkennbar, dass **Big Data** vor allem **Big Power** und **Big Business** bedeutet. Unternehmen, Staat und öffentliche Organisationen sollten sich dazu verpflichten, bei der Datenerhebung den Grundsätzen **Verhältnismäßigkeit** (Zweckbindung), **Informationsgleichheit** und **Informationsgerechtigkeit** soweit als möglich gerecht zu werden. Ebenso sollte transparent gemacht werden, welche Algorithmen und Parameter zur Anwendung kommen und die „Auswahl und Qualität der Dateneingabe (…) ständig geprüft und validiert werden"[40].

7.4 Privacy by Design

Bereits bei der Entwicklung von neuen Technologien, Produkten und Vernetzungssystemen sollte gemäß Art. 25 DSGVO eine wesentliche Anforderung sein, den Umfang der verarbeiteten schützenswerten Daten zu minimieren (Datensparsamkeit) und transparent zu machen, welche Daten zu welchem Zweck erhoben und an Dritte weitergegeben werden. Ebenso sollte den Nutzern durch Voreinstellungen ermöglicht werden, sich auch ohne einschlägige IT-Kenntnisse weitgehend schützen zu können (**Privacy by default**). Hierfür müsste eine verstärkte ethische Sensibilisierung der Entwickler erfolgen, auch schon in der Ausbildung. Das Triple-I-Konzept – Informationsgerechtigkeit, Informationsgleichheit und informationelle Autonomie – sollte als kategorischer **Imperativ der Privatsphäre** für Unternehmen und staatliche Einrichtungen eine Art Leitbildfunktion erhalten.



1_1 Datenschutz/Big Data
1_2 Datenschutz – Arbeitsblätter
1_3 Datensatz, Datenschatz – Arbeitsblätter
1_4 Daten unter Artenschutz

Endnoten

[1] **Heller,** 2013, S. 2.
[2] **Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI),** 2014, S. 118.
[3] **Rössler,** 2001, S. 17; vgl. im Folgenden ebd., S. 16–20.
[4] Vgl. **Boyd**, 2008, S. 27.
[5] Vgl. **GfK Verein,** 2013.
[6] **Barnes,** 2006.
[7] **Haller,** 2013.
[8] **Lobo,** 2014.
[9] Vgl. **Kutscher,** 2013, S. 1.
[10] **Albers,** 2013, S. 124.
[11] **Rössler,** 2001, S. 23.
[12] **Kutscher,** 2013, S. 1, eigene Hervorhebung.
[13] **Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI),** 2014, S. 120.
[14] Vgl. **ebd.,** S. 121.
[15] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 3.
[16] Vgl. **Heuer/Tranberg,** 2013, S. 26.
[17] **Ebd.,** S. 127.
[18] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 99ff.
[19] Vgl. **Heuer/Tranberg,** 2013, S. 101.
[20] **Ebd.**
[21] Vgl. **Olejnik/Castelluccia/Janc,** 2012.
[22] Vgl. **Heuer/Tranberg,** 2013, S. 120.
[23] **Kluemper/Rosen/Mossholder,** 2012, S. 1143–1172.
[24] **Landesanstalt für Medien Nordrhein-Westfalen (LfM),** 2014.
[25] **Zit. nach Döpfner,** 2014.
[26] **Gemeinsam mit Jared Cohen,** 2013.
[27] Vgl. **Mill,** 2010/1859.
[28] Vgl. **Assheuer,** 2013.
[29] Vgl. **van den Hoven,** 2010, S. 319.
[30] **Zit. nach Maier,** 2014.
[31] **Döpfner,** 2014.
[32] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 242.
[33] **Filipović,** 2014.
[34] Vgl. **hierzu insbesondere Rössler,** 2001.
[35] **Hierzu zählen etwa Nissenbaum** (2010)**, van den Hoven** (2008, S. 302) **und Nagenborg** (2005, S. 65–72).
[36] **Rössler,** 2001, S. 218.
[37] **Kant,** 1999/1786, S. 61.
[38] Die EU-Datenschutzgrundverordnung kommt seit 25. Mai 2018 zur Anwendung.
[39] Vgl. **Europäische Kommission,** 2012.
[40] Vgl. **European Group on Ethics in Science and New Technologies to the European Commission (EGE),** 2014, S. 158.

Methodisch-didaktische Hinweise – Übersicht über die Projekte

Mittlerer Schwierigkeitsgrad (ab 14 Jahren)

Projekt	Titel	Kompetenzen	Methoden	Material	Zeit	Zugang Internet/PC
1	**Privatsphäre – wozu?**	Die SuS* können den Wert der Privatheit erkennen und Folgen für die Verletzung der Privatsphäre formulieren.	Skala, Szenario-Methode „Was wäre wenn …", Kopiervorlage „Gesetzlicher Schutz …" der Privatsphäre	Kärtchen (3 pro SuS)	45 min	Nein (evtl. Beispiel Stasi zeigen)
2	**Sag mir, was du kaufst, und ich sag dir, wer du bist.**	Die SuS erkennen Kunden-Profiling-Strategien der Konsumindustrie.	Black Story, Partnergespräch	Film „Verräterischer Kassenbon"	45 min	Nein (Film zeigen)
3	**Big Data – Big problem?**	Die SuS können die Chancen und Risiken von Big Data erkennen.	Rollenspiel, Mindmap	Trailer „Data Dealer", Filme zu „Big Data" zur Verfügung stellen, Rollenkärtchen kopieren, Zusatz-ABs „Internet der Dinge" und „Überwachung" auf www.klicksafe.de/medienethik	60 min	Nein (Videos verfügbar wmachen)
4	**Wie soll ich mich entscheiden?**	Die SuS lernen, sich mit schwierigen Situationen auseinanderzusetzen und auf Grundlage ihrer Wertvorstellungen Entscheidungen zu treffen.	Wertediskussion	Kärtchen, Dilemma-Beispiele ausschneiden	45 min	Nein
5	**Aktiv werden!**	Die SuS lernen Handlungsoptionen zum Schutz digitaler Grundrechte kennen.	Gruppenarbeit	Aufgabenkärtchen, Hilfskärtchen	60 min	Ja (für alle Gruppen)

* Die Abkürzung SuS steht für Schüler und Schülerinnen.

Auf www.klicksafe.de/medienethik finden Sie Zusatz-Projekte zu diesem Baustein.

Beschreibung zu Projekt 1: Privatsphäre – wozu?

Kompetenzen	**Die SuS können den Wert der Privatheit erkennen und Folgen für die Verletzung der Privatsphäre formulieren.**
Zeit	45 Minuten
Methoden	Skala, Szenario-Methode „Was wäre wenn …“, Kopiervorlage „Gesetzlicher Schutz der Privatsphäre“ auf ⓘ **www.klicksafe.de/medienethik**
Material	Post-its (3 pro SuS)
Zugang Internet/PC	Nein (evtl. Beispiel Stasi zeigen)
Einstieg	Zeigen Sie etwas „Privates“ (z. B. Ihre Geldbörse) oder etwas provokanter: Verlangen Sie das Smartphone eines/r Schülers/in sowie den Zugangscode. „Warum würdet ihr das z. B. nicht an einen Fremden weitergeben?“ – Das ist problematisch, weil es „privat“ ist, also Informationen enthält, die man selbst kontrollieren und schützen möchte. **Im Sitzkreis:** Die SuS schreiben jeweils auf 3 Post-its, was für sie privat ist. Die Beispiele können aus allen Bereichen des Lebens stammen. Bereiten Sie Post-its mit interessanten Beispielen vor, falls die SuS Probleme haben, Privates zu formulieren (z. B. sexuelle Orientierung, Kontonummer). Lassen Sie einige Beispiele der SuS nennen, die anschließend auf einer Fußboden- oder Tafel-Skala zwischen 1–10 eingeordnet werden (Grad der Privatheit: 1= am wenigsten privat, 10 = sehr privat). So können besonders private Situationen von der Klasse bestimmt und diskutiert werden. **Auswertungsfragen:** Wie viel Digitales wird (im Gesamtverhältnis) genannt? Was hätten wohl eure Großeltern aufgeschrieben?  Beispiel für Skala der Privatheit. Quelle: klicksafe, eigenes Bild
Erarbeitung	**Was wäre, wenn Privates öffentlich wäre?** Die Folgen von Verletzungen der Privatsphäre werden mit der Szenario-Methode erarbeitet. Die Übung kann als Partnerübung an den Tischen durchgeführt werden oder – falls Sie im Sitzkreis bleiben wollen – formulieren die SuS im Sitzkreis mögliche Szenarios für das eigene Beispiel. **Szenario-Methode:** *Was wäre, wenn…* diese Dinge, die die SuS in der Einstiegsübung als sehr privat eingeordnet haben, nicht mehr privat, sondern öffentlich wären? Die SuS formulieren mögliche Folgen: *„Wenn dein Tagebuch für alle zu lesen wäre, dann wüssten alle deine intimsten Dinge, deine Geheimnisse und könnten dieses Wissen gegen dich verwenden.“* Die möglichen negativen Folgen wie z. B. Ausschluss, Mobbing, Bloßstellen, Erpressung können ausformuliert werden. Kennen die SuS weitere Beispiele für Verletzungen der Privatsphäre? Wozu ist also im Umkehrschluss die Privatsphäre gut? Die **Funktionen** der Privatsphäre können herausgearbeitet werden: Schutz, Autonomie, Selbstbestimmtheit (vgl. Sachinformationen Kapitel 1.2 Formen und Funktionen).
Sicherung	Machen Sie deutlich, dass in Deutschland die Privatsphäre vom Gesetzgeber her geschützt wird, u. a. durch das „Recht auf Informationelle Selbstbestimmung“ (AB „Gesetzlicher Schutz der Privatsphäre“ zum Download auf ⓘ **www.klicksafe.de/medienethik**). Dies war nicht zu allen Zeiten so. Ein eindrucksvolles Beispiel für Verletzungen der Privatsphäre durch die Stasi ist ein Bericht über eine Hausdurchsuchung, die Sie den SuS zum Abschluss zeigen können: ⓘ **http://bit.ly/1uowIMY.** **Zusatzaufgabe/Hausaufgabe:** *„Ich habe doch nichts zu verbergen!“*. Warum ist diese Aussage ein gefährlicher Irrtum? siehe Sachinformationen 1.3 Privacy-Paradox oder ⓘ **www.datenschutzbeauftragter-online.de/datenschutz-antrittsvorlesung-michael-schmidl-informationelle-selbstbestimmung-theorie-praxis/5594/** Kapitel I. Bedeutung der Informationellen Selbstbestimmung

Beschreibung zu Projekt 2: Sag mir, was du kaufst, und ich sag dir, wer du bist.

Kompetenzen	**Die SuS erkennen Kunden-Profiling-Strategien der Konsumindustrie.**
Zeit	45 Minuten
Methoden	Black Story, Partnergespräch
Material	Film „Verräterischer Kassenbon“
Zugang Internet/PC	Nein (Film zeigen)
Einstieg	Erzählen Sie das folgende Rätsel, das dem Kartenspiel „Black Stories“ nachempfunden ist, und wecken damit die Neugier der SuS auf die Geschichte: *„Warum hast du mir nicht gesagt, dass du schwanger bist?“*, will ein Vater von seiner Tochter wissen. Wie hat er das erfahren? **Methode „Black Story“:** Eine zumeist skurrile Ausgangssituation wird beschrieben. Durch Fragen der SuS, die Sie nur mit Ja oder Nein beantworten dürfen, versuchen die SuS die Geschichte zu rekonstruieren, die hinter der beschriebenen Situation steckt. **Lösung:** Zeigen Sie den Film „Verräterischer Kassenbon“ aus der Sendereihe Quarks & Co und lösen damit das Rätsel auf: **http://bit.ly/13CCi2T** Ein amerikanischer Vater beschwert sich bei einem Kaufhaus (Target) über Gutscheine für Schwangerschaftsartikel/Babyartikel, die seine 16-jährige Tochter geschickt bekommen hatte, ohne zu diesem Zeitpunkt zu wissen, dass sie tatsächlich schwanger war. Die Firma hatte dies bereits anhand der Konsumgewohnheiten der Tochter ermittelt.
Erarbeitung	**Aufgabe 1:** Was genau kann man über Menschen anhand ihres Einkaufverhaltens herausfinden? Die SuS bearbeiten das Arbeitsblatt und beschreiben die vermuteten Konsumenten anhand ihrer Einkäufe. Machen Sie ein Beispiel zu Person 1: *Ist krank, wahrscheinlich Magen- Darmerkrankung, weiblich, zwischen 17 und 23, sehr modeinteressiert.* Die SuS lesen einige Profile vor. **TIPP**: Die SuS können einen eigenen Einkauf erstellen und die Klassenkameraden erraten die Person, die ihn tätigt, sowie deren Hintergründe. **Sammlung im Plenum:** **Wie** können Firmen noch mehr über die Personen herausfinden? Erfassung und Analyse von Kaufverhalten über Rabattkarten (z. B. Payback) sowie Gewinnspiele oder Meinungsumfragen, Auswertung von Videoüberwachung in Verkaufsräumen, Tracking von RFID-Chips auf Produkten oder in Einkaufswagen, Speichern von Bank-Transaktionen, Auskunfteien, Schufa-Abfragen. **Weshalb** machen Firmen das? Kundenbindung, Handel mit Kundendaten, personalisierte Werbung, Grundlage für Scoring-Verfahren (Erfassen und Bewerten der Zahlungsmodalitäten/ Aufschluss über die Zahlungsmoral), Optimierung von Unternehmensabläufen.
Sicherung	**Aufgabe 2:** Wie kann man sich vor Kundenprofilbildung schützen? Keine Kundenkarten wie Payback nutzen, keine Bonusprogramme, nicht „nur“ online einkaufen, verschiedene Anbieter nutzen, Anti-Tracking Add-ons für den Webbrowser nutzen, wie z. B. Ghostery, Adblock, Trackerblock. **Zusatzaufgabe/Hausaufgabe:** Was können Firmen über die SuS selbst herausfinden? Beachtet werden soll hier vor allem die personalisierte Werbung. Die SuS sollen die gleiche Google-Suchanfrage auf unterschiedlichen Geräten (z. B. auf ihren Smartphones) durchführen und die unterschiedliche Werbung, die sie wahrscheinlich erhalten, miteinander vergleichen. Welche Werbung erhalten sie auch sonst noch, z. B. über Facebook? Ist diese auf sie zugeschnitten? **Filmtipp:** Mobile Payment – Die Zukunft des Einkaufens (LfM): **http://bit.ly/102ok8j** Broschüre: **www.lfm-nrw.de/fileadmin/lfm-nrw/nrw_digital/DK_Mobile_Payment.pdf** Film „Der gläserne Deutsche“: **https://archive.org/details/Der_glaeserne_Deutsche**

Sag mir, was du kaufst, und ich sag dir, wer du bist!

*Lebensmittel, Kleidung, Pflegeprodukte, Zeitschriften, Bücher, Spiele, Deko, Sportsachen – über deine Einkäufe kann man dich kennenlernen. Wenn man dein Konsumverhalten über eine gewisse Zeit beobachtet, kann man herausfinden, ob du alt oder jung, reich oder arm, gesund oder krank, schwanger oder nicht schwanger bist. Dein Verhalten zu beobachten, zu bewerten und zu vergleichen nennt man **Tracking** und **Scoring**.*

Aufgabe 1:
Auch kleine Einkäufe sagen etwas aus. Was kannst du über die Person anhand ihrer Konsumgewohnheiten herausfinden?
Schreibe auf, wer den Einkauf jeweils getätigt haben könnte und in welcher Situation sich die Person gerade befindet:

Person 1:
Einkauf im Supermarkt
Fencheltee, Salzstangen, Zwieback, DVD-Box „Twilight", Vogue
Beschreibung:

Person 2:
Warenkorb Webseite Planet Sport
Bermuda Shorts, Bikini Oberteil, Surfboard
Beschreibung:

Person 3:
Zalando Warenkorb
Pumps, Kleid, Handtasche, Haarschmuck
Beschreibung:

Person 4:
Einkauf im Supermarkt
Zero-Cola, Blu-Ray „Marvel's The Avengers", Axe Deospray, Durex Kondome
Beschreibung:

Person 5:
Rechnung Baumarkt
Stemmeisen, Stoffhandschuhe, Glasschneider, schwarze Arbeitshosen
Beschreibung:

Person 6:
Amazon Bücherliste
„Backpacker-Tipps fürs Überleben ohne Geld", „Und was kommt nach der Schule?", „TOP 50 Partystädte der Welt", „Die Welt umsonst"
Beschreibung:

Person 7:
Google Play Store
Taschenlampe-App, Die besten 10 Witze, Subway Surfer, Whats-APP, facebook, Bundesliga APP
Beschreibung:

Person 8:
App Store
Dr. Schiwagos Gedächtnis-training, Blutdruckmess-App, Busfahrplan-App, die besten Strickmuster-App, Tierfutterliefe-rung nach Hause-App
Beschreibung:

Person 9:

Aufgabe 2: Durch Onlinekäufe und Kundenkarten können Firmen deine Konsumgewohnheiten gut nachverfolgen und beurteilen. Wie schaffst du es, dich vor dieser Art der Profilbildung zu schützen? ***Sammle Ideen*** mit deinem/deiner Tischnachbarn/Tischnachbarin und stellt sie der Klasse vor.

Zum Nachdenken: *If you are not paying for something, you are not the customer. You are the product being sold.*
Andrew Lewis

Beschreibung zu Projekt 3: Big Data – Big problem?

(ab 16 Jahren)

Kompetenzen	**Die SuS können die Chancen und Risiken von Big Data erkennen.**
Zeit	60 Minuten
Methoden	Rollenspiel, Mindmap
Material	Trailer „Data Dealer", Filme zu „Big Data" zur Verfügung stellen, Rollenkärtchen kopieren, Zusatz-ABs „Internet der Dinge" und „Überwachung" auf ⓘ **www.klicksafe.de/medienethik**
Zugang Internet/PC	Nein (Videos verfügbar machen)
Einstieg	Zeigen Sie den Trailer zum Online-Spiel „Data Dealer" bis ca. 1:32 min (http://datadealer.com/de/). Das Spiel ist eine kritische Auseinandersetzung mit den Themen Datenhandel und Datenmissbrauch. Die SuS sollen nun in die Rollen eines Data-Dealers sowie möglicher Kunden (z. B. Vertreter einer Bank) schlüpfen. Teilen Sie dazu Ihre Gruppe in Kleingruppen à 5 SuS. Auf einen Data-Dealer kommen dann im Schnitt vier Kunden. Die Rollen werden durch die Rollenkärtchen (Data-Dealer, Bank, Online-Kaufhaus, Krankenversicherung, Überwachungsstaat) verdeutlicht. Der Data-Dealer befragt die Kunden, welche Informationen für sie von Interesse sind und notiert sich die Nennungen. Diese werden später in der Gesamtgruppe von den Data-Dealern vorgestellt. Der Wert der einzelnen Daten kann gerankt werden (*„Welche Information ist möglicherweise wertvoller als eine andere?"*).

Mögliche Ergebnisse:

Bank	Online-Kaufhaus	Kranken-versicherung	Überwachungsstaat
Schulden, Vermögen, Beruf, Alter, Gehalt	Interessen/Vorlieben, Konsumgewohnheiten, Zahlungsverhalten/Moral (schnelles oder langsames Begleichen von Rechnungen), Alter, Lifestyle, Musikgeschmack	Ernährungsverhalten, Gewicht, Krankheiten, Hobbys, Familie, Alkoholkonsum, sexuelle Orientierung, DNA-Profil	Politische Einstellung, Vermögen, Kommunikationsverhalten, Freundeskreis, Bewegungsprofil

TIPP: Die SuS können die Demoversion des Online-Spiels „Data Dealer" z. B. in einer Vertretungsstunde ⓘ **http://demo.datadealer.net/** spielen.

Erarbeitung

Die SuS haben spielerisch kennen gelernt welche Daten von Interesse sind. Was mit der Flut an Informationen („Big Data") heute und in Zukunft getan werden kann, soll in einem nächsten Schritt anhand der Aufgabe 1 erarbeitet werden. Die SuS finden sich erneut in den Gruppen vom Einstieg zusammen und sehen sich verschiedene Filme zum Thema „Big Data" an. Sie können auch einen der Filme (z. B. das Video „Big Data – Revolution in allen Lebensbereichen" des Schülers Mats) frontal zeigen. Aufgabe: *„Sammelt in der Mindmap auf dem Arbeitsblatt, was heute alles mit Big Data möglich ist. Die Aspekte sollen in einem nächsten Schritt (eher) als Chance oder als Risiko gekennzeichnet werden (mit +/- oder grüner/roter Farbe)."*

Weitere Videos zum Thema Big Data:

1. „Big Data – Revolution in allen Lebensbereichen" ⓘ **http://bit.ly/1wZwPzn**
2. „Big Data" (LfM) ⓘ **http://bit.ly/1dALYhd** Begleitbroschüre zum Film: ⓘ **www.lfm-nrw.de/fileadmin/lfm-nrw/nrw_digital/Publikationen/DK_Big_Data.pdf**
3. „Big Data einfach erklärt" (Telekom) ⓘ **http://bit.ly/1x2iP6o**

1_2 Datenschutz – Arbeitsblätter
methodisch-didaktische Hinweise

Erarbeitung	Mögliche Lösung: **Chancen:** Auf den einzelnen Nutzer zugeschnittene Medien- und Konsumwelt (Suchmaschinen, Nachrichtenseiten, Online-Shops), neue Geschäftsmodelle, neue Analysewerkzeuge für den Verkehr (Vermeidung von Staus und Unfällen), genauere Erkenntnisse (Partnervermittlung, Schule), Unternehmen können transparenter und effizienter arbeiten, neue Arbeitsplätze, Maßnahmen gegen Armut und Krankheiten (Verbreitungswege von Erkrankungen erkennen, z.B.: Google Flu Trends), Wahrscheinlichkeiten für Straftaten werden errechnet (Predictive Policing) – Erhöhung der Sicherheit **Risiken:** Verdächtigung/Verhaftung aufgrund von Vorhersagen, nicht aufgrund einer Tat, Kreditwürdigkeit wird errechnet, unterschiedliche Preise/Rabatte (Dynamic Pricing), Überwachung (umfassendes Wissen über uns), Kostenerhöhung (Versicherungen), Mensch ist Kunde, nicht Bürger, keine Chance auf Vergessen (Jugendsünden), Manipulation („Effektive Kundenansprache“)
Sicherung	Die Ergebnisse aus den Arbeitsgruppen werden an der Tafel in einer gemeinsamen Mindmap gesammelt und besprochen.

Quellen:
- **www.spiegel.de/netzwelt/web/das-internet-der-dinge-erzeugt-2-8-zettabyte-daten-a-872280.html,**
- **https://blog.telekomcloud.com/ist-eigentlich-big-data/**

Du bist als Data-Dealer ein Einsteiger und triffst heute zum ersten Mal mögliche Kunden.

- **Finde heraus, welche Daten du an einzelne Kunden verkaufen kannst.**
- **Sammle bei deinen Kunden die Daten, die du brauchst.**

Bank	Online-Kaufhaus	Krankenversicherung	Überwachungsstaat

Dir gehört die Bank. Du möchtest möglichst viel verdienen und wenig schlechte Geschäfte machen.

- **Welches Wissen über deine Kunden würde dir dabei helfen?**

Als großer Krankenversicherer brauchst du viele gesunde Mitglieder, damit du mit Gewinn wirtschaften kannst.

- **Welche Infos über mögliche Kunden würden dir helfen, Gewinn zu machen?**

Du bist Alleinherrscher in einem Staat. Das soll auch so bleiben.

- **Welche Informationen über die Bürger deines Landes kannst du brauchen, um deine Macht zu erhalten?**

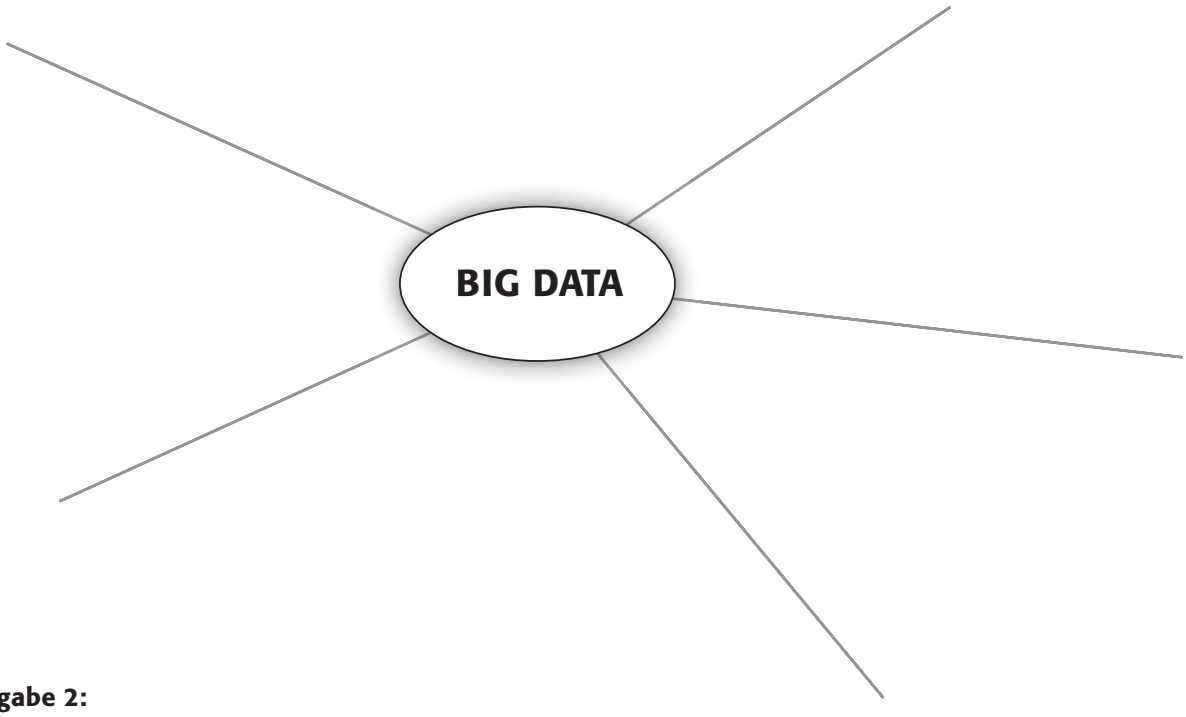
Du bist kurz davor, mit deinem Online-Kaufhaus den weltweiten Markt zu beherrschen. Um Marktführer zu werden, möchtest du noch zielgenauere Werbung schalten.

- **Welche Daten benötigst du hierfür?**

Big Data – kaum vorstellbar…

Big Data steht als Sammelbegriff für riesige Datenmengen und für die Datenanalyse und Auswertung auf der Grundlage gewaltiger Speicherkapazitäten.
Schätzungen gehen für das Jahr 2020 von bis zu 40 Zettabyte Big Data aus.
***Zum Verständnis:** Ein Zettabyte ist eine Zahl mit 21 Nullen! 40 Zettabyte entsprechen laut Wissenschaftlern 57 mal der Menge an Sandkörnern aller Strände der Erde!*

Aufgabe 1:
Wozu soll Big Data heute und in Zukunft verwendet werden? Sammelt in einer Mindmap.



Aufgabe 2:
Markiert, was davon positiv ist (+), was davon negativ (-)?

***TIPP:** Das Online-Spiel **„Data Dealer"** beschäftigt sich mit Datenhandel. Daten sind Macht und Geld. Dein Ziel ist es, möglichst viele Informationen über Menschen zu erhalten, die du dann weiterverkaufen kannst.*
Werde selbst Data-Dealer!
Hier kannst du es spielen: **http://demo.datadealer.net/**



Quelle: © datadealer.net CC-BY-SA 3.0

Beschreibung zu Projekt 4: Wie soll ich mich entscheiden?

Kompetenzen	**Die SuS lernen, sich mit schwierigen Situationen auseinanderzusetzen und auf Grundlage ihrer Wertvorstellungen Entscheidungen zu treffen.**
Zeit	45 Minuten
Methoden	Wertediskussion
Material	Kärtchen, Dilemma-Beispiele ausschneiden
Zugang Internet/PC	Nein
Einstieg	In einem *Sitzkreis* schreiben die SuS auf 3 Kärtchen die 3 für sie wichtigsten Werte (z. B. Familie, Frieden, Gesundheit, Ehrlichkeit etc.). *Sammlung* an der Tafel (Strichliste) oder mit dem Programm **www.wordle.net.** *Auswertung:* Welche 3 Werte sind für die Klasse am wichtigsten? Was sagt das über die Klasse aus? **Hinweis:** Je nach Wissensstand der SuS klären Sie vor der Übung, was ein „Wert" ist und wozu Werte da sind. Werte können als häufig unbewusste Orientierungsstandards und Leitvorstellungen bezeichnet werden. Sie können auch die Übersicht „Wertefelder" aus der Einleitung verwenden.
Erarbeitung	**Wie würden sich Ihre SuS entscheiden?** Die Dilemma-Beispiele dienen dazu, den SuS Denkanstöße zu geben, über Fragestellungen nachzudenken, bei denen es kein einfaches und auch kein eindeutiges Ja oder Nein als Antwort gibt. Sie können eine eigene Stunde mit ausgewählten Entscheidungs-Situationen durchführen oder sie am Ende einiger Arbeitsblätter als wiederkehrende Methode einsetzen. **https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-Polizei-arbeitet-verstaerkt-wie-ein-Geheimdienst-4008214.html** **https://www.sueddeutsche.de/thema/360%C2%B0_Predictive_Policing** **https://www.sueddeutsche.de/digital/polizei-software-zur-vorhersage-von-verbrechen-gesucht-einbrecher-der-zukunft-1.2115086** **Methode „Entscheidungsfindung":** 1. Ein Beispiel wird ausgeteilt oder vorgelesen. 2. Probeabstimmung: Was soll die Person tun? Die SuS stimmen per Handzeichen ab. 3. Begründungen finden für die Entscheidung im Plenum. Die Argumente werden stichwortartig auf der Tafel festgehalten. 4. Analyse der Argumente im Bezug auf Werte (siehe Wertsammlung): Welche Werte stecken hinter den Argumenten? Welche Werte werden hier außer Acht gelassen? Welche Werte kollidieren miteinander? Welche Werte beeinflussen unsere Entscheidungen? 5. Schlussdiskussion: Die Ausgangsfrage wird nochmals zur Abstimmung gestellt. Es wird sichtbar, ob und wie sich Meinungen verändert haben und welche Begründungen überzeugend sind. Wichtig ist auch zu thematisieren, welche Konsequenzen oder Konflikte die jeweilige Entscheidung mit sich bringt. Am Ende der Übung kann auch diskutiert werden, ob man aus der Dilemma-Situation herauskommen könnte. Quelle: Methode modifiziert nach Gugel, Günther; Didaktisches Handbuch, Werte vermitteln – Werte leben; Berghof Foundation
Sicherung	**Auswertung:** Welche Entscheidungen waren für die SuS am schwierigsten? Warum? **Zusatzaufgabe/Hausaufgabe:** Die SuS können eigene Entscheidungs-Situationen entwerfen und diese der Klasse vorstellen. **So entwirft man ein Werte-Dilemma:** Liegt eine Zwangslage/Zwickmühle vor? Lassen sich keine leichten Auswege aus der Zwangslage/Zwickmühle finden? Ist die Geschichte kurz und verständlich dargestellt (max. eine halbe Seite)? Wird Neugier, Empathie und Spannung ausgelöst? Haben die beteiligten Personen Namen? Quelle: Günther Gugel: Didaktisches Handbuch, Werte vermitteln – Werte leben, S.83 **TIPP:** Kartenspiel zum Entscheidungslernen **http://www.bpb.de/shop/lernen/spiele/34263/jetzt-mal-ehrlich**

Wie soll ich mich entscheiden?

Konflikt: Privates in der Öffentlichkeit

Tim und Lisa sind seit zwei Monaten ein Paar. Um ihm ihre Liebe öffentlich zu zeigen, hat Lisa Tim eine Foto-Diashow geschnitten und auf sein Facebook-Profil gepostet. Die schönsten gemeinsamen Momente, Ausflüge und Kuschelsessions sind auf den Bildern festgehalten. Schon viele Freunde haben den Film kommentiert und geliked. Tim ist hin- und hergerissen. Er findet es einerseits sehr süß, andererseits ist es ihm viel zu privat.

Soll er die Diashow löschen?

Konflikt: Data Deals

Lina hat einen neuen Online-Shop entdeckt, der Einzelstücke von bekannten Modehäusern stark reduziert anbietet. Für einen Schulball will sie sich ein tolles neues Kleid kaufen. Allerdings gibt es im Internet schlechte Kritiken über den Shop zu lesen (Datenpannen, Hacking usw.). Beim letzten Schritt der Onlinebestellung muss Lina einige Daten eingeben, darunter ihre Bankkontodaten. Ihre Mutter hat sie ausdrücklich vor der Weitergabe solcher Daten gewarnt und sie gebeten, immer auf Rechnung zu bestellen. Dies ist aber nicht möglich.

Soll Lina die Daten eingeben?

Konflikt: Gierige Apps

Eine neue Messenger-App ist auf dem Markt und total angesagt. Allerdings nimmt sie Zugriff auf das Telefonbuch des Handys, den Bildspeicher, das Mailpostfach und die Verbindungsdaten, wenn man telefoniert. Joel weiß das eigentlich und sein Vater hat ihn schon vor solchen Diensten gewarnt, die es darauf angelegt haben, möglichst viele Daten zu sammeln. Aber alle Freunde haben diese App.

Soll Joel sie auch auf sein Handy laden?

Wie soll ich mich entscheiden?

Konflikt: Big Brother fährt mit

Matthias möchte sich ein neues Auto kaufen. Beim Autohändler erfährt er, dass er bei der Versicherung viel Geld sparen könnte, wenn er zustimmt eine Blackbox installieren zu lassen. Diese würde sein Fahrverhalten über Funk und GPS aufzeichnen und auswerten, wann, wo, wie schnell, wie oft und wie sicher er unterwegs ist. Die Kosten für Matthias' Traumwagen liegen über seinem Budget, aber durch das Geld, das er spart, wenn er der Black Box zustimmt, könnte er sein Traumauto vielleicht doch finanzieren.

Wie soll Matthias sich entscheiden?

Konflikt: Predictive Policing

In den USA gibt es seit den Anschlägen vom 11. September 2001 ein verschärftes Sicherheitsdenken. So wurde beispielweise ein Programm entwickelt, das aufgrund von Datenanalysen berechnen kann, wann und wo Verbrechen in Zukunft stattfinden. Auch personenbezogene Daten über ehemalige Strafgefangene könnten in solche Programme eingespeist und analysiert werden. Lilly liest dazu einen Artikel und erfährt, dass auch schon solche Programme in Deutschland eingesetzt werden.

Was haltet ihr von der Idee über Voraussagen zu kriminellem Verhalten?

Konflikt: Abmelden oder nicht?

Sonia hat in der Schule einen Vortrag über Datenschutz im Internet gehalten. Seitdem sie sich besser informiert hat, hat sie bei allem, was sie im Internet oder mit dem Smartphone tut, ein ungutes Gefühl. Sie möchte nicht der gläserne Mensch sein, von dem überall berichtet wird. Eigentlich will sie sich nur noch überall abmelden. Aber als sie die Entscheidung trifft, sich endgültig abzumelden, bekommt sie plötzlich doch Zweifel. Immerhin läuft die ganze Kommunikation mit ihrem Freundeskreis über Online-Dienste.

Soll sie sich abmelden?

Beschreibung zu Projekt 5: Aktiv werden!

Kompetenzen	**Die SuS lernen Handlungsoptionen zum Schutz digitaler Grundrechte kennen.**
Zeit	60 Minuten
Methoden	Gruppenarbeit
Material	Aufgabenkärtchen, Hilfskärtchen
Zugang Internet/PC	Ja (für alle Gruppen)
Einstieg	*„Was ihr selbst tun könnt, um zumindest ein bisschen Einfluss darauf zu nehmen was mit euren Daten geschieht, lernt ihr nun in einer Stationenarbeit kennen."* Legen Sie die 4 Aufgabenkärtchen (Selbstdatenschutz, Abgeordnetenwatch, Das Recht auf Informationelle Selbstbestimmung, Privacy by design) auf 4 Tischen aus. Die SuS bewegen sich ca. 3 Minuten im Klassenzimmer, lesen die Stationenaufgaben und setzen sich an den Tisch, an dem sie die Aufgabenstellung besonders interessiert. Es können bei Mehrfachinteresse Stationen auch doppelt vergeben werden (bedenken Sie dies beim Kopieren der Kärtchen). Sie können auch nur ausgewählte Stationen von allen bearbeiten lassen. Sie können die Hilfen/„Vorschläge für die Gruppe..." für die einzelnen Stationen gleich mit austeilen oder erst bei Bedarf. **TIPP:** Die Gruppe Selbstdatenschutz ist auch für jüngere/schwächere SuS geeignet. Die SuS erstellen aus den Tipps eines Schülers aus dem klicksafe-Jugendbeirat eigene Dateien (z. B. Textdatei, Foto, Handyvideo), die sie an andere SuS weiterleiten sollen. **Kriterien:** ▪ Der Inhalt soll gut verständlich sein. ▪ Die Datei soll den Inhalt ansprechend und kreativ vermitteln. ▪ Sie sollte als Teil einer Kampagne zum Thema Datenschutz verwendbar sein. ▪ Die Jugendlichen sollen die Datei in einer angegebenen Zeit fertigstellen. ▪ Bei Verbreitung außerhalb der Schule auf Urheberrechte achten.
Erarbeitung	Die SuS haben 45–60 Minuten Zeit für die Bearbeitung der Aufgabenstellung.
Sicherung	Die SuS berichten nacheinander an ihrem Tisch über ihre Vorgehensweise bzw. präsentieren ihre Ergebnisse.

Gruppe: Selbstdatenschutz

Hier könnt ihr für eure Klasse, eure Freunde, eure Schule Tipps für den Selbstdatenschutz formulieren.

Aufgaben:

1. Wie kann man sich selbst im Internet vor Datensammelwut und Datenklau schützen? Überlegt euch mindestens fünf Tipps für den Selbstdatenschutz.
2. Erstellt aus den Tipps einen Flyer und verteilt ihn bei euch an der Schule (auch digital über eure Schulwebseite oder Soziale Netzwerke). Denkt daran, ihn interessant zu gestalten!

Hier könnt ihr euch Anregungen holen:

http://www.youngdata.de/datenschutz/datenschutz-tipps/

Vorschläge für Gruppe: Selbstdatenschutz

Datenschutztipps:
von Hendrik aus dem klicksafe Youth Panel (Jugendbeirat).

1. Nutze verschlüsselte Messenger (Telegram, Threema). Achte auch bei verschlüsselten Diensten darauf, möglichst einen Nickname als Namen anzugeben (Kommunikation kann einem so nicht zugeordnet werden).
2. Wenn du im Web vorhast, private Daten anzugeben, immer! schauen ob die Website https-verschlüsselt und gültig ist (achte auf grünen Balken in der Adresszeile). Hilfreich kann dazu ein Browser-Add-on wie z. B. „HTTPS Everywhere“ sein.
3. Achte bei Apps darauf, wirklich die offizielle Version der Software zu verwenden. In App-Stores tauchen gerne Klone von Apps auf, denen es (wie bei Phishing) möglich ist, z. B. durch Eingabe deines „SMS-Bestätigungscodes“ deinen Account zu übernehmen.
4. Nutze alternative, sicherere Cloud-Speicher-Lösungen, falls es wirklich nötig ist, wichtige Dokumente/Bilder online zu stellen und mit anderen zu teilen. Zum Beispiel Spideroak (von Edward Snowden empfohlen): Dort kann man verschlüsselt Daten ablegen.
5. Auch wenn du scheinbar sicher unterwegs bist – selbst die beste Verschlüsselung hat Schwächen, also überlege immer genau, was du versendest oder angibst. Auch Snapchat wurde schon gehackt und die Bilder online gestellt.
6. Auch Suchmaschinen wissen viel über dich. Schau dir doch mal eine alternative Suchmaschine, wie Startpage oder Duck Duck Go an, die keine Daten speichern.
7. Streue deine Nutzung, d. h. nutze nicht alle Dienste nur von einem Anbieter. Wenn du beispielsweise Facebook und WhatsApp nutzt, hat Facebook einen Überblick über deine gesamte private Kommunikation.
8. Nutze möglichst nur Dienste, von denen du weißt, dass sie sicher sind oder von denen du schon einmal (positiv) gehört hast (z. B. in den Medien oder von Freunden). Es gibt tausende von Diensten im Internet, die aufgrund ihrer Unbekanntheit von keinem unter die Lupe genommen wurden.

Gruppe: Abgeordnetenwatch

Hier bekommt ihr die Möglichkeit, einmal einem Politiker eine Frage zum Thema Datenschutz zu stellen.

Aufgaben:

1. Recherchiert zu einem aktuellen Datenschutz-Thema, das euch interessiert.
2. Bereitet zwei Fragen zu diesem Thema vor, die ihr an einen Abgeordneten stellen wollt.
3. Stimmt ab, welche der beiden Fragen ihr stellen sollt und tut dies auf der Seite Abgeordnetenwatch, auf der jeder öffentlich einem Bundestags- oder Europaabgeordneten eine Frage stellen kann: **www.abgeordnetenwatch.de/ueber-uns/faq**
4. Auch wenn die Antwort auf sich warten lässt: Bleibt dran und teilt die Antwort des/der Abgeordneten euren Klassenkameraden mit.

Vorschläge für Gruppe: Abgeordnetenwatch

Vorschlag Themen:

- Datenschutz-Grundverordnung (DSGVO)
  https://deinedatendeinerechte.de/
  https://dsgvo-gesetz.de
  https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.pdf?__blob=publicationFile&v=38
- Künstliche Intelligenz (KI) und Automatisierung
- Big Data **https://www.youtube.com/user/alexanderlehmann**

Vorschlag Politiker:

Stellt Fragen an unsere Staatsministerin für Digitalisierung Dorothee Bär:
https://www.abgeordnetenwatch.de/eu/profile

Ihr könntet z. B. Bezug nehmen auf die Veränderung unseres Lebens durch Digitalisierung.

Gruppe: Privacy by design (Art. 25 DSGVO)

Hier könnt ihr Vorschläge für die Verbesserung des Datenschutzbereichs bei Facebook machen.

Aufgabe:

Schaut euch den Datenschutzbereich bei Facebook an: https://www.facebook.com/policy.php
Sammelt schriftlich, was ihr als jugendliche Nutzer gut und was ihr schlecht daran findet. Achtet vor allem auf Verständlichkeit des Textes und Design der Seite. Wie könnte der Bereich bei einer Seite wie Facebook verbessert werden? Ihr dürft auch kreativ werden.

Vielleicht findet ihr Anregung bei den AGB von anderen Diensten.

Gruppe: Das Recht auf informationelle Selbstbestimmung – Praxistest!

Hier könnt ihr bei Facebook, Amazon, Payback oder Google Auskunft über eure Daten einholen.

Aufgaben:

1. Schaut euch an, wie und wo Daten über den Politiker Malte Spitz gesammelt wurden.
   http://bit.ly/1szImxA
2. Macht es wie Malte Spitz! Sucht euch einen Dienst aus, den die meisten von euch kennen oder nutzen und findet heraus, wie ihr Auskunft über eure Daten, die dort gespeichert werden, einholen könnt.
3. Formuliert ein Anschreiben und einen passenden Text.
4. Stellt eine Anfrage und holt euch Auskunft über eure Daten.

Vorschläge für Gruppe: Informationelle Selbstbestimmung

Musterbrief: Auskunftsersuchen und Widerruf der Einwilligung in die Datenweitergabe

Absender
Name
Anschrift
weitere Angabe zur Identifikation, z.B. E-Mail-Adresse, Kundennummer, Geburtsdatum

Unternehmen
Anschrift

Ort, Datum

Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO)

Sehr geehrte Damen und Herren,

ich bitte um Auskunft darüber, ob Sie personenbezogene Daten über meine Person gespeichert haben. Sollte dies der Fall sein, bitte ich um Auskunft darüber,

a) welche personenbezogenen Daten ganz konkret bei Ihnen verarbeitet werden (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde) sowie
b) zu welchem Zweck diese Daten verarbeitet werden.

Darüber hinaus fordere ich Informationen über

c) die Kategorien personenbezogener Daten, die verarbeitet werden,
d) Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
e) die geplante Speicherdauer bzw. die Kriterien für die Festlegung dieser Dauer,
f) das Bestehen eines Rechts auf Berichtigung oder Löschung der Daten oder auf Einschränkung der Verarbeitung,
g) ein ggf. bestehendes Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
h) mein Beschwerderecht bei der zuständigen Aufsichtsbehörde,
i) die Herkunft der Daten.
j) Sollte eine automatisierte Entscheidungsfindung einschließlich Profiling stattfinden bitte ich um aussagekräftige Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.
k) Falls eine Datenübermittlung in Drittländer stattfindet, bitte ich um Informationen, welche Garantien gemäß Art. 46 DSGVO vorgesehen sind.

Bitte stellen Sie mir außerdem kostenfrei eine Kopie meiner bei Ihnen gespeicherten personenbezogenen Daten zur Verfügung.

Mit freundlichen Grüßen
(Unterschrift)

Hinweise zur Nutzung des Musterbriefs:

1. Kopiert den Text in ein Textverarbeitungsprogramm (MS Word, Open Office, etc.).
2. Ergänzt ihn mit euren Absenderangaben, einer Frist (Datum) sowie der Anschrift des Unternehmens, an das der Musterbrief gehen soll.
3. Schickt diesen Brief an das Unternehmen.

Quelle: ©Copyright Verbraucherzentrale www.vzbv.de, Stand: April 2018



1_1 Datenschutz/Big Data
1_2 Datenschutz – Arbeitsblätter
1_3 Datensatz, Datenschatz – Arbeitsblätter
1_4 Daten unter Artenschutz

Sachinformation

Datenschutzgesetze: International, in der EU, in Deutschland

Was Datenschutz bedeutet, wird weltweit unterschiedlich betrachtet. Das Internet kennt im digitalen Zeitalter keine Ländergrenzen, und so ergeben sich schnell Probleme, wenn persönliche Daten häufig durch mehrere Länder wandern. Das **Demo-Tool „Traceroute"** (http://bit.ly/1SnzzxW) macht den internationalen Weg von Daten eindrucksvoll sichtbar. Um die Daten der eigenen Bürger zu schützen, gibt es zwischen Ländern Abkommen wie das **„EU-US Privacy Shield"** (http://bit.ly/2amwkaf). Dieses Abkommen regelt den Austausch zwischen den USA sowie der Schweiz und Europa in Bezug auf Datenverarbeitung.

Bereits Ende 1983 – also lange vor dem Entstehen des kommerziellen Internets in den 1990er-Jahren – hat das deutsche Bundesverfassungsgericht ein **„Recht auf informationelle Selbstbestimmung"** (http://bit.ly/2FTPNi3) aus den Artikeln 1 und 2 des Grundgesetzes abgeleitet. Es spricht jedem Menschen das Recht zu, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, bis auf notwendige, im Gesetz klar geregelte Ausnahmen. „Datenschutz" ist ein relativ neuer Rechtsbegriff aus den 1970er Jahren und findet sich daher nicht im Grundgesetz. Das Bundesland Hessen war Vorreiter, als es das weltweit erste Datenschutzgesetz verabschiedete.

Auf EU-Ebene wird seit Anfang 2016 mit der **„Datenschutz-Grundverordnung"** (http://bit.ly/2Ed2YtN) eine EU-weite Vereinheitlichung der Regeln für die Verarbeitung von personenbezogenen Daten durch Behörden und private Unternehmen geschaffen. Diese muss nun in den einzelnen Mitgliedsstaaten bis zum Ende der Übergangszeit am 25. Mai 2018 umgesetzt werden.

IP-Routing und -Adressen: Möchten sich Geräte in Computernetzwerken verbinden bzw. Daten, auch international, austauschen, müssen sie füreinander erreichbar sein. Ähnlich wie unsere Postadressen bzw. unsere Telefonnummern gibt es dazu im Internet IP-Adressen. Welche IP-Adresse Ihnen gerade von Ihrem Provider zugeordnet ist, können Sie auf einer Seite wie **www.utrace.de** sehen.

Recht an den eigenen Daten

Die Datenschutzgesetze schützen Menschen, indem sie die Verarbeitung ihrer personenbezogenen Daten beschränken. Das sind Daten, die eine Person direkt bestimmen oder durch weitere Informationen bestimmbar machen. Dies kann der eigene Name, ein WhatsApp-Chat oder auch nur die Augenfarbe sein.

Mit dem „Recht auf informationelle Selbstbestimmung" brauchen Dritte in Deutschland immer die Einwilligung des Betroffenen, um seine Daten verarbeiten zu dürfen. Allerdings gibt es gesetzlich geregelte Ausnahmen, z. B. für Steuerbehörden oder Schulen, die personenbezogene Daten verarbeiten müssen, um ihre Aufgaben erfüllen zu können. Dabei ist die Verhältnismäßigkeit (legitimer Zweck, Geeignetheit, Erforderlichkeit, Angemessenheit) zu achten. Werden personenbezogene Daten verarbeitet, hat man immer ein Auskunftsrecht und ein Recht auf Berichtigung, Löschung oder Sperrung dieser Daten, falls sie nicht korrekt erhoben wurden. Das „Recht auf Selbstauskunft" kann jeder Bürger bei staatlichen Behörden oder Firmen geltend machen, über einen **Generator** (https://www.datenschmutz.de/cgi-bin/auskunft) lässt sich leicht ein Auskunftsersuchen erstellen.

Eine einmal erteilte Einwilligung zur Verarbeitung der eigenen Daten kann widerrufen werden oder ist gegebenfalls gar nicht gültig. Insbesondere junge Menschen gelten nicht immer als einwilligungsfähig, da man davon ausgeht, dass sie noch nicht einschätzen können, welche Auswirkungen ihr heutiges Handeln auf ihre Zukunft hat. Aber auch von Erwachsenen erteilte Einwilligungen können unwirksam sein, wenn es keine umfängliche Aufklärung gab. Es reicht beispielsweise nicht, Eltern zu fragen, ob sie damit einverstanden sind, wenn ein Foto ihre Kindes auf der Schulhomepage veröffentlicht wird. Sie müssen vorher darüber aufgeklärt werden, dass einmal ins Internet hochgeladene Inhalte nicht mehr kontrollierbar sind, da viele Kopien angelegt werden können und dort normalerweise dauerhaft verbleiben.

Automatisierte Datenverarbeitung und Big Data

Daten werden heute meist automatisiert verarbeitet, was deren Verfügbarkeit erhöht und ermöglicht, zu verschiedenen Zwecken erhobene Daten einfach zu verknüpfen und damit neue Informationen zu gewinnen. Dies ist nach deutschem Recht unzulässig. Natürlich wäre ein Kreditgeber daran interessiert, den genauen Gesundheitszustand eines Bürgers zu kennen, bevor sein Kredit freigegeben wird. Gesundheitsdaten werden jedoch erhoben, damit Ärzte den Menschen besser behandeln können, und nicht, um anderen damit zu ermöglichen, ihre Geschäftsrisiken zu minimieren.

Auch kann man Daten über Daten sammeln, sogenannte Metadaten, die zusätzliche interessante Rückschlüsse auf Personen ermöglichen. Ein Beispiel sind Verbindungsdaten von Telefonen. Die eigentlichen Gespräche sind unbekannt, aber anhand von Zeiten und Kontakten können viele Rückschlüsse auf den Nutzer gezogen werden.

Data Mining
Falls Sie interessiert, wie solches „Data Mining", also das automatisierte Auswerten großer Datenmengen, funktioniert, und eine Stunde investieren können, schauen Sie sich den **Vortrag** (http://bit.ly/2ErfVn9) eines Fachmannes an. Alternativ können Sie sich einige **Vorratsdaten von Malte Spitz** (http://bit.ly/2GZ3Owd) ansehen, die er bei der Telekom eingeklagt hat.

Datensicherheit durch Verschlüsselung und Signatur

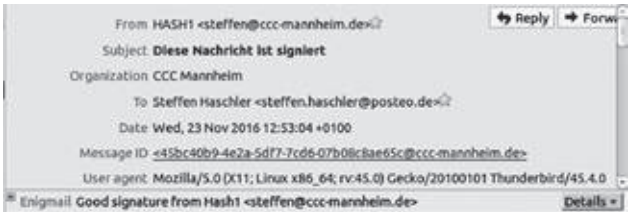
Beim Verarbeiten von Daten muss darauf geachtet werden, dass sie nicht in die Hände Unberechtigter fallen, zerstört oder manipuliert werden. Diese Datensicherheit ist eine technische Voraussetzung dafür, dass Datenschutzgesetze eingehalten werden können.

Analoge Datensätze werden deswegen in Firmen und Behörden oft in Aktenschränken weggeschlossen und an mehreren Orten aufbewahrt. Für das Übertragen der Daten kommen oft besondere Kuriere zum Einsatz. In der digitalen Welt verschlüsselt man die Daten mit kryptografischen Verfahren und legt Sicherheitskopien an.

Mailverschlüsselung und -signatur
Unverschlüsselte E-Mails sind mit Postkarten vergleichbar. Denn anders als Briefe, die durch einen Umschlag geschützt sind, können solche von jedem, der sie in Händen hält, gelesen werden, wie etwa der Postbote, der sie zwangsläufig einmal in der Hand halten wird. Daher sollte man E-Mails verschlüsseln, denn die Verschlüsselung entspricht einem Briefumschlag. Gleichzeitig verhindert die digitale Signatur, dass der Absender gefälscht wird. Sie entspricht der analogen Unterschrift unter dem Brief. Wer seine E-Mails verschlüsseln will, schaut sich diese **Textanleitung** (http://bit.ly/1ar0QJ2) von netzpolitik.org an.

Um die Manipulation von digitalen Daten zu verhindern, verwendet man – ähnlich wie dies Stempel und Unterschriften im Analogen gewährleisten sollen – erneut kryptografische Verfahren. Im Folgenden sehen Sie ein Beispiel für einen solchen digitalen Stempel, auch „Signatur" genannt:

Die E-Mail unten stammt scheinbar von „steffen@ccc-mannheim.de". Sie wurde digital signiert, was ein Programm wie Enigmail erkennt, prüft und verifiziert.



Der Absender ist überprüfbar, da diese Mail eine digitale Unterschrift enthält (Quelle: Steffen Haschler)

Anders ist es bei der folgenden Nachricht:



Sie stammt nicht von unserem Bundesinnenminister, ohne Signatur lässt sich dies kaum feststellen (Quelle: Steffen Haschler)

Hier stammt die Nachricht scheinbar von „thomas.demaiziere@bundestag.de", also vom aktuellen Bundesinnenminister. Da E-Mails immer noch nicht standardmäßig signiert werden, kann man solch eine Fälschung nur schwer erkennen.

Ransomware, Bundestags-Trojaner und weltweite Hacks: Das Zeitalter der Cyberkriege?
Genauso, wie es Einbrüche in Gebäude gibt, werden digitale Speicherplätze angegriffen. Cloudspeicher und Netzwerke von Unternehmen sind aus praktischen Gründen oft weltweit erreichbar. Sie können damit auch von überallher angegriffen werden. Die eingesetzten IT-Systeme weisen fast immer Sicherheitslücken auf oder werden falsch genutzt, sodass viele solcher Angriffe erfolgreich sind. Dabei kann es sich um den Diebstahl von Informationen handeln, wie beim **Bundestag-Hack** im Jahr 2015. Durch eine infizierte E-Mail, die von Abgeordneten geöffnet wurde, verschafften sich die Angreifer Zugang zum Bundestagsnetz und einigen Abgeordnetenkonten.

Die dabei gestohlenen Informationen werden uns gegebenenfalls bei den anstehenden Bundestagswahlen in kompromittierender Form wieder begegnen, ähnlich wie die Veröffentlichungen geheimer E-Mails von Hillary Clinton in der heißen Phase ihres US-Wahlkampfes.

Ein weiteres lohnendes Geschäftsmodell der Hacker ist es, die Daten, auf die sie Zugriff erlangen, als Geisel zu nehmen und Lösegeld zu fordern. Eine solche **Ransomware-Attacke ist WannaCry** (http://bit.ly/2nSMVdK). Mitte 2017 wurden Zehntausende Rechner weltweit infiziert, u. a. auch Rechner der Deutschen Bahn. Die Schadsoftware verschlüsselt dabei Daten, auf die sie Zugriff bekommt, und gibt den Schlüssel zu ihrer Wiederherstellung nur gegen Zahlung einer Geldsumme heraus.

Exploits, die „Brechstangen" des Hackers: Ein modernes Betriebssystem wie Windows besteht aus vielen Millionen Zeilen Code – damit erhöht sich die Wahrscheinlichkeit, dass er Fehler aufweist. Ein Browser alleine besteht schon aus vielen Hunderttausend **Codezeilen.** Manchmal ermöglicht dies, in das System einzubrechen. Es gibt verschiedene Arten solcher Exploits, die ähnlich wie Brechstangen im Analogen dazu verwendet werden, die **Kontrolle über Computer** (http://bit.ly/2sdow8o) zu erlangen. Dabei werden neben bekannten Sicherheitslücken auch Lücken ausgenutzt, die der Allgemeinheit unbekannt sind, jedoch bspw. von **Geheimdiensten** (http://bit.ly/2nP5wZ5) genutzt werden („Zero-Day-Exploits").

Cookies und andere Arten von Tracking
Oft werden sogenannte „Cookies" dazu verwendet, um das Surfverhalten von Nutzern auszuspionieren. Dies nennt man „Tracking". Insbesondere bei kostenfreien Diensten findet es Anwendung. Cookies sind einfache Textdateien, die von Webseiten gelesen und geschrieben werden können. Sie werden dabei lokal im eigenen Browser hinterlegt. Sie gewährleisten, dass eine Webseite einen Besucher wiedererkennt. Das ist praktisch, weil man sich nicht immer wieder neu „ausweisen" muss, indem man sich mit seinem Namen und Passwort erneut einloggt.

Der Nachteil ist, dass viele Seiten Inhalte von Drittanbietern einbinden, z. B. von Google Analytics oder Facebook. Die besuchte Webseite liefert dann nicht nur den eigenen (praktischen) Cookie aus, sondern auch die Cookies dieser anderen Anbieter. Da solche Drittanbieter mit vielen Seiten zusammenarbeiten, erhalten sie so Informationen über fast alle Besuche, die ein Nutzer diversen Seiten abstattet.

Neben Cookies gibt es viele weitere Methoden wie das „digitale Fingerprinting", um einen Nutzer anhand seiner Browsereinstellungen wiederzuerkennen (Einstellungen wie benutztes Betriebssystem, Do-Not-Track-Informationen, die Bildschirmauflösung oder die Wahl bestimmter Adblocker). Die Werbenetzwerke sind hier **kreativ** (http://bit.ly/2BNJbUs). Mit der Vielzahl an Methoden und deren geschickter Kombination ergeben sich detaillierte Nutzerprofile, die dann gehandelt und für das Ausliefern personalisierter Werbung genutzt werden.

Selbstdatenschutz und die Problematik kostenfreier Dienste
Es gibt für den Verbraucher einige Möglichkeiten, sich zu schützen; doch genauso wie im analogen Leben gibt es auch in der digitalen Welt keine Garantien und keine absolute Sicherheit.

- Um Angriffen zu entgehen, sollte man seine Software immer auf dem aktuellsten Stand halten. Leider liefern viele Hersteller die dazu nötigen Sicherheits-Updates („Patches") nur verspätet oder gar nicht aus. Dann bleibt nur der Wechsel zu einem zuverlässigeren Anbieter. Insbesondere bei mobilen Endgeräten ist das ein Problem.
- Man sollte regelmäßig eine Datensicherungskopie („Back-up") der eigenen Daten erstellen, um Datenverlust vorzubeugen. Wenn Sie sich nicht damit auskennen, finden Sie hierzu beim Bundesamt für Sicherheit in der Informationstechnik **ausführliche Informationen** (http://bit.ly/2GXkUKX).

- Die eigenen Daten sollten immer verschlüsselt verschickt und abgelegt werden, damit sie für Fremde nicht direkt lesbar sind. Dies gilt insbesondere dann, wenn man weder den Transportweg noch die Speicherorte genau kennt – und das ist im Internet eigentlich immer der Fall. In dieser Einheit lernen die SuS „Veracrypt" kennen (https://veracrypt.codeplex.com), welches primär für das Ablegen von Daten auf Rechnern und mobilen Speichermedien wie USB-Sticks gedacht ist und auch für Sie als Lehrer interessant sein könnte. Sie können zum Thema Verschlüsselung eine „CryptoParty" in Ihrer (Nachbar-)Stadt besuchen (https://www.cryptoparty.in), um von Experten mehr darüber zu erfahren und sich schließlich selbst besser schützen zu können.

Sicher(er) surfen mit HTTPS:
Mittlerweile haben viele Anbieter im Internet von „http" auf „https" umgestellt. Dies erkennt man am Schloss-Symbol im Browser neben der Adressleiste:



Daten, die mittels „https" ausgetauscht werden, sind verschlüsselt und daher nicht so einfach einsehbar. Dies ist insbesondere von Bedeutung, wenn Passwörter in fremden Netzwerken (Hotel, Café usw.) übertragen werden. Ein schönes **Erklärvideo** (http://bit.ly/2BOIeLm) hierzu hat Alexander Lehmann erstellt. Ist man regelmäßig in fremden Netzen unterwegs, empfiehlt sich der Einsatz eines VPN wie **IPredator** (https://ipredator.se), um gesichert aus dem unbekannten Netzwerk zu kommen.

- Man sollte auf kommerzielle, aber kostenfreie Dienste, z. B. WhatsApp, verzichten, da man durch die Einwilligung zur monetären Nutzung der eigenen Daten immer das Produkt und nicht der Kunde sein wird. Denn die Firmen haben Ausgaben und müssen daher ihren Geldgebern etwas vorlegen. Nutzt man solche Dienste, sollte man sich dieser Problematik zumindest bewusst sein.
- Datensparsamkeit: Es sollten immer nur so viele Daten herausgegeben werden wie unbedingt erforderlich. Dies gilt gegenüber Behörden und Firmen, aber auch gegenüber Fremden in Sozialen Netzwerken.

Datensparsamkeit „Das Internet vergisst nicht"

Problematisieren Sie im Unterricht, dass Daten im Netz, egal ob verschlüsselt oder unverschlüsselt, sich für immer außerhalb der eigenen Kontrolle befinden. Eine heute noch sichere Verschlüsselung wird morgen zu knacken sein; somit sind verschlüsselte Inhalte eher als zeitverzögert lesbar anzusehen.
Sie können diese Problematik mit der **WayBack Machine** (https://archive.org/web) verdeutlichen.

- Als Beispiel können Sie Ihre Schulhomepage oder den Sportverein eines Schülers verwenden und eine kleine Zeitreise unternehmen.
- Verfügen die SuS über eigene Internetzugänge, sollten sie selbst recherchieren.
- Diskutieren Sie die Vor- und Nachteile eines solchen Internetarchives.

Mit diesem Wissen sollte das Prinzip der Datensparsamkeit besser einleuchten. Lassen Sie dazu die SuS bspw. mittels des Merkspruchs „Stop – look – think – post" Überlegungen dazu anstellen, was man beachten sollte, bevor man etwas hochlädt oder veröffentlicht.

Inhalte der Praxisprojekte

Mit den ersten beiden Projekten erarbeiten sich die SuS anhand des Trackings, dass ihre Daten zum einen sensibel sind und zum anderen ausgewertet werden durch Dritte, wenn diese ihre Daten erlangen.

Das dritte und das vierte Projekt zeigen auf, wieso Verschlüsselung notwendig ist und wie man Daten verschlüsselt, Back-ups erstellt und die anfallenden Passwörter organisieren kann.

Ziel der gesamten Einheit ist es, die digitale Mündigkeit der Jugendlichen zu steigern. Es ist denkbar, diese Einheit an einem Projekttag im Ganzen durchzuführen, da sie für vier Einzelstunden konzipiert ist und sich leicht ausdehnen lässt. Es ist zusätzlich denkbar, den Vortrag von **David Kriesel** (http://bit.ly/2C3Pteg) zu schauen oder einen Film wie **„Im Rausch der Daten"** (www.democracy-film.de) bzw. **„Citizenfour"** (https://citizenfourfilm.com) – je nach Altersstufe und Kenntnisstand der SuS.



In der Unterrichtseinheit verwendete Dienste:

- **Traceroute** (www.dnstools.ch/visual-traceroute.html) macht die Wege verschickter Daten im Internet sichtbar. Man gibt eine Zielseite, bspw. „instagram.com", ein. In der Konsole werden die IP-Adressen der Zwischenstationen für diese Anfrage angezeigt. Die ungefähren Standorte dieser Etappen werden auf der Karte ebenfalls sichtbar gemacht.
- **Lightbeam** (als Firefox-Add-on: https://www.mozilla.org/de/lightbeam) zeigt Drittparteien, die ohne Ihr Wissen Ihre Daten sammeln (sog. „Tracking"). Startet man Lightbeam und besucht danach beliebige Internetseiten, so werden Tracker sichtbar. In Lightbeam gibt es einen Reset-Button, der bereits besuchte Seiten mit deren Trackern löscht. Dies ist nützlich, wenn Sie Lightbeam als Demo-Tool mit unterschiedlichen Lerngruppen einsetzen.
- **Self-Destructing Cookies** (als Firefox-Add-on: https://mzl.la/2BKB0rO) löscht verlässlich alle Cookies (kleine Dateien, die Internetseiten im Browser bei Ihrem Besuch ablegen), wenn man einen Tab im Browser schließt. So muss man sich später zwar erneut einloggen, aber man verhindert auch eine Art des Trackings.
- **Startpage** (https://www.startpage.com – auch als Browser-Erweiterung erhältlich) ist eine Suchmaschine, die Ergebnisse von Google ausliefert, jedoch lediglich als „Zwischenstation". So wird verhindert, dass Google Informationen über einen sammelt – denn gerade Suchanfragen können etwas sehr Persönliches sein. Allerdings muss man nun Startpage vertrauen. Da es sich aber um ein europäisches Unternehmen handelt, gilt hier das europäische (Datenschutz-)Recht, und das ist – gegenüber dem US-Konzern Google – ein bedeutender Vorteil.
- **Privacy Badger** (als Firefox-Add-on: https://mzl.la/2EbVzez) schützt vor Tracking, während man surft. Allerdings muss man sich etwas in das Programm einarbeiten.
- **VeraCrypt** (https://archive.codeplex.com/?p=veracrypt) ist eine kostenlose Software, die zudem Open Source ist (d. h. der Code kann von jedem eingesehen werden). Sie verschlüsselt Dateien und Speichermedien. Sie ist ein Nachfolgeprojekt des ggf. bekannteren TrueCrypt, das vor Kurzem eingestellt wurde. VeraCrypt läuft plattformunabhängig auf Linux, Windows und MacOS.
- **KeePassX** (https://www.keepassx.org) ist eine kostenlose Open-Source-Software, die Passwörter verwaltet und verschlüsselt ablegt. Sie läuft plattformunabhängig auf Linux, Windows und MacOS. Es gibt mobile Versionen, wobei man mobilen Endgeräten grundsätzlich misstrauen und sensitive Daten wie Passwortsammlungen dort nicht ablegen sollte.

Übersicht über die Projekte

Projekt	1	2	3	4
Titel	**Datensammeln als Geschäft** (ab 13 Jahren)	**Tracking und personalisierte Werbung** (ab 13 Jahren)	**Selbstdatenschutz durch Verschlüsselung** (ab 14 Jahren)	**Passwort-Management und Back-ups** (ab 14 Jahren)
Ziele	Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt.	Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren. Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können.	Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt.	Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management.
Unterrichtsstunden à 45 min.	1	1–2	1–2	1–2
Methoden und Material	Video, Gespräch, Screenshot/Live-Demonstration: Google Translate, optional: Live-Demonstration Traceroute	Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Live-Demonstration (dazu zunächst das Firefox-Plug-in herunterladen)	Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.codeplex.com), optional: Zip-ordner-Verschlüsselung	Video, Gespräch, Live-Demonstration: KeePass (https://www.keepassx.org/ bzw. https://keepass.info)
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit



Methodisch-didaktische Hinweise zu AB 1: Datensammeln als Geschäft (ab 13 Jahren)

Titel	**Datensammeln als Geschäft**
Ziele	**Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt.**
Unterrichtsstunden à 45 min.	1
Methoden und Material	Video, Gespräch, Screenshot/Live-Demonstration: Google Translate, optional: Live-Demonstration Traceroute
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät – falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren
Einstieg	Stellen Sie den SuS zum Einstieg folgende Fragen: *Habt ihr euch schon mal gefragt, wieso Dienste wie WhatsApp kostenlos sind?* Antwort: Die Betreiber haben hohe Kosten, so müssen sie etwa Entwickler beschäftigen und Rechenzentren bereitstellen, um ihren Dienst anbieten zu können. Als Nutzer bezahlt man kostenlose Dienste meist mit seinen eigenen Daten – wie genau dieses Geschäftsmodell funktioniert, lernen die SuS in dieser Einheit. *Wieso sind eure Daten aber etwas wert? Wir schauen jetzt eine Reportage dazu als Einstieg in unser Thema.* Schauen Sie den 12-minütigen Clip **„Nackt im Netz"** (http://bit.ly/2EO6xYH) des NDR, Beitrag von Panorama. Kurzes Nachbesprechen anhand der Leitfragen auf dem Arbeitsblatt: • *Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?* Datensätze von 3 Mio. Deutschen (ca. 1 von 30 Bürgern ist betroffen → einer in diesem Raum?), lückenlos über 3 Jahre, dauerhaftes Abo für 10.000,– Euro/Monat • *Welche der Personen im Film sind aus deiner Sicht besonders angreifbar und warum?* (bspw. der Richter, der Polizist oder die Politikerin) **Hinweis:** Es kann als Vergleich eine kurze Abstimmung durchgeführt werden, und man lässt je Votum eine Schülerin oder einen Schüler deren Wahl begründen. **Richter:** ist ggf. erpressbar wegen seiner Recherchen zu Sexuellem, insbesondere, wenn er Familie hat **Polizist:** verstößt gegen Datenschutz, riskiert seine Karriere und wird dadurch erpressbar **Verdächtigter:** ist noch nicht verurteilt, ggf. ist er unschuldig, und sein Ruf wird so geschädigt **EU-Abgeordneter:** sein Handeln wird durchschaubar und vorhersagbar, womit man ihn besser beeinflussen oder einschüchtern kann **Politikerin:** es gibt die Möglichkeit, sie bloßzustellen, bspw. im Wahlkampf, aber auch eine Krankenversicherung könnte sich dafür interessieren, dass sie nach Antidepressiva Ausschau hält **gilt für alle:** Falls den oben aufgeführten Personen bewusst ist, dass sie ausspioniert werden, könnten sie sich beobachtet fühlen und sich daher anders verhalten (dieses Phänomen ist im Englischen als „Chilling Effect" bekannt). • *Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?* Es gibt bei uns Datenschutzgesetze; deshalb müssen Menschen bei uns grundsätzlich darüber informiert werden, was mit ihren Daten geschieht. Leider halten sich viele Firmen nicht daran bzw. unsere Gesetze gelten nicht weltweit. Da Daten sich oft durch mehrere Länder bewegen, lässt sich selten garantieren, dass die in Deutschland geltenden Datenschutzgesetze eingehalten werden.

Einstieg



Die Wege von Datenströmen im Internet
Um zu veranschaulichen, welche internationalen Wege Daten im Internet zurücklegen, zeigen Sie **Traceroute** (www.dnstools.ch/visual-traceroute.html) – wenn die SuS selbst Internetzugang haben, können sie diesen Dienst selbst aufrufen.
Download des Screenshots auch auf www.klicksafe.de/klicksafetogo

www.dnstools.ch/visual-traceroute.html mit Domain-Eingabe „instagram.com“ Quelle: Steffen Haschler (Abruf: 8. 6. 2017)

Die SuS sollen nun das Problem einer verräterischen URL (kurz für „Uniform Resource Locator“ – ein Link, unter dem man einen bestimmten Dienst erreicht) – wie im Film (Polizist) gesehen – nachvollziehen.

Gehen Sie dazu auf **Google Translate** (https://translate.google.com) und geben Sie einen beliebigen Text in das Übersetzungsfenster ein.

Falls keine Internetverbindung vorhanden ist, können Sie vorher diesen Screenshot herunterladen unter www.klicksafe.de/klicksafetogo:



Auf dem Screenshot ist die URL in der Adressleiste zu lesen. Sie wird aus der Eingabe bei Google Translate gebildet. Wer diese URL sieht, kennt auch den Text, der zur Übersetzung eingegeben wurde. Manche Add-ons im Browser oder Apps auf mobilen Endgeräten haben Zugriff auf die URLs. Deren Anbieter können diese speichern und verkaufen. URLs sind ein wichtiger Bestandteil der weltweit gehandelten Datensätze.
Die SuS bearbeiten Aufgabe 2, bei der sie in der URL von booking.com markieren sollen, was sie alles über einen Nutzer allein anhand seiner Eingabe in ein Formular erfahren können.

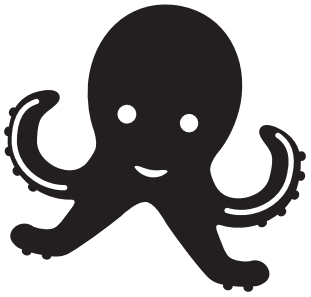
Sicherung

Die Auswertung von Aufgabe 2 erfolgt im Plenum. Informationen über Aufenthaltsort, Reisedaten, Anzahl der Personen und Zimmer können herausgelesen werden.

http://www.booking.com/hotel/ae/**emirates-tower**.en-gb.html?label=gen173nr-1FCAEogg JCAlhYSDNiBW5vcmVmaDuIAQGYAS64AQrIAQzYAQHoAQH4AQuoAgM;sid=a7ab1d928 ff6b9aef4984f9c059b6339;all_sr_blocks=7299609_86367266_2_2_0;**checkin=2016-11-27**; **checkout=2016-11-28**;dest_id=-782831;dest_type=city;dist=0;**group_adults=2**; highlighted_blocks=7299609_86367266_2_2_0;hpos=1;**no_rooms=1**;room1=A%2CA; sb_price_type=total;srfid=8cd932864b73d3ec559a12456221082fa38619a3X1; type=total;ucfs=1&

In dieser Stunde haben die SuS einen Einblick erhalten, wieso Datensammeln lukrativ ist und dass es intransparenten Handel trotz nationaler Gesetze gibt.
Zum eigenen Schutz sollten keine unnötigen Add-ons in ihren Browsern oder Apps auf ihren Geräten installiert sein, da Add-ons und Apps Informationen übertragen können.

AB 1: Datensammeln als Geschäft



Icon made by Freepik from www.flaticon.com

Aufgaben:

1. Beantworte die folgenden Fragen zum Film. Besprecht eure Antworten in der Klasse: Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?

Welche der Personen im Film ist aus deiner Sicht besonders angreifbar und warum? (bspw. der Richter, der Polizist oder die Politikerin)

Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?

2. Was kann man alles aus der folgenden (durch ein booking.com-Formular erzeugten) URL herauslesen? Unterstreiche!

http://www.booking.com/hotel/ae/emirates-tower.en-gb.html?label=gen173nr-1FCAEoggJCAlhYSDNiBW5vcm VmaDuIAQGYAS64AQrIAQzYAQHoAQH4AQuoAgM;sid=a7ab1d928ff6b9aef4984f9c059b6339;all_sr_blocks= 7299609_86367266_2_2_0;checkin=2016-11-27;checkout=2016-11-28;dest_id=-782831;dest_type=city; dist=0;group_adults=2;highlighted_blocks=7299609_86367266_2_2_0;hpos=1;no_rooms=1;room1=A%2CA; sb_price_type=total;srfid=8cd932864b73d3ec559a12456221082fa38619a3X1;type=total;ucfs=1&

Methodisch-didaktische Hinweise zu AB 2: Tracking und personalisierte Werbung

(ab 13 Jahren)

Titel	**Tracking und personalisierte Werbung**
Ziele	**Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren. Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Live-Demonstration (dazu das Firefox-Plug-in vorher herunterladen)
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät – alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit
Einstieg	Zeigen Sie den SuS **diesen Ausschnitt aus dem Hollywood-Film „Minority Report"** (http://bit.ly/2sw8jta). Suche über Suchmaschinen: „Minority report – Mall Scene"

Minority Report
In einer nahen Zukunft werden Mörder mithilfe von Technologien verhaftet, bevor sie ihre Tat begehen können („predictive policing"). Der Hauptdarsteller ist ein Polizist, der solche Verhaftungen durchführt und selbst ins Visier der Fahnder gerät. Da Menschen mittels Augenscannern erkannt werden, muss er sich im Laufe des Filmes einer gefährlichen Augenoperation unterziehen. „predictive policing" wird bereits heute getestet. Mehr dazu finden Sie hier: https://netzpolitik.org/tag/predictive-policing

Was habt ihr in diesem kurzen Ausschnitt beobachtet?

- ggf. den Film und „predictive policing" kurz erläutern
- Die Augen des Protagonisten werde gescannt, er wird persönlich begrüßt („Good evening, John Anderton"), und er erhält individuelle Werbung.

Wie im Filmausschnitt geht es heute um personalisierte Werbung. Habt ihr euch schon einmal gefragt, wieso ihr manchmal Werbung im Internet seht von den Dingen, die ihr euch gerade woanders angeschaut habt oder die euch gerade interessieren? Und dass passende Werbung sogar auf Seiten eingeblendet wird, die ihr vorher nie besucht habt?

- Die SuS sollen von ihren Erfahrungen damit berichten.
- Viele Werbefirmen nutzen das sogenannte „Tracking", um mehr über ihre potenziellen Kunden zu erfahren. Damit können Firmen sie gezielter bewerben. Dies spart Ressourcen und erhöht die Chance, dass eigene Produkt gekauft werden.

Erarbeitung	Um Tracking zu veranschaulichen, nutzen Sie das Firefox-Plug-in „Lightbeam", das sie sich vor der Stunde herunterladen müssen. Es macht Drittanbieter sichtbar, die ihre Inhalte auf Webseiten platzieren, die wir besuchen, und so davon erfahren, dass wir dort waren. Diese Drittanbieter sind oft Firmen, die im Hintergrund unsere Daten sammeln und ggf. verwerten bzw. damit handeln. Wenn Sie die folgende Live-Demonstration nicht durchführen können, verwenden Sie den Screenshot in Anhang 1. Er ist auch auf klicksafe.de/klicksafetogo verfügbar. *Schauen wir uns gemeinsam Lightbeam an, welches aufzeigt, wie das Datensammeln funktioniert. Auf welche Seiten sollen wir gehen?* • z. B.: booking.com, spiegel.de, faz.net, amazon.de, bild.de Hinweis: Nachrichtenseiten verwenden in der Regel viele Tracker und eignen sich daher besonders gut für diese Demo • Es entsteht nach kurzer Zeit ein Bild, wie in Anhang 1 dargestellt. Hinweis: Rufen Sie nicht zu viele Seiten auf, da der Browser schnell langsam wird.

Erarbeitung

Erarbeitung mithilfe von Lightbeam anhand des Screenshots in Anhang 1:

Woher weiß Google, dass wir auf bild.de und booking.com waren?
Hinweis: Wenn Sie nicht bild.de und booking.com besucht haben, wird sich ihr Graph von dem aus Anhang 1 unterscheiden. Sie werden jedoch eine ähnliche Konstellation finden wie mit Google, bild.de und booking.com, die ausgewählt wurden, weil sie viele Verbindungen aufzeigen.

- Wir haben einige Seiten besucht, die in Lightbeam als Kreis (mit Logo) angezeigt werden.
- Diese Webseiten werden von Drittanbietern umgeben, die auf den von uns besuchten Seiten eigene Inhalte anbieten. Viele von ihnen sind sogenannte „Tracker" und verfolgen uns über mehrere Seiten hinweg.
- Die Tracker werden als Dreiecke dargestellt werden und scharen sich um die eigentlich von uns besuchten Webseiten. Ihre Verbindung zu einer von uns besuchten Seite wird durch eine Linie dargestellt.
- Im Screenshot im Anhang erkennt man das Google-Logo zwischen bild.de und booking.com. Daran erkennt man, dass beide Seiten Google-Inhalte nachladen (bspw. Google Analytics, ein Analyse-Tool, das auf sehr vielen Seiten für Nutzeranalysen eingebunden wird). Damit weiß Google aber, welche unterschiedlichen Seiten (hier bild.de und booking.com) der gleiche Nutzer besucht, und diese können so personalisiert werben.

Da der technische Ablauf beim Surfen den SuS wahrscheinlich nicht geläufig ist, folgt zur Vertiefung nun das Rollenspiel (Aufgabe 1 des Arbeitsblatts in Anhang 2). Dafür brauchen Sie 4 SuS („du", „dein Browser", die Seite „booking.com" und die Seite „bild.de").

Jetzt versteht ihr, wieso man personalisierte Werbung angezeigt bekommt.

Optionale Zusatzaufgabe: **Welche Cookies liegen auf meinem Gerät?**
Ermutigen Sie die SuS, auf ihren eigenen Geräten in die Browser-Einstellungen zu gehen und dort nach den hinterlegten Cookies zu schauen. Bei Chrome findet man diese bspw. unter „chrome://settings/cookies". Anhand der Cookies kann man, ähnlich wie anhand der Browser-History, auf das Surfverhalten des Nutzers detailliert rückschließen. Daher sollte man die Cookies nicht vor einer Gruppe aufrufen.

Wie können wir ein solches (rechtlich z. T. unzulässiges) Tracking verhindern?
Die SuS bearbeiten die Aufgabe 2 des Arbeitsblatts zunächst in Einzelarbeit.

Sicherung

Auswertung von Aufgabe 2 im Plenum oder an der Tafel.
Mögliche Lösungen (über Beamer zeigen oder Tipps kopieren und austeilen): siehe Anhang 2

Live-Demonstration mit der Proxy-Suchmaschine Startpage

Bei ausreichend Zeit können Sie für den 6. Punkt auf Startpage (https://www.startpage.com) gehen und demonstrieren, wie man direktes „Googeln" vermeidet.

Geben Sie dort einen Begriff wie „Jogginghose" ein und vergleichen Sie das Suchergebnis mit einer gleichlautenden Anfrage auf Google. Abgesehen davon, dass die Personalisierung wegfällt, sind die Ergebnisse identisch.

Statt dass der Browser Google direkt um Inhalte bittet, fragt man stellvertretend Startpage als „Proxy" an. Ein Proxy ist dabei eine Zwischenstelle, der man vertraut. Sie sucht stellvertretend nach Inhalten im Netz und liefert diese an uns aus. Vergleichbar wäre, im Restaurant nicht direkt beim Koch zu bestellen, sondern beim Ober als Schnittstelle zwischen Kunde und Hersteller.

Der Proxy fragt nun bei Google direkt an und gibt die Inhalte an uns weiter, ohne Google zu verraten, für wen die Inhalte eigentlich sind.

Neues Problem: Jetzt muss man seinem Proxy, hier Startpage, vertrauen!

Zusatzaufgabe oder Hausaufgabe
Pro-und-Kontra-Diskussion „personalisierte Werbung"

Im Folgenden sind je zwei gegensätzliche Aussagen genannt. Lesen Sie diese nacheinander vor und diskutieren Sie mit den SuS, für welche sie sich entscheiden würden.

Weitere Informationen zu den Themen „Datenschutz" und „Filterblase" finden Sie in den Unterrichtsmaterialien „Ethik macht klick" (Baustein 1) sowie im Material „Fakt oder Fake" (Projekt 2) auf www.klicksafe.de/materialien.

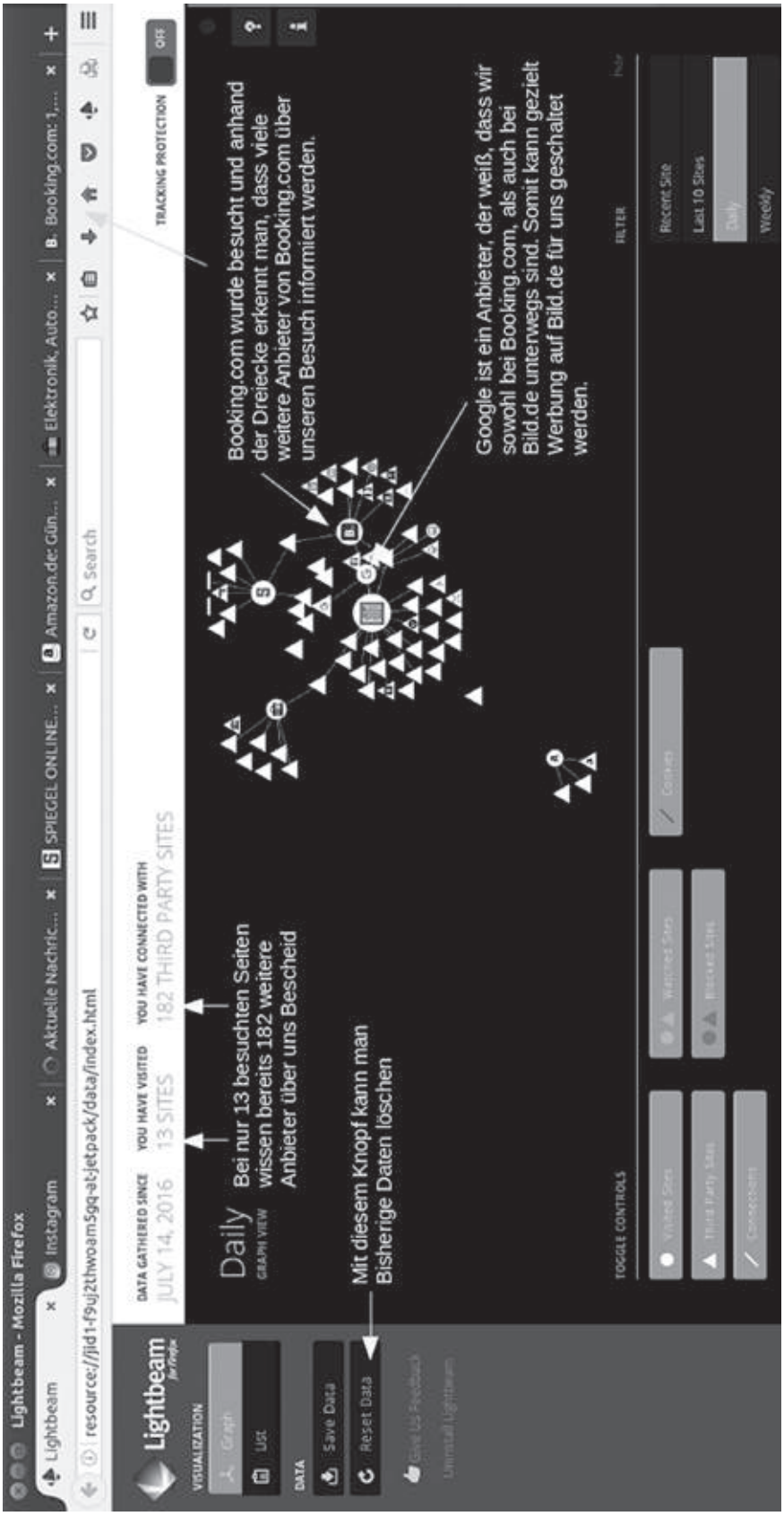
a

- Personalisierte Werbung ist harmlos und hat sogar Vorteile, da man die Dinge sieht, die einen interessieren und Anbieter wie bild.de mehr Geld verdienen können.
- Das Problem bei Werbenetzwerken wie Google ist, dass nach und nach detaillierte Nutzerprofile entstehen, die sehr viel über einen Menschen aussagen, weil Informationen, die einzelne Seiten über uns haben, miteinander verknüpft werden. Firmen wie Versicherer oder Kreditbanken interessieren sich für diese Daten, genauso wie dein zukünftiger Arbeitgeber oder Staaten – sie können dich so besser einschätzen.

b

- Es ist sehr nützlich, wenn man als Golfspieler bei einer Suchmaschinenanfrage zum Thema „Golf“ keine Autos (VW Golf) mehr angezeigt bekommt.
- Dass Ergebnisse im Internet automatisiert personalisiert werden, birgt die Gefahr einer „Filterblase“. Menschen sehen nur noch das, was sie interessieren könnte, und übersehen so andere Dinge. Das kann auch bei der politischen Meinungsbildung negative Auswirkungen haben.

AB 2: Anhang 1 – Screenshot „Wer trackt mich eigentlich?“



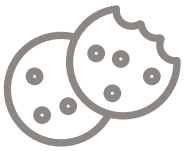
Screenshot, erstellt mit dem Firefox-Add-on „Lightbeam“

AB 2: Anhang 2 – Tipps, wie man Tracking verhindern kann



1. Eine Maßnahme ist, die Cookies für Drittanbieter im Browser zu sperren. Das geht auch auf mobilen Geräten.
   Hinweis: Leider gibt es zahlreiche andere Tracking-Methoden, sodass sich Tracking dadurch nicht ganz verhindern lässt.

2. Bei Firmen wie Apple, Microsoft oder Google gibt es an den Mail-Account gebundene Verläufe, in denen Browser-Eingaben gespeichert werden, bspw. https://myactivity.google.com. Man sollte regelmäßig überprüfen, welche Informationen dort liegen und diese ggf. löschen.

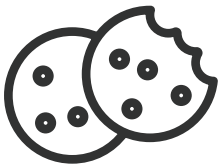


3. In Firefox und Chrome kann man die folgenden zwei Add-ons installieren:
   · https://addons.mozilla.org/de/firefox/addon/self-destructing-cookies/
   · https://addons.mozilla.org/de/firefox/addon/privacy-badger17/

4. Man kann bewusste Produkt- und Kaufentscheidungen treffen, indem man auf Firmen ausweicht, die auf das Auswerten ihrer Kundendaten verzichten bzw. diese nicht an Dritte weitergeben.
   Beispiel: Es gibt datensparsame und werbefreie Mail-Anbieter wie posteo.de oder mailbox.org. (Achtung: Das ist keine Produktempfehlung! In der Vergangenheit haben sich diese beiden Anbieter jedoch positiv hervorgetan.)

5. Es empfiehlt sich, auf seinen Geräten nicht zu viele Apps und Add-ons zu installieren bzw. vorher zu prüfen, welche Berechtigungen diese verlangen.
   Hinweis: Ein regelmäßiger **„Frühjahrsputz"** der eigenen Geräte ist sinnvoll!

6. Für private Suchen (Krankheiten, sexuelle Vorlieben etc.) sollte man eine Proxy-Suchmaschine wie **Startpage** (https://www.startpage.com) oder den **Tor-Browser** (http://bit.ly/2Bjpx1F) verwenden, wobei dieser Browser erst verwendet werden sollte, wenn man sich damit auskennt.



AB 2: Tracking und personalisierte Werbung

Aufgaben:

1. Wie funktioniert Tracking mit Cookies? Ein Rollenspiel für vier Personen.

Du: Hey Browser, ich will mal wieder in den Urlaub. Kannst du mir bitte mal booking.com aufrufen?

Dein Browser: Ja klar, das mache ich sofort! Hey booking.com, mein Meister will Inhalte von dir. Gib mir deine Startseite!

booking.com: Klar, hier hast du die gewünschten Inhalte. Ich binde übrigens externe Inhalte mit ein, bspw. von Google. Kennst du „Google Analytics"? Das ist voll praktisch für meinen Betreiber!

Dein Browser: Nee, kenn ich nicht, und ist mir auch egal. Ich möchte nur das, was mein Meister mir befiehlt. Sag einfach, was ich laden soll, er wird ungeduldig.

booking.com: Ja ja, hier sind deine Inhalte. Ach, übrigens, damit ich dich später wiedererkenne, gebe ich dir diese kleine Textdatei, ein Cookie. Wenn du noch was von mir willst, zeig mir den. So erinnere ich mich an dich, und du musst Formulardaten nicht neu eingeben, oder ich habe vielleicht gerade ein Sonderangebot für deinen Meister, das ihm gefällt.

Dein Browser: Das klingt praktisch, den speichere ich mir ab. Jetzt kann ich meinem Nutzer schneller Inhalte von dir ausliefern, das macht ihn sicher glücklich.

booking.com: Ach, hier sind übrigens noch ein paar Cookies von Anbietern, mit denen ich zusammenarbeite. Sie schalten manchmal Sonderangebote auf anderen Seiten. Damit sie dich ebenfalls wiedererkennen können, habe ich auch von denen Cookies, die ich dir gerne geben würde.

Dein Browser: Klingt sinnvoll, die nehme ich auch, danke. Meister, hier sind die von dir gewünschten Inhalte von booking.com! Was wünschst du jetzt?

Du: Danke, Browser. Jetzt hätte ich gerne, dass du mir die neuesten Nachrichten von dieser „Bild-Zeitung" anzeigst. Die habe ich bisher noch nie angeschaut.

Dein Browser: Wird sofort erledigt! He, bild.de, zeig mal, was es Neues gibt!

bild.de: Klar, gerne doch. Ich binde dir aber Werbung ein, denn damit verdiene ich mein Geld. So kann ich deinem Meister meine Inhalte kostenlos anbieten!

Dein Browser: Das klingt nur fair. Hoffentlich interessiert sich mein Meister für diese Werbung …

bild.de: Aber sicher doch! Kennen wir uns denn schon? Denn dann kann ich dir definitiv passende Werbung einblenden.

Dein Browser: Ich schau mal in meinen Cookies nach … keiner von bild.de. Ich war noch nie bei dir.

bild.de: Wir kennen uns noch nicht, aber ich arbeite unter anderem mit Google zusammen. Die schalten auch Werbung für uns. Vielleicht kennt Google dich? Ah, da ist ein Google-Cookie. Sei unbesorgt: Die Werbung, die dein Meister zu sehen bekommt, wird ihm gefallen. Google kennt ihn bereits (woher auch immer, das weiß ich nicht, und ist mir auch egal) und kann für ihn gezielt Werbung einblenden.

Du: Wow, wie geht das denn? Ich bin noch nie auf bild.de gewesen mit dem Browser, aber trotzdem kommt da jetzt Werbung von booking.com? Echt krass!

2. Sammelt zunächst in Einzelarbeit, dann gemeinsam an der Tafel, was man gegen Tracking tun kann:

Methodisch-didaktische Hinweise zu AB3: Selbstdatenschutz durch Verschlüsselung

(ab 14 Jahren)

Titel	**Selbstdatenschutz durch Verschlüsselung**
Ziele	**Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.codeplex.com/), optional: Zipordner-Verschlüsselung
Zugang Internet/PC	ja
Hinweise für die Durchführung	• Bestenfalls bringen die SuS eigene Rechner mit, um die Software direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen). • Alternativ können die SuS an den Schulrechnern ihre mitgebrachten USB-Sticks verschlüsseln. Hierzu muss VeraCrypt vorinstalliert sein. • Sollten die beiden obigen Varianten nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen. · Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen. · **Wichtig:** Die hier verwendeten Tutorials sind sehr wahrscheinlich nicht ganz auf Ihr System übertragbar. Testen Sie vorher alles.
Einstieg	Gehen Sie zum Einstieg auf die Seite **www.insecam.org,** auf der gehackte Kameras verlinkt sind. • Diese Kameras sind ein gutes Beispiel für das ständig und rasant wachsende „Internet of Things" (kurz: IoT oder dt. „Internet der Dinge"), bei dem in schnell wachsender Zahl Alltagsgegenstände mehr oder weniger sinnvoll bzw. sicher mit dem Internet vernetzt werden. • Sie können als alternativen Einstieg **aktuelle Nachrichten über Hacks** (http://bit.ly/2C4QMK3) zeigen und dabei darauf eingehen, dass solche Daten gerne **im Darknet** (http://bit.ly/2BMaMoO) gehandelt werden. *Wer von euch fühlt sich online sicher?* • Holen Sie ein kleines Meinungsbild ein.
Erarbeitung	*Offensichtlich gibt es Probleme mit der „Datensicherheit" in der IT. Was meinen wir eigentlich mit dem Begriff „Datensicherheit"?* • Lassen Sie die SuS Aufgabe 1 des Arbeitsblatts bearbeiten und lassen Sie sich Lösungen einiger SuS nennen. Datensicherheit hat vor allem das technische Ziel, Daten aller Art in ausreichendem Maße gegen Manipulationen, Verlust und andere Bedrohungen abzusichern. *Nähern wir uns dem Begriff „Datensicherheit" mit einer Analogie: Was seht ihr auf diesem Bild?* • Zeigen Sie direkt das Fahrrad-Bild aus Anhang 1. • Ein Fahrrad, sein Hinterrad ist abgeschlossen. *Wieso ist es abgeschlossen? Fahrraddiebstahl ist doch per Gesetz verboten.* • Weil es Leute gibt, die dennoch Fahrräder stehlen. Daher trifft man eigene Schutzvorkehrungen → Selbstdatenschutz. **„Hacker-Paragraf"** Es gibt auch für Diebstahl im Digitalen Gesetze, die uns als Bürger schützen. Neben den Datenschutzgesetzen gibt es den **„Hacker-Paragrafen"** (§ 202 c; https://dejure.org/gesetze/StGB/202c.html) im Strafgesetzbuch, der das Vorbereiten des Ausspähens und Abfangens von Daten sowie ihre Beschaffung und Weitergabe unter Strafe stellt. *Genauso wie im Analogen gibt es im Digitalen Kriminelle. Trefft ihr im Digitalen wie mit dem Fahrradschloss ähnliche Vorkehrungen?* **Hinweis:** Eine passwortgeschützte Verschlüsselung entspricht dem Fahrradschloss im Analogen. • Die SuS bearbeiten Aufgabe 2. Kurz im Plenum vergleichen. • Die SuS bearbeiten Aufgabe 3 auf dem Arbeitsblatt. Lassen Sie eine Lösung vorlesen und die Gruppe beurteilen, ob die Analogien gut formuliert wurden.

Erarbeitung

Ransomware – Verschlüsselungstrojaner legen Rechner lahm
Wenn man die Zeit hat oder falls die Lerngruppe etwas älter ist, kann man mit dem Fahrrad-Vergleich außerdem den Begriff „Ransomware" erläutern. Eine solche Ransomware-Attacke ist z. B. WannaCry, die Mitte Mai 2017 Zehntausende Rechner weltweit infizierte.
Es gibt zwei Sprechrollen – „das Digitale" und „die analoge Welt", die von je einer Schülerin oder einem Schüler vorgelesen werden.
Die analoge Welt: Du kommst nach der Schule zu deinem Fahrrad und siehst, dass der Vorderreifen mit einem fremden Schloss abgeschlossen ist. Hast du keinen Bolzenschneider, hast du ein Problem. In der IT-Welt gibt es einen solchen Angriff ebenfalls: „Ransomware".
Das Digitale: Deine Daten werden dabei von einem Verschlüsselungstrojaner unbrauchbar gemacht, und ein Erpresser fordert Lösegeld für den richtigen Schlüssel, damit du sie wieder „aufschließen" und so weiterverwenden kannst.
Die analoge Welt: In der realen Welt ohne Bolzenschneider baue ich das angeschlossene Vorderrad aus. Habe ich ein Ersatzrad zur Hand, kann ich ohne großen Aufwand weiterfahren.
Das Digitale: In der IT löscht man die unbrauchbar gemachten Daten einfach. Das Ersatzrad heißt hier „Sicherheitskopie" (oder „Back-up"). Ist sie vorhanden, spielt man sie auf den Rechner auf und arbeitet normal weiter.

Welche Dateiverschlüsselungsverfahren kennt ihr?

- In-File-Verschlüsselung, bspw. eines Office-Dokuments (MS Word etc.)
- Verschlüsselung eines Zipordners (nur optional besprechen)
- Verschlüsselungsprogramme wie „VeraCrypt" (es gibt viele Alternativen)

Live-Demonstration 1:
Schauen wir uns zuerst die Verschlüsselung eines Dokuments in Microsoft Office an.

- **Hinweis:** MS Word wurde hierfür gewählt, da die meisten Office-Installationen auf das Konto von Microsoft gehen. Alternativen wie Libre Office bieten diese Art der Verschlüsselung ebenfalls an. Anleitungen dazu finden Sie sehr leicht im Internet. Es lohnt sich ggf., LibreOffice vorzustellen, da dieses auf allen Plattformen kostenlos installiert werden kann.
- Zeigen Sie, wie man eine Datei mit einem Passwort abspeichert, bspw. mit dieser **Anleitung** von Microsoft: http://bit.ly/2FXuXyg



Erarbeitung

Je nach Version ergibt sich ein der folgenden Abbildung ähnliches Bild:



Beispiel Windows 10, Quelle: Windows 10

Optional: **Verschlüsseln eines Zipordners**
Zeigen Sie, wie man einen Zipordner mit einem Passwort versehen kann, z. B. zum Versenden von Bildern oder mehreren Dateien per E-Mail. Sie können dazu **diese Anleitung** verwenden: www.bitdefender.de/support/erstellen-eines-passwort-geschuetzten-zip-archives-363.html

Vielleicht möchtet ihr andere Dateitypen als Office-Dokumente versenden oder in einem Online-speicherdienst wie GoogleDrive ablegen. Dafür gibt es nützliche Programme wie VeraCrypt.

- Schauen Sie gemeinsam **das Video „Daten verschlüsseln"** (http://bit.ly/2tcfTdq), auch zu finden auf www.klicksafe.de/klicksafetogo.
- Direkt danach öffnen Sie über einen Präsentationsrechner oder in der Gruppe VeraCrypt. Die Installation können Sie, falls möglich, den SuS zeigen und dazu **die Anleitung aus der Lehrerfortbildung BaWü** (http://bit.ly/2FXtZSP) nutzen.
- Gehen Sie mit den SuS Schritt für Schritt die Installationsanleitung durch, und erzeugen Sie einen Container mit einem Passwort. Spätestens an dieser Stelle wird man auf die Problematik von sicheren Passwörtern und deren Verwaltung aufmerksam. Dies wird in der nächsten Stunde genauer beleuchtet.

Alternativen zu VeraCrypt
Es gibt viele andere Angebote neben VeraCrypt, wie bspw. DiskCryptor oder BoxCryptor. VeraCrypt hat sich in seiner (noch relativ jungen) Vergangenheit als zuverlässig erwiesen und ist „Open Source", d. h., man kann den Quellcode sehen, wodurch Sicherheitslücken transparent werden. Es ist zudem kostenlos und plattformübergreifend nutzbar. VeraCrypt ist ein Nachfolger des mittlerweile eingestellten TrueCrypt-Programmes.

Sicherung

Die SuS bearbeiten Aufgabe 4 und fassen damit zusammen, welche Verschlüsselungsverfahren sie kennengelernt haben.

AB 3: Anhang: Fahrradsicherheit vs. Datensicherheit



Quelle: https://pixabay.com/en/bike-wheel-stadtrad-bike-lock-780049 (CC0-Lizenz)

AB 3: Selbstdatenschutz durch Verschlüsselung

Aufgaben

1. Was bedeutet für dich der Begriff „Datensicherheit"?



2. Was tust du dafür, dass deine Daten online sicher sind?

3. Notiere mit eigenen Worten die Analogie zwischen einem Fahrrad(schloss) und dem Absichern der eigenen Daten.

4. Welche Möglichkeiten hast du kennengelernt, um deine Daten zu verschlüsseln?

Hausaufgabe

Falls du es nicht bereits im Unterricht installiert hast, installiere VeraCrypt zu Hause und berichte in der Klasse von deinen Erfahrungen. Folge diesem Tutorial: https://lehrerfortbildung-bw.de/werkstatt/sicherheit/stickcrypt/vc. Es gibt aber auch zahlreiche andere Tutorials, bspw. auf YouTube. Achte darauf, woher du die Installationsdatei beziehst. Du solltest immer auf die Herstellerseite gehen, auch wenn Tutorials auf andere Quellen verweisen.

Methodisch-didaktische Hinweise zu AB 4: Passwort-Management und Back-ups

(ab 14 Jahren)

Titel	**Passwort-Management und Back-ups**
Ziele	**Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Gespräch, Live-Demonstration: KeePass (https://www.keepassx.org bzw. https://keepass.info)
Zugang Internet/PC	ja
Hinweise für die Durchführung	• Bestenfalls bringen die SuS eigene Rechner mit, um die Software Keepass direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen). • Sollte die obige Variante nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen. · Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen. · **Wichtig:** Die hier verwendeten Tutorials sind wahrscheinlich nicht genauso auf Ihr System übertragbar. Testen Sie vorher alles.
Einstieg	Schauen Sie das Video **„Passwörter einfach erklärt" von Alexander Lehmann** (http://bit.ly/2BO4ftV), welches auch auf **www.klicksafe.de/klicksafetogo** verlinkt ist. Die SuS sollen sich dazu bei Aufgabe 1 auf dem Arbeitsblatt bereits Notizen machen. *Welche Tipps gibt es im Video zu Passwörtern?* • Passwörter sollten lang sein (mind. 10 Zeichen). • Sie sollen Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben enthalten. • Passphrasen sind oft leicht zu merken und lang → hohe Sicherheit. • Verwende nie ein bestimmtes Passwort für verschiedene Dienste (auch kein Single-Sign-in verwenden, z. B. über Facebook für einen anderen Dienst anmelden). • Ändere deine Passwörter regelmäßig. • Verschicke deine Passwörter nie per Mail, denn unverschlüsselte E-Mails sind wie Postkarten – von Unbekannten lesbar. Wenn man doch wichtige Passwörter übermitteln muss, kann man sie bspw. zerteilen und auf verschiedenen Kommunikationskanälen verschicken. Generell sollte man seine Passwörter natürlich gar nicht preisgeben.



Quelle: www.haveibeenpwned.com (Abruf: 10. 5. 2017)

Passwörter werden oft Beute von Hackern
Zeigen Sie auf der Seite www.haveibeenpwned.com, dass in vielen Fällen bereits eigene Passwörter und Accounts gestohlen wurden und online gehandelt werden. Der Screenshot zeigt einen solchen Fall mit einer Mail-Adresse des Autors. Wenn eine Ihrer Mail-Adressen betroffen ist, sollten Sie diesen Fall zeigen. Alternativ probieren Sie einige Mail-Adressen von SuS durch.

Erarbeitung

Im Video kam ein sogenannter Passwort-Tresor vor. Wir schauen uns einen solchen an, er heißt „KeePass".

Führen Sie die Installation selbst zentral einmal durch. Alternativ schauen Sie sich zusammen dieses Beispiel-Tutorial an: https://www.youtube.com/watch?v=tX-Izo7o4a4

Die SuS installieren KeePass auf ihren mitgebrachten Laptops oder installieren die Software als Hausaufgabe.

Diskutieren Sie die Problematik, wenn man sein Master-Passwort (für den Tresor) vergisst oder falls es in falsche Hände gelangt oder eine solche Software Schwachstellen hat.

- Wie immer gilt: Bequemlichkeit und Sicherheit schließen sich gegenseitig aus. Manche Sicherheitsexperten lehnen daher Passwort-Manager grundsätzlich ab.
- Jeder soll eine eigene Risikobewertung durchführen und eine eigene Entscheidung treffen. (Anmerkung: Der Autor verwendet aktuell den Passwort-Manager KeePassX)
- Man muss dort nicht alle Passwörter ablegen; die hochsensitiven sind meistens wenige, und die kann man sich ggf. anders merken.

Alternativen zu VeraCrypt
Es gibt viele Angebote neben KeePass, z. B. LastPass. KeePass hat sich in der Vergangenheit als zuverlässig erwiesen, ist kostenlos und plattformübergreifend. Der Quellcode ist für jedermann einsehbar. Wer trotzdem nach Alternativen sucht, kann hier weiterrecherchieren: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html.

Sind Daten verschlüsselt, ist der Zugriff für Unbefugte unterbunden. Sollen die Daten für einen selbst zugänglich bleiben, ist es wichtig, Sicherungskopien anzulegen. Denn es reicht nicht, sich ein Passwort zu merken, da Unbefugte auch ohne dieses in der Lage sind, die Daten unbrauchbar zu machen. Außerdem kann Technik ausfallen oder verloren gehen. Auch hiervor schützt ein Back-up.

Um Daten vor Unbefugten zu schützen, kann man sie verschlüsseln und mit einem sicheren Passwort versehen. Um uns vor ihrem Verlust zu schützen, sollten wir sie zudem regelmäßig mit einem Back-up sichern.

Was man beim Erstellen von Back-ups beachten sollte, lernen die SuS mit Aufgabe 2. Diese ist neben der auf dem Arbeitsblatt vermerkten 3-2-1-Regel die Sicherung.

Sicherung

Lösung:

Die folgenden Teile von Aufgabe 2 sind korrekt, die anderen sind zu streichen:

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Das externe Speichermedium sollte nie unnötig mit dem Rechner verbunden sein, damit es nicht von Viren befallen werden kann.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
  Bemerkung: Dies kann als Hausaufgabe gestellt werden.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.

AB 4: Passwort-Management und Back-ups

1234567 abc123abc Hasi_007

Aufgaben:

1. Das will ich mir zu Passwörtern merken:

Hausaufgabe:

Falls du es nicht bereits im Unterricht installiert hast, probiere den Passwortmanager KeePass Zu Hause aus und berichte in der Klasse von deinen Erfahrungen. Nutze dazu ein YouTube-Tutorial, wie z. B. „Passwörter verwalten mit KeePass 2" von PC Welt: www.youtube.com/watch?v=tX-Izo7o4a4

2. Nachdem du weißt, wie man Daten verschlüsselt und die dafür nötigen Passwörter verwalten kannst, lies den folgenden Text zu Back-ups. In diesen Text haben sich Fehler eingeschlichen. Streiche die aus deiner Sicht falschen Tipps durch!

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Ein Back-up soll nie verschlüsselt sein, damit man im Notfall sicher drankommt.
- Das externe Speichermedium sollte nie unnötig am Rechner hängen, damit es nicht von Viren befallen werden kann.
- Private Daten sollte man immer unverschlüsselt in der Cloud, also bei Onlinespeicherdiensten, ablegen. Da sind sie sicher.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.
- Das Back-up (bspw. ein Stick) und die eigentlichen Daten (z. B. in deinem Laptop) sollten immer nebeneinanderliegen, damit man schnell auf das Back-up zugreifen kann.

Für Profis gibt es die 3-2-1-Regel

- Daten immer in **dreifacher** Kopie aufbewahren.
- Daten mit **zwei** verschiedenen Technologien sichern. Das können Festplatte, USB-Stick, CD, NAS, Cloud usw. sein.
- Immer **eine** Datensicherung außer Haus aufbewahren, bspw. im Banksafe oder bei den Eltern, nachdem man ausgezogen ist. Achte auf Verschlüsselung!

Methodisch-didaktische Hinweise zu Projekt: Daten unter Artenschutz

(ab 10 Jahren, Autorin: Stefanie Rack)

Titel	**Daten unter Artenschutz**
Ziele	**Die SuS lernen anhand eines Datenschutz-Rapps Grundregeln für den Selbst-Datenschutz kennen.**
Unterrichtsstunden à 45 min.	1
Methoden und Material	Erstellung Poster, Song Datenschutz, Songtext, Poster, evtl. Apps zur Erstellung digitales Poster (zum Teilen in Sozialen Netzwerken)
Zugang Internet/PC	nein (nur für Video)
Einstieg	Zeigen Sie zum Einstieg das Video Datenschutz. Der Rapper und ehrenamtliche Berater Kevin Lehmann von der Plattform JUUUPORT.de und der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. haben mit Unterstützung der DATEV-Stiftung Zukunft ein Musik-Video produziert. Der Rap-Song „Datenschutz", den der 18-jährige Musiker selbst geschrieben hat, erzählt von den Gefahren vor allem für junge Leute, die aus Unkenntnis oder Nachlässigkeit im Umgang mit Datenschutz im Internet entstehen können.  *Abbildung: Screenshot aus dem Video.* Link: **https://www.youtube.com/watch?v=xQzm3OH3zxc&index=21&list=PL6C_wY6dWQLZy7q3fsFFNI8Y3qcxUI9Gk&t=0s** oder Kurzlink: **https://bit.ly/2P4kKbs** In dem Video gibt er 6 Tipps zum Thema Selbstdatenschutz. **juuuport.de – Das Beratungsportal von Jugendlichen für Jugendliche** JUUUPORT.de ist eine bundesweite Online-Beratungsplattform, an die sich Jugendliche wenden können, wenn sie Probleme im Netz haben, z. B. gemobbt oder abgezockt wurden. Hier bekommen sie Hilfe von Jugendlichen, den JUUUPORT-Scouts. Ihre Beratung ist anonym und kostenlos.
Erarbeitung	Die SuS schreiben die Tipps aus dem Video auf die Arbeitsblattvorlage. Mit einer Gestaltungs-App am Tablet oder einem Textverarbeitungsprogramm am PC gestalten die SuS die Regeln (z. B. Piktogramme finden, Bilder, Metaphern aus dem Songtext verwenden). Das Plakat, das den meisten Zuspruch der Klassengemeinschaft erhält kann als „Werbeplakat" im Schulhaus aufgehängt, auf die Schulwebseite gestellt oder über die Sozialen Medien der SuS geteilt werden. **Pufferaufgabe für Schnelle:** Spiel Data-Clash **https://deinedatendeinerechte.de/spielen/**
Sicherung	Die SuS stellen ihre Version der Plakate vor, das „Werbeplakat" wird bestimmt.

Songtext Datenschutz

Stell Dir vor, Du veröffentlichst ein Bild von Dir auf Insta
Und loggst Dich mit ´nem Passwort ein auf Facebook oder Twitter
Damit nicht fremde Leute Deine Daten einfach stehlen
Kannst Du immer auf den Datenschutz zählen

Du musst trotzdem aufpassen, das kann ich Dir nur raten
Sonst nehmen sie Deine Daten und versuchen Dir zu schaden
Ich erkläre Dir, was Du machen kannst, um Dich zu schützen
Befolge diese Tipps, denn sie werden Dir was nützen

Nummer 1:
Gib nicht zu viel Infos von Dir Preis, weil sonst jeder von Dir weiß,
wo Du wohnst und wie Du heißt

Nummer 2:
Pass auf, was für Apps Du runterlädst
Dass nicht bei kunterbunter Auswahl der Zugriff untergeht
Denn was die App so darf, wird am Anfang kurz erwähnt
Doch dann ist es schon zu spät und Deine Daten unterwegs

Nummer 3:
Du darfst alles schreiben, irgendwie
Aber „think before you post", das Internet vergisst nie
Vergesse niemals Deinen Datenschutz
Diese Regel verleiht Deinen Daten Schutz
Diese Regel stellt die Daten unter Artenschutz
So wirst Du im Internet nicht ausgenutzt

Nummer 4:
Nimm nicht immer dasselbe Passwort
Denn hat es jemand, ist es fast dasselbe wie ein Passport
Er kommt über Deinen Namen überall rein
Und schreibt dann Unsinn über Dich – wie gemein

Nummer 5:
Bilder posten ist nicht schwer
Doch manche Deiner Freunde trifft es vielleicht sehr
Wenn Du Bilder postest, ohne um Erlaubnis zu fragen
Ich würde es nicht wagen, lieber Freundschaft bewahren

Nummer 6:
Zeig Respekt im Netz „be the best" und vermeide Stress
Lass Dich nicht auf Streitigkeiten ein, nein
Du bist zwar anonym, doch Datenschutz sollte niemals Anlass für Beleidigung sein
Befolgst Du diese Tipps, sei ruhig stolz auf Dich
Pass auf, dass Deine Sicht auf diese Dinge nicht bricht,
Dieses schlichte Gedicht überbringt die Nachricht über Datenschutz –
so wirst Du nicht ausgenutzt

Vergesse niemals Deinen Datenschutz
Diese Regel verleiht Deinen Daten Schutz
Diese Regel stellt die Daten unter Artenschutz
So wirst Du im Internet nicht ausgenutzt

Arbeitsblatt zu Projekt: Daten unter Artenschutz – Regeln





Mobiles Internet und das Internet der Dinge

2|1 Handy / Smartphone / Tablet

2|2 WhatsApp & Co

2|3 SmartTV

Übersicht der Bausteine:

- **Handy / Smartphone / Tablet** | **Arbeitsblätter**
- **WhatsApp & Co** | **Arbeitsblätter**
- **SmartTV** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



AlwaysON – Arbeitsmaterial für den Unterricht – Heft 1
https://www.handysektor.de/fileadmin/user_upload/bilder/basisthemen/Paedagogenecke/mobile_medien_-_neue_herausforderungen/AlwaysOn2015.pdf



Safer Smartphone – Sicherheit und Schutz für das Handy
Arbeitsmaterial für den Unterricht – Heft 2
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/SaferSmartphone_Heft2.pdf



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Ergänzende Arbeitsblätter zum Baustein „Privatsphäre und Big Data“
http://www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data



Mobiles Internet und das Internet der Dinge



2_1 Handy/Smartphone/Tablet – Arbeitsblätter methodisch-didaktische Hinweise

Projekt 1 Immer on		
	Ziele	*Die SuS reflektieren problematische Aspekte der Handynutzung.*
	Zeit	*45 min.*
	Methoden	*„Augen auf im Straßenverkehr", Textarbeit, Tafelbild*
	Material	*Ausdrucke Einstiegsübung*
	Zugang Internet/PC	*Nein*

Einstieg

Beginnen Sie die Stunde mit der aktivierenden Übung „Augen auf im Straßenverkehr".

Augen auf im Straßenverkehr!
Die SuS bewegen sich frei im Klassenraum, während sie einen Text über den Einfluss der Handynutzung am Steuer auf die Unfallhäufigkeit in ein Text- oder Notizprogramm ihres Handys tippen. Die Lehrperson oder ein/e SuS diktiert zügig. Bei Berührung stehen bleiben und Handy wegpacken. Sieger ist, wer bis zuletzt im Raum herumläuft und den Text fehlerfrei nachweisen kann. Bauen Sie Richtungswechsel und Schwierigkeiten ein > Ausdrucke, auf die die SuS nicht treten dürfen, mehrfach auf dem Boden verteilen und diese während der Übung verschieben (Bilder ‚Hundekot' und ‚Baustelle' zum Auslegen anbei).

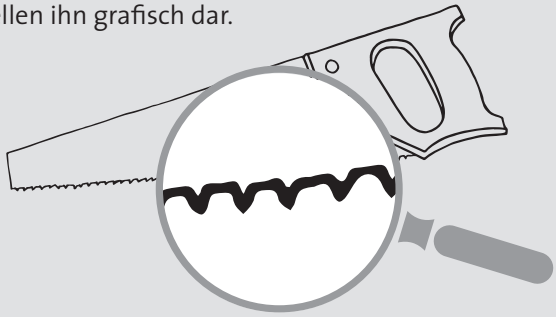
Text: *Einer Schätzung des Allgemeinen Deutschen Automobil-Club (ADAC) zufolge ereignen sich mittlerweile über 10% aller Verkehrsunfälle wegen der Nutzung von Smartphones und Handys. Hier stechen vor allem die jungen Nutzer hervor. So schreibt jeder Vierte zwischen 18 und 24 am Steuer Kurznachrichten.*

Auswertung: Wie schwer ist es euch gefallen, all die Aufgaben gleichzeitig zu schaffen (Aspekt Multitasking ansprechen)? Wie viel Prozent eurer Aufmerksamkeit schluckt das Handy? Geht es euch im Alltag manchmal so wie bei dieser Übung?

Erarbeitung

Wie schwierig es ist, die Konzentration trotz ständiger Ablenkung durch Handys im Alltag zu behalten, sollen die SuS in einer Textarbeit kritisch reflektieren. Sie lernen den Sägeblatt-Effekt kennen und stellen ihn grafisch dar.

Aufgabe 2: Lösung b).
Die Ideen der SuS zur Sägeblatt-Grafik können an die Tafel gezeichnet werden. Beispielsweise können besonders schnelle SuS die Grafiken bereits anzeichnen und später erklären.



Sicherung

Die Tipps der SuS, wie man sich gegen Handystress wehrt, aber auch, wie man die Medien vorteilhaft nutzen kann, werden gemeinsam an der Tafel gesammelt.

Mögliche Lösung: ***Medien in den Griff bekommen = Ablenkung durch Geräte minimieren***	***Medien vorteilhaft nutzen = Abläufe mit den Geräten optimieren***
Push-Benachrichtigungen aus	*bewusste Nutzung (z.B. für Recherche)*
Gruppen stumm schalten	*Sinnvolle Apps (Vokabeltrainer, Lern-Apps, Bahn)*
Räumliche Trennung > Handy in anderen Raum legen	*Aufgabenmanagement (Klassenarbeiten eintragen, Stundenplan-Apps, Noten-Apps, Kalender-Apps)*
Auszeiten und Internet-Sperren > Auszeit-Apps (z.B. Focal Filter)	...

Vollständiger Artikel auf
https://www.handysektor.de/artikel/fomo-bist-du-auch-betroffen/



Immer on – wie Handys uns beherrschen

Etliche Male am Tag schauen wir auf unser Handy, viele wichtige und private Infos speichern wir darin, und ein Leben ohne, das ist für viele von uns kaum vorstellbar. Aber was nimmt es uns eigentlich weg, das Handy, oder wo bringt es uns sogar Probleme?

Aufgaben:

1. Lies den Text aufmerksam.

Medien streben nach Aufmerksamkeit

Mit gezielten Tricks schaffen es Medien, unsere Aufmerksamkeit zu steuern. Sie haben damit eine gewisse Macht über uns, können uns lenken, haben uns im Griff. Eigentlich wollten wir doch jetzt arbeiten. Doch das Gerät weiß, was es tun muss: ein bisschen Lärm machen, ein paar Lichter erleuchten lassen – schon hat es die gewünschte Aufmerksamkeit und wir sind abgelenkt.

In der Regel braucht es einige Minuten, bis wir nach einer Unterbrechung wieder die volle Aufmerksamkeit erreicht haben. Daraus entsteht der sogenannte Sägeblatt-Effekt, der unsere Produktivität einschränkt, da wir nicht mit konstanter Konzentration arbeiten können, weil sie immer wieder absinkt und es anschließend einige Zeit braucht, bis sie wieder dasselbe Niveau erreicht hat.

Medien beherrschen Multitasking. Wir nicht!

Es ist bewiesen: Je mehr wir gleichzeitig machen, desto schlechter machen wir es. Überprüf das mal bei dir selbst. Medien verleiten uns zum Multitasking. Wir sind im Griff der Medien und überfordert vom Multitasking, dem Datenchaos, der Ablenkung und der komplizierten Technik. Überleg dir, wann es das letzte Mal richtig still war, als du gearbeitet hast. Stille gibt es kaum noch. Die folgenden Tipps sollen dir dabei helfen, die Medien in den Griff zu bekommen und sie vorteilhaft zu nutzen, um Zeit und Nerven zu sparen...

Quelle: *www.handysektor.de/geraete-technik/detailansicht/article/blinken-tuten-vibrieren-wie-medien-uns-beherrschen.html*

2. Kreuze an, was man unter „Sägeblatt- Effekt“ versteht:

- ◯ a) Wenn ein Sägeblatt bei einer Säge nach ca. 50 Einsätzen ausgetauscht werden muss, sollte man in etwa auch den Akku seines Handys wechseln.
- ◯ b) Mit dem Sägeblatt-Effekt ist gemeint, dass man nach einer Störung durch das Handy (SMS, WhatsApp, Facebook) eine bestimmte Zeit benötigt, bis man wieder auf der Höhe seiner Konzentrationsfähigkeit angelangt ist.
- ◯ c) Die Stressbelastung, die die Dauernutzung des Handys bei uns auslöst, ist in etwa zu vergleichen mit der Beschallung einer Motorsäge für 10 Minuten.

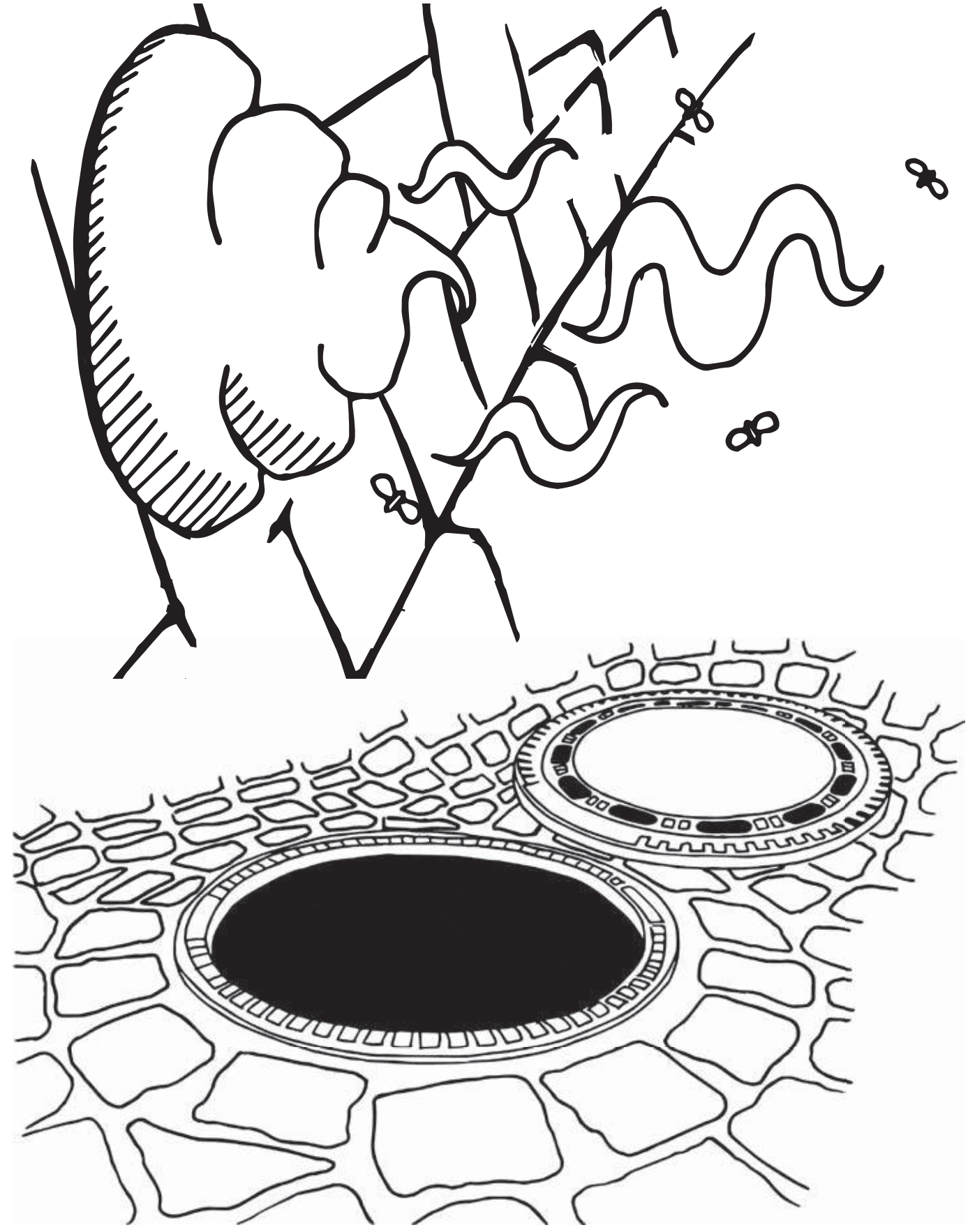
3. Kannst du auf die Rückseite des Arbeitsblattes eine Grafik zum Sägeblatt-Effekt zeichnen, die das Phänomen erklärt?

4. Ups, die Tipps am Ende des Textes fehlen. Welche Tipps würdest du geben? Unterscheide zwischen, Medien in den Griff‘ bekommen und ‚Medien vorteilhaft nutzen‘. Sammelt in der Klasse. Ergänze deine Sammlung.

Hausaufgabe/Zusatzaufgabe:

Schau dir den Spot an: „Dein Leben ist nicht als App erhältlich!“ *bit.ly/1AhGoWI*

Schreibe drei weitere Dinge auf, die in deinem Leben wichtig, aber nicht als App erhältlich sind, und begründe.



Projekt 2 WhatsApp-Regeln		
	Ziele	*Die SuS formulieren Regeln für die Nutzung von WhatsApp.*
	Zeit	*45 (–90) min.*
	Methoden	*versch. Präsentationsformen*
	Material	*Download Video WhatsApp-Stress*
	Zugang Internet/PC	*Nein (Ja für Ausgestaltung der Regeln)*

Einstieg

- Zeigen Sie das Video „WhatsApp-Stress" als Anknüpfung und Wiederholung zu Projekt 1 „Always on".
  Download: *https://www.handysektor.de/mediathek/erklaervideos/*
  Kurze mündliche Sammlung.
  Fragen: **Was stresst Lisa?**
  Welche der Situationen kommt euch aus eurem Leben bekannt vor?

Test: WhatsApp-Nutzung der SuS: Es ist interessant, das Nutzungsverhalten der SuS an dieser Stelle abzufragen. Dazu können die SuS ihren WhatsApp-Traffic – die Anzahl geschriebener und gesendeter Nachrichten – am Handy nachschauen.
Bei iOS und Android: In WhatsApp > Einstellungen > Daten- und Speichernutzung > Netzwerknutzung

Fragen Sie der Reihe nach ab und schreiben Sie die Zahlen in 3 Spalten an die Tafel:

Nachrichten gesendet
Nachrichten empfangen
Nutzung von WhatsApp seit

Die Auswertung soll vor allem ein Gesamtbild vermitteln, wie stark die WhatsApp-Nutzung in der Klasse verbreitet ist. Welche Schlüsse können daraus gezogen werden? Durchschnittswert Nutzung/Monat kann errechnet werden.

Erarbeitung

Die Nutzung von WhatsApp bringt Vorteile, aber auch Probleme mit sich (Stress, Ablenkung, Mobbing). Dies soll nun anhand einer mündlichen Sammlung – „Was ist problematisch an WhatsApp?" – konkretisiert werden. Nutzen Sie zur Veranschaulichung der Problematiken die Schlagzeilen/Teaser von Zeitungs-Artikeln auf dem AB „Mein Kind, ein Smartphone-Junkie", „Cybermobbing: Quälereien über WhatsApp", „Bring dich doch um, alle wären froh, wenn du tot wärst".

Was kann man gegen die gesammelten Probleme in WhatsApp tun?
> Regeln aufstellen > Tabelle auf dem AB wird präsentiert.

Variation: Erfahrungen der SuS mit WhatsApp abfragen durch Satzergänzung.
Satzanfang an die Tafel schreiben: „An WhatsApp finde ich gut/nicht gut..."
Sammlung an der Tafel durch Weitergabe der Kreide/des Whiteboardstifts.

In Arbeitsgruppen (Teilung in 3 Gruppen), Einzel- oder Partnerarbeit werden Regeln für den Umgang mit WhatsApp-Klassen-Gruppen erarbeitet. Aspekte zur Organisation, der Reduktion von Stress bei der Nutzung sowie des fairen Umgangs miteinander sollen berücksichtigt werden.

Sicherung

Die Regelvorschläge der Jugendlichen werden an der Tafel gesammelt, gerankt und abgestimmt (mind. 5 Regeln). Sie werden auf das AB übertragen.

Beispiele:

1. In der Gruppe werden nur Informationen zu Klassenarbeiten, Hausaufgaben und Terminen ausgetauscht.
2. Alle dürfen mitmachen.
3. Keine Beleidigungen, Lästereien und Gerüchte.
4. Als Administrator wird jemand bestimmt, dem wir vertrauen können.
5. ...

Die Regeln können, wenn ausreichend Zeit besteht, in eine anschauliche Form gebracht werden. Sie sollen in WhatsApp-Gruppen, Klasse/Klassenstufe/Schule als Beispiel verbreitet werden. Zur Auswahl:

- Plakat
- Comic

→ z. B. mit der App *www.powtoon.com*

→ digitaler Infoflyer, z. B. mit der App Pic Collage
http://pic-collage.com

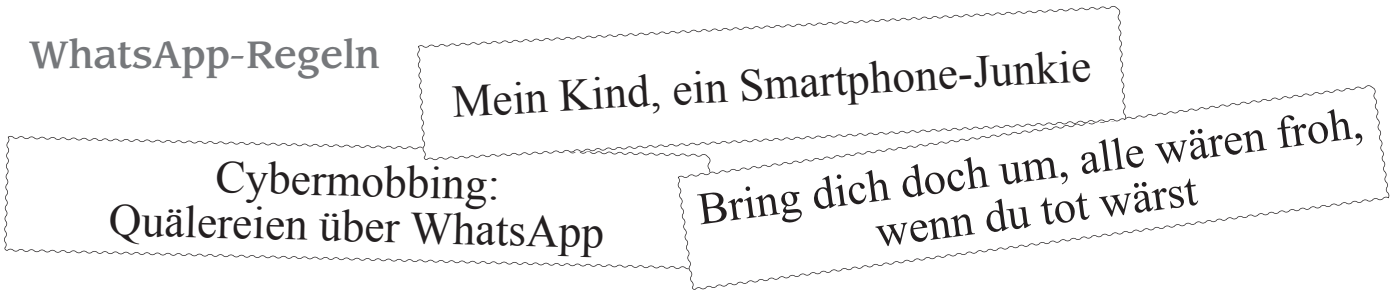
→ auf Medienknigge einstellen:
http://medien-knigge.de

Versuchen Sie, die SuS dazu zu animieren, alternative Krypto-Messenger statt WhatsApp zu nutzen, vielleicht mit einem kleinen Contest?
Wer es schafft, so viele Freunde und Klassenkameraden wie möglich in einen anderen Messenger „mitzunehmen", bekommt eine kleine Belohnung.

Alle Grafiken im Material stehen zum Download unter
https://www.klicksafe.de/mobilemedien zur Verfügung.



WhatsApp-Regeln



Aufgaben:

1. Überlegt euch Regeln für den Umgang mit WhatsApp in eurer Klasse.
   Die Fragen sollen euch dabei helfen, mindestens 2 Regeln pro Überschrift zu formulieren.

1. Organisation der Gruppe	***2. Stressfreie Nutzung***	***3. Fairer Umgang***
Welche Gruppen haben wir? *Warum wurden diese Gruppen gegründet?* *Wer ist für welche Gruppen verantwortlich?* *Sollen gemeinsam Moderatoren festgelegt werden?*	*Welche Einstellungen helfen beim „Anti-Stress-Management“?* *Gibt es Zeiten, zu denen nichts in die Gruppe geschrieben werden soll?*	*Was muss man beachten, damit es nicht zu Mobbing oder schlimmen Vorfällen kommt?* *Was tun, wenn ich bemerke, dass jemand fertiggemacht wird?*

2. Notiere hier die Regeln, auf die ihr euch geeinigt habt:

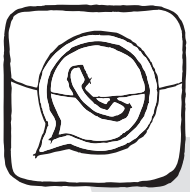
Unsere WhatsApp-Regeln: _____

_____

_____

_____

_____



Lerne auch einmal andere Messenger kennen. Informiere dich auf www.handysektor.de z. B. über Wire, Threema und Signal und überlege dir, wie du deine Klassenkameraden / Freunde dazu bekommen könntest, diese Messenger zu nutzen. Weitere Infos:
https://www.handysektor.de/artikel/messenger-und-sicherheit-wie-sicher-chattest-du/



2_1 Handy/Smartphone/Tablet – Arbeitsblätter
2_2 WhatsApp & Co – Arbeitsblätter
2_3 SmartTV – Arbeitsblätter

Cloud – Wie man Informationen in der Daten-Wolke sicher speichert



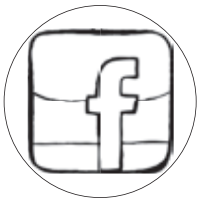
Wie der Begriff „Internet“ schon verrät: die digitale Welt ist eine vernetzte Welt. Alle Computer, Smartphones, Server stehen miteinander in Verbindung und tauschen Daten aus. Dazu gehören auch die Server und Datenspeicher, die das Rückgrat des Internets bilden. Diese stehen auf der ganzen Welt verteilt, meist in großen Datenzentren. Der genaue Aufbau dieser Verbindungen ist allerdings für den „einfachen“ Nutzer nicht sichtbar und wirkt wie von einer Wolke verschleiert. Daher hat sich als Überbegriff für diese Server, Webdienste und Angebote das Wort „Cloud“ (engl. Wolke) etabliert.

Die Cloud ist mehr als nur ein Speicher

Zu Beginn des Cloud-Zeitalters um das Jahr 2007 (Start von Dropbox und Google Docs) wurden damit vor allem Speicherdienste assoziiert, die so etwas wie eine externe Festplatte im Internet anbieten. Zu den bekannten Vertretern gehören unter anderen Dropbox, Google Drive oder OneDrive. Auf ihnen lassen sich Daten ähnlich wie auf einer Festplatte ablegen. Der Vorteil: Der Zugriff auf die Dienste erfolgt per Nutzername und Passwort und man ist daher nicht mehr an ein einziges Endgerät gebunden. Daten können so am PC verarbeitet, dann in den Cloud-Speicher geladen und an einem anderen Computer oder am Smartphone wieder geöffnet werden – und das völlig automatisch und ohne, dass die Geräte direkt, z.B. über ein Kabel, miteinander verbunden sind. Zudem können die online gespeicherten Daten sehr einfach mit anderen Nutzern ausgetauscht werden, was beispielsweise kollaboratives Arbeiten oder das Austauschen von Urlaubsfotos erleichtert.

Heutzutage wird der Begriff Cloud viel weiter gefasst und geht über das reine Speichern von Daten hinaus. Auch komplexe Software wird mittlerweile in der Cloud angeboten. Die Bandbreite reicht von Office-Programmen (z.B. Google Docs und Google Tabellen, Microsoft Office Online) bis hin zu komplexer Bildbearbeitung (z.B. Photoshop Express Editor). Auch hier liegt der Hauptvorteil darin, dass auf die Dienste und die darin gespeicherten Daten (z.B. Textdokumente) von fast jedem internetfähigen Gerät zugegriffen und somit auch gemeinsam an Dokumenten gearbeitet werden kann. Das Installieren von Software auf einem Computer wird damit teilweise überflüssig.

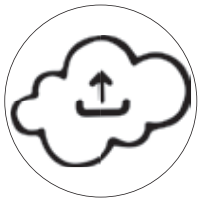
Apps als Tor in die Cloud



Doch tatsächlich sind mittlerweile auch fast alle auf Computern oder Smartphones installierten Apps mit Cloud-Diensten verbunden. Am eindrucksvollsten zeigt sich das, wenn am Smartphone der Flugmodus aktiviert wird. Fast jede App, die dann nicht mehr funktioniert (da sie keinen Internetzugriff mehr hat), greift auf irgendeine Form von Cloud-Dienst zurück. Die meisten Smartphone-Apps sind also nicht viel mehr als das Tor zu einem Cloud-Angebot. Dazu gehören natürlich auch soziale Medien wie Facebook, Instagram oder Snapchat, die ebenfalls darauf setzen, dass wir unsere privaten Daten ihren Internetspeichern anvertrauen. In vielen Webdiensten und Apps hat man heute die Möglichkeit, statt einer Registrierung das Prinzip „Single Sign-On“ (SSO) zu nutzen. Dabei können Nutzer ihre Login-Daten für Facebook, Google oder Twitter einsetzen, um diesen Dienst zu nutzen. Dies ist aus verschiedenen Gründen problematisch: Meldet man sich bei einem der SSO-Anbieter ab, kann man alle damit verknüpften Profile nicht mehr nutzen. Außerdem darf nicht vergessen werden, dass der SSO-Anbieter durch die Verknüpfung der Profile Einsicht in das Nutzungsverhalten hat.

Bei diesen unterschiedlichen und unübersichtlichen Angeboten von Speichern über Software bis zu Social Media haben alle Cloud-Dienste eindeutige Charakteristika: In ihnen können Informationen online gespeichert, mit anderen geteilt und von überall auf der Welt geräteunabhängig abgerufen werden. Auf jedes Cloud-Angebot trifft mindestens eines, meist sogar mehrere dieser Merkmale zu.

Wo genau liegen meine Daten?



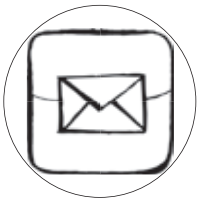
Obwohl die Server, die das Internet bilden, über den ganzen Globus verteilt sind, stehen die meisten in Rechenzentren von nur einigen wenigen Unternehmen. Viele große Anbieter von Cloud-Diensten nutzen deren Infrastruktur. So liegen die Daten von Dropbox oder Instagram etwa auf Servern von Amazon. Was kaum jemand weiß: Obwohl Amazon hauptsächlich als Webshop bekannt ist, ist das Unternehmen zudem einer der größten Serveranbieter der Welt!

Selbst wenn in Europa – auch in Deutschland – einige Rechenzentren existieren, z.B. von Amazon, Microsoft, Google oder Facebook, heißt das nicht, dass alle Daten von deutschen Nutzern auch auf diesen Servern gespeichert werden. Der größte Teil der Daten wird noch immer in den USA abgelegt und verarbeitet. Vor allem im Hinblick auf den NSA-Skandal ist das durchaus bemerkenswert.

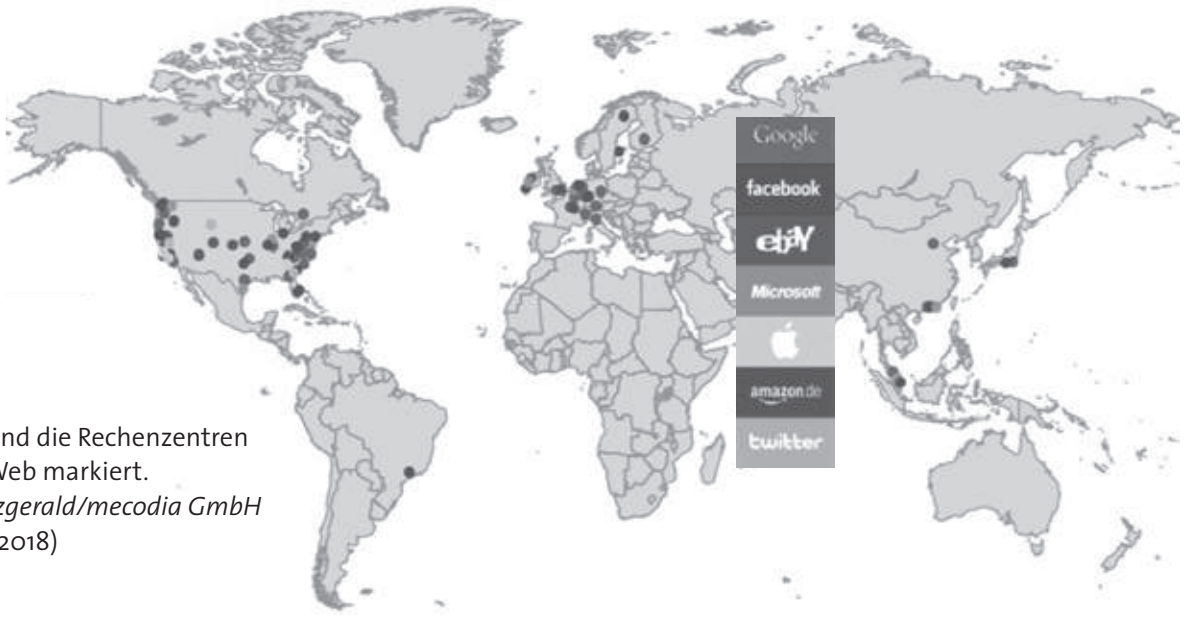
Wie steht es um die Sicherheit von Cloud-Diensten?

Unabhängig von dem Land, in dem sich Daten befinden, können Anbieter einige Sicherheitsmaßnahmen ergreifen. Die wichtigste ist die Verschlüsselung. Liegen die Daten unverschlüsselt auf den Servern, kann jeder mit Zugang zum Speicher alle Informationen auslesen – also auch Hacker, die sich Eintritt zum System verschaffen. Sind sie allerdings verschlüsselt abgespeichert, können nur autorisierte Nutzer mit den entsprechenden Zugangsdaten auf die Daten zugreifen. Cyberkriminelle oder Geheimdienste haben dann keine Möglichkeit, die Informationen auszuwerten – für sie sind diese Daten reinstes Kauderwelsch. Dies ist jedoch nur der erste Schritt.

Wie im Umschlag: Verschlüsselte Datenübertragung



Sind Daten nur auf dem Speicher und nicht auf dem Weg dorthin verschlüsselt, besteht kein vollständiger Schutz. Deshalb ist es wichtig, auch den Übertragungsweg vom Endgerät des Nutzers bis zum Server zu verschlüsseln. Dies ist vergleichbar mit dem Unterschied zwischen einem Brief und einer Postkarte. Ein Brief ist sicher verpackt und kann nur vom Adressaten gelesen werden. Eine Postkarte hingegen ist auch während der Übersendung für alle zugänglich, und auf dem Weg zum Empfänger kann jeder einen Blick auf den Inhalt werfen. Beim Teilen von Daten mit anderen Menschen besteht im besten Fall sogar eine Ende-zu-Ende-Verschlüsselung. Das bedeutet, dass nur die Endnutzer mit ihren Zugangsdaten auf die Inhalte zugreifen können. Selbst für den Anbieter des Dienstes ist das Ausspähen dann unmöglich, da ihm der richtige „Schlüssel“ fehlt.



Auf der Karte sind die Rechenzentren der „Big 7“ im Web markiert.
Quelle: *Peterfitzgerald/mecodia GmbH* (Abruf: August 2018)

Sichere Übertragung prüfen

Ob Daten im Netz sicher übertragen werden, lässt sich bei Webseiten recht einfach ermitteln. Steht bei der aufgerufenen Internetadresse zu Beginn nicht nur „http“, sondern „https“, so steht dies für eine verschlüsselte Verbindung. Nicht ganz so einfach ist es bei Apps. Dort hilft meist nur eine Recherche über den Anbieter, um die Frage der Verschlüsselung zu klären. Offen bleibt in jedem Fall, ob die Daten auch auf den Servern der Anbieter sicher gespeichert werden. Es gibt einige Anbieter von Datenspeichern (z.B. Spideroak) oder Messengern (z.B. Signal, Telegram), die explizit damit werben, den Nutzern eine sichere und gut verschlüsselte Übertragung und Speicherung ihrer Daten zu bieten. Eine wirkliche Möglichkeit, dies nachzuprüfen, haben Nutzer faktisch nicht.

Der Weg der Daten

Die Datenschutzregeln innerhalb Deutschlands und der EU zählen zu den strengsten der Welt. Doch selbst, wenn ein deutsches Cloud-Angebot genutzt wird, ist die Verschlüsselung wichtig. Denn der genaue Weg, den Daten durch das Internet bis zu ihrem Ziel nehmen, ist kaum nachvollziehbar. Selbst beim Zugriff auf ein deutsches Angebot können Informationen um die halbe Welt geleitet werden. Egal ob WhatsApp, Skype oder Bild.de – der Weg der Daten ist immer international. Besonders eindrucksvoll zeigen das die Seiten:
https://apps.opendatacity.de/prism

Das Problem mit dem gekündigten „Mietvertrag“

Bei der Nutzung von Cloud-Diensten begeben sich Nutzer in eine bisher ungekannte Abhängigkeit. Gibt es technische Probleme oder Datenverluste beim Anbieter, sind wichtige Dokumente oder die Urlaubsfotos möglicherweise für immer verloren, es sei denn, es gibt eine Sicherheitskopie auf dem lokalen Computer – aber genau die wollte man sich ja durch die Nutzung von Cloud-Diensten ersparen!

Was ist Streaming?

Die sogenannten Streaming-Dienste sind eine neue Form der Cloud-Nutzung. Bei diesen Anbietern werden Inhalte nur „gestreamt“, d.h. sie liegen nur im Zwischenspeicher des Gerätes. Wie beim Video-dienst YouTube können diese Dienste also nur noch mit Internetverbindung genossen werden. Die große Verbreitung von Streaming-Angeboten hängt stark mit dem Ausbau von Breitbandinternet und mobilem Internet mit hohen Datenraten zusammen, da diese das ruckelfreie Übertragen von Multimediainhalten erst ermöglichen.

Ähnlich problematisch wie bei Cloud-Speichern kann es bei der Nutzung von Streaming-Diensten verlaufen. Wird also die lokale DVD- oder CD-Sammlung durch das Monatsabo für Filme und Serien bei Netflix oder Musik bei Spotify ersetzt, so sind alle Inhalte dort nur „gemietet“. Meistens liegt keine lokale Kopie mehr vor, und wenn doch, kann sie nur innerhalb des Dienstes genutzt werden. Immer wieder kommt es vor, dass die Anbieter Lizenzen nicht verlängern oder Musiker ihre Musik aus den Streaming-Diensten zurückziehen. Es kann also durchaus vorkommen, dass die Lieblingsserie oder der Lieblingsmusiker von heute auf morgen aus dem Angebot verschwinden.

Die Cloud sicher nutzen – und gute Alternativen finden

Auch wenn absolute Sicherheit unmöglich scheint, haben Nutzer trotzdem einige Möglichkeiten, ihre Daten in der Welt der Cloud besser zu schützen.

1. Deutsche Anbieter vorziehen
Gegen Dropbox und Co. ist grundsätzlich nichts einzuwenden. Nutzer sollten sich aber vor der Nutzung darüber informieren, ob die Daten beim gewählten Dienst sicher und gut verschlüsselt übertragen und gelagert werden. Wenn möglich, sollten sie (vor allem bei sensibleren Daten) auf deutsche Anbieter zurückgreifen. Diese sind gesetzlich an Sorgfalts-, Auskunfts-, und Löschpflichten gebunden und müssen Nutzerdaten daher sorgfältiger behandeln, als dies z.B. bei amerikanischen Diensten der Fall ist.

2. Automatischen Upload deaktivieren
Viele Kamera- und Cloudspeicher-Apps bieten einen automatischen Upload von Fotos oder Dokumenten direkt vom Smartphone. Diese Funktion sollte deaktiviert werden. Besser ist es, jede Datei einzeln auf ihre „Cloud-Tauglichkeit" hin zu prüfen.

3. Kritische private Daten nur offline speichern
Besonders kritische Daten wie intime Fotos oder geheime Dokumente sollten grundsätzlich nur offline gespeichert werden – hier geht Sicherheit vor. Eine lokale Sicherheitskopie auf einer externen Festplatte beugt zudem Datenverlusten in der Cloud vor.

4. Passwortschutz nicht vergessen
Und wie immer gilt: Nichts geht über ein sicheres Passwort! Keine noch so gute Verschlüsselung hilft, wenn der Zugang zum Cloud-Dienst mit einem schwachen Passwort gesichert ist.

Die eigene Cloud in der Schule

„Tech-Nerds" bauen sich zu Hause einen eigenen Server und nutzen dafür Software wie ownCloud *http://owncloud.org*. Mit der Software lässt sich mit einigem technischen Know-how und der passenden Hardware eine eigene Cloud erstellen. Dies bietet sich auch als Projekt für den Informatik-Unterricht oder eine Internet-AG an.

Zukunftsvisionen – Wohin geht der Weg?

Auch wenn die Rolle der Cloud in Zukunft weiter zunehmen wird, ist sie für den meisten Deutschen aktuell noch nicht besonders wichtig. Nur 11% aller 15- bis 19-Jährigen halten Cloud-Dienste nach einer Umfrage der GfK aktuell für unverzichtbar. Das mag aber auch daran liegen, dass viele Cloud-Dienste für den Nutzer unbemerkt im Hintergrund ablaufen. Schon in naher Zukunft werden sie für die meisten Internet- und Smartphone-Nutzer folglich immer wichtiger werden, und die Bedeutung von lokalen Datenspeichern wird abnehmen.

Eine logische Weiterentwicklung zeichnet sich aktuell schon ab: Mit dem Nextbit Robin ist das erste Smartphone auf dem Markt, das fast komplett auf lokalen Speicher verzichtet, Daten und Apps befinden sich fast ausschließlich in der Cloud. Die Schlussfolgerung: Ohne Internetzugang funktioniert nichts mehr. Smartphones, Computer und Tablets degenerieren zunehmend zu Bildschirmen mit Internetanbindung, Berechnung und Speicherung finden nur noch online statt, und Nutzer sind mehr und mehr den Anbietern ausgeliefert. Auch das „Internet der Dinge" (engl. IoT = Internet of Things) wird uns in Zukunft beschäftigen. Fast jedes elektronische Gerät kann an das Netz angeschlossen und mit neuen Funktionen ausgestattet werden – auch im Klassenzimmer. Die mit all diesen Entwicklungen einhergehenden Herausforderungen der sicheren Datenübertragung und -speicherung sowie die offensichtlichen Datenschutzprobleme werden uns zukünftig verstärkt beschäftigen. Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl? Auch diese Fragen sollten wir mit den Schülern reflektieren.

Links und weiterführende Informationen

Materialien:

- Always on – Arbeitsmaterial für den Unterricht Heft 1 aus der Reihe „Mobile Medien – Neue Herausforderungen“ *www.klicksafe.de/AlwaysOn*
- Smart mobil – Ein Elternratgeber zu Handys, Apps und mobilen Netzen *www.klicksafe.de/service/materialien/broschueren-ratgeber/smart-mobil-elternratgeber-handys-smartphones-mobile-netze/s/smart/mobil*

Webseiten:

- CheckDeinPasswort *https://checkdeinpasswort.de*
- klicksafe informiert über Passwörter *www.klicksafe.de/themen/datenschutz/privatsphaere/wie-sollte-ein-sicheres-passwort-aussehen/*
- Handysektor Infografik „Smartphone sicher“ *https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html*



Literaturverzeichnis

- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (05. August 2015). Was tun bei Handy-Verlust?. Von Bitkom *https://www.bitkom.org/Presse/Presseinformation/Was-tun-bei-Handy-Verlust.html* (Abruf: 25.01.2018).
- Boyd, Danah (2008): Taken Out of Context: American Teen Sociality in Networked Publics. Dissertation, University of California, Berkeley. Von Danah *www.danah.org/papers/TakenOutOfContext.pdf* (Abruf: 25.01.2018).
- Deutschland sicher im Netz e.V. (2015). DsiN-Sicherheitsindex 2015 | Digitale Sicherheitslage der Verbraucher in Deutschland. Von DsiN *https://www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf* (Abruf: 25.01.2018).
- Die Welt (06. Dezember 2013). Taschenlampen-App spioniert Handynutzer aus. Von Welt.de *http://www.welt.de/wirtschaft/webwelt/article122654943/Taschenlampen-App-spioniert-Handynutzer-aus.html* (Abruf: 25.01.2018).
- GfK (30. Juli 2015). Cloud? Kein Muss für Deutsche. Von GfK *http://www.gfk.com/es-ar/insights/press-release/cloud-kein-muss-fuer-deutsche/* (Abruf: 25.01.2018).
- Herrmann, E. (23. Juli 2015). Diese Apps kommen ohne Werbung oder absurde Zusatzbe-rechtigungen aus. Von AndroidPIT *https://www.androidpit.de/kostenlose-apps-ohne-werbung-oder-zusatzberechtigungen* (Abruf: 25.01.2018).
- Kling, B. (19. September 2015). Dutzende iOS-Apps mit Malware XcodeGhost verseucht. Von ZDNet *http://www.zdnet.de/88246866/dutzende-ios-apps-mit-malware-xcodeghost-verseucht/* (Abruf: 25.01.2018).
- Kremp, M. (18. Februar 2016). Nextbit Robin im Test: Geister-Apps aus der Datenwolke. Von SPON *http://www.spiegel.de/netzwelt/gadgets/nextbit-robin-im-test-dieses-smartphone-hat-den-wolkenspeicher-a-1077571.html* (Abruf: 25.01.2018).
- Tanriverdi, H. (9. Februar 2015). Samsung hört mit – aber nur manchmal. Von SZ.de *http://www.sueddeutsche.de/digital/aufregung-um-spracherkennung-samsung-hoert-mit-aber-nur-manchmal-1.2341288* (Abruf: 25.01.2018).

Projekt	1	2	3
Titel	Standort, Mikro, Kamera... ??? Durchblick bei Berechtigungen	Smartphone – aber sicher! Der Smartphone-Führerschein	Daten in den Wolken
Ziele	Die SuS können App-Berechtigungen einschätzen.	Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen.	Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind.
Zeit	60 min.	120 min., pro Station ca. 10 min.	45 min.
Methoden	Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps	Stationenarbeit	Sammlung Pro & Kontra (Tafelbild), Tipps gestalten, Recherche
Material	Video App-Berechtigungen (02:54), Screenshots, Memory-Kärtchen, Beamer, App Clueful	Smartphoneführerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys	Video Cloud (03:16), Kopiervorlage Wolke
Zugang Internet/PC	Nein (Video App Berechtigungen downloaden)	Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren.	Nein (Video downloaden)

Standort, Mikro, Kamera… ??? Durchblick bei Berechtigungen

Projekt 1	***Ziele***	*Die SuS können App-Berechtigungen einschätzen.*
	Zeit	*60 min.*
	Methoden	*Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps*
	Material	*Video App-Berechtigungen (2,54 min.), Screenshots, Memory Kärtchen, Beamer, App Clueful*
	Zugang Internet/PC	*Nein (Video „Berechtigungen" downloaden)*

Einstieg

Zeigen Sie das Handysektor-Erklärvideo „Berechtigungen" auf *http://bit.ly/1Sol2qP* und stellen Sie die Frage: *Wozu sind bei Apps Berechtigungen nötig? Berechtigungen, die auf Standort, Kontakte, Bilder etc. zugreifen, sind bei einer App einerseits zum Funktionieren notwendig, andererseits gibt es – vor allem bei kostenlosen Apps – Zugriffe, die dafür nicht nötig wären. Dann wird vor allem darauf abgezielt, Daten zu sammeln und zu verkaufen.*



Quelle: *https://play.google.com/store/apps/* (Abruf: 25.01.2018)

Zeigen Sie anhand einer bei SuS beliebten App im Google Playstore die geforderten Berechtigungen: *https://play.google.com/store/apps*
Anleitung Berechtigungen überprüfen bei iOS und Android unter *www.handysektor.de/apps-upps/appgesichert/berechtigungen.html*

Bei dem neuen Betriebssystem Android 6 und bei iOS (bereits bei älteren Versionen) kann man gezielt einzelne Berechtigungen erteilen. Weisen Sie die SuS darauf hin! Screenshots aus den Stores und Betriebssystemen zum Präsentieren finden Sie unter *www.klicksafe.de/mobilemedien*

Erarbeitung

Berechtigungen sind häufig in großen Gruppen zusammengefasst und schwammig formuliert. Um die Bedeutung von Berechtigungen besser verstehen zu können, sollen die SuS in einem Memory Berechtigungen mit der jeweiligen Erklärung zusammenbringen – oder Sie zeigen die Kopiervorlage im Anhang über den Beamer.

Methode Memory: Empfehlenswert ist die Arbeit in Vierergruppen. Kopieren Sie dazu die Kopiervorlage „Memory-Kärtchen" in entsprechender Anzahl. Die SuS schneiden die Kärtchen aus und legen sie auf dem Tisch aus. Sie können auch die vereinfachte Variante spielen, d.h. Kärtchen offen liegen lassen und nicht – wie beim Memory üblich – verdeckt. In Gemeinschaftsarbeit finden die SuS die zusammengehörigen Paare. Zeigen Sie zur Auflösung die Kopiervorlage „Memory-Kärtchen" via Beamer oder OHP.

Einschätzung	Teilen Sie das Arbeitsblatt aus. Die SuS entscheiden bei vier Apps, ob sie diese auf Grundlage der geforderten Berechtigungen herunterladen würden oder nicht, und begründen ihre Entscheidung. Die Apps sowie ihre Berechtigungen sind zwar frei erfunden, orientieren sich aber an realen, von Jugendlichen häufig verwendeten Apps aus verschiedenen Nutzungskategorien (Messenger, Spiele etc.). Vielleicht müssen Sie bei den Berechtigungen In-App-Käufe erklären > *www.handysektor.de/lexikon.html* Auswertung am Platz. • **App Swarmy:** OK/Nein > Wenn man die In-App-Käufe an seinem Gerät bzw. im Store deaktiviert, kann diese App genutzt werden. • **App Soundo:** OK/Nein > Eine Musik-App mit diesen Funktionen benötigt die meisten Berechtigungen zum Funktionieren. Der Zugriff auf die Kontaktdaten dient zwar zur Verbindung mit den Freunden, ist aber wegen der Weitergabe von Kontaktinformationen an Dritte als problematisch einzustufen und für das Funktionieren nicht notwendig. • **App WConnect:** OK > Eine Messenger-App mit diesen Funktionen benötigt alle Berechtigungen zum Funktionieren. In fast allen Messengern kann man den Standort mit anderen teilen, insofern ist es nicht außergewöhnlich, den Zugriff zu erteilen. Man sollte aber, wenn es die Möglichkeit gibt, die Ortung ausschalten (in den Einstellungen des Handys Ortung deaktivieren oder, wenn möglich, für betreffende App ausschalten). • **App Style Checkas:** Nein > Diese App sollte man nicht installieren, da sie die Berechtigung für zu viele Zugriffe verlangt, die für das Funktionieren nicht nötig sind.
Sicherung	Die SuS formulieren am Ende der Einheit mündlich oder an der Tafel gemeinsam Tipps, wie man bei App-Berechtigungen die Kontrolle behalten kann. Sie können die folgenden Tipps übernehmen.

TIPP: Wie behalte ich die Kontrolle über Berechtigungen?

1. Zugriffe mithilfe des Betriebssystems einschränken (bei iOS oder bei Android 6)
2. Schon vor dem Download Entscheidung treffen:
   Welche Apps brauche ich wirklich?
3. Alternative Dienste nutzen, die auf weniger Daten zugreifen.
   Informationen dazu einholen.
4. Apps ausmisten. Nicht mehr verwendete Apps löschen, denn Apps greifen auch dann noch auf Daten zu, wenn sie nicht mehr aktiv genutzt werden (siehe AB App-Ausmistaktion).

Hausaufgabe/Zusatzaufgabe:

Die SuS überprüfen ihre drei Lieblings-Apps auf dem eigenen Handy auf deren Zugriffsberechtigungen. Bei der Einschätzung kann ihnen die App Clueful helfen, die Apps aufgrund von deren Berechtigungen einschätzt (App nur für Android erhältlich).

Kopiervorlage Berechtigungen Memory-Kärtchen

Berechtigung	Erklärung
Körpersensoren	Manche Smartphones verfügen über Sensoren, mit denen z. B. der Puls gemessen werden kann. Darauf wollen vor allem Fitness-Apps zugreifen.
Kalender	Durch den Zugriff auf den Kalender können Apps während Terminen das Handy stumm schalten oder Geburtstage aus Sozialen Netzwerken als Termin anlegen.
Kamera	Viele Apps, die Fotos machen, QR-Codes einlesen oder das LED-Licht als Taschenlampe nutzen, benötigen dafür diese Freigabe.
Kontakte	Viele Apps nutzen diese Zugriffe, um Kontaktdaten abzugleichen, z. B. WhatsApp.
Standort	Über den Standort können Apps ermitteln und teilen, wo sich ein Nutzer gerade befindet, z.B. in Sozialen Netzwerken. Außerdem kann die Berechtigung für Navigation genutzt werden.
Mikrofon	Diese Berechtigung benötigen alle Apps, mit denen man Geräusche aufnehmen kann, z. B. WhatsApp für Sprachnachrichten.
Telefon	Mit manchen Apps, die Zugriff auf das Telefon haben, können Nutzer direkt einen Anruf starten. Systemreiniger-Apps können mit dieser Berechtigung die Anrufliste löschen.
SMS	Mit Zugriff auf SMS können Apps Kurznachrichten senden und auslesen. Das nutzen alternative SMS-Apps oder Apps für Bestätigungscodes, z.B. WhatsApp.
Speicher	Komplexe Spiele, Galerie- oder Musik-Apps können mithilfe dieser Berechtigung Daten auf einem externen Speicher (Speicherkarte) abspeichern.

Quelle: *Berechtigungen Google Play Store (Stand 25.01.2018). Erklärung: Handysektor*

Standort, Mikro, Kamera… ??? Durchblick bei Berechtigungen

Durch BERECHTIGUNGEN erlaubst du dem Anbieter einer App schon beim Download den Zugriff auf Informationen und Funktionen auf deinem Handy (z.B. Telefonbuch, Mikrofon). Nicht immer aber sind Berechtigungen „böse“ oder „schlecht“, denn manche Berechtigungen brauchen Apps einfach zum Funktionieren.

Aufgaben:

1. Wann ist eine Berechtigung „OK“ oder wann sagst du eher „Nein“?
Würdest du dir die vier Apps **Swarmy**, **Soundo**, **Wconnect** und **Style Checkas** auf dein Handy laden?
Entscheide und begründe. Du kannst zu jeder App ein Logo erfinden!

2. Überlege dir vier Tipps, wie du die Kontrolle über Berechtigungen behältst.

_____

_____

_____

_____

TIPP: App-Ausmist-Aktion – Mach's wie mit deinem Kleiderschrank

Apps greifen auch dann noch auf deine Daten zu, wenn du sie gar nicht mehr aktiv nutzt. Das kannst du prüfen, z.B. bei Android-Handys unter Einstellungen > Datenverbrauch („Hintergrunddaten“). Er-stelle eine Liste mit den zehn Apps, die du in den letzten vier Wochen benutzt hast. Lösche die anderen – vor allem kostenlosen – Apps, die du nicht mehr benötigst, von deinem Handy.

_____

_____

_____

_____

_____

_____

_____

_____

_____



SWARMY

Beschreibung:
Leite den Fischschwarm durch ein Unterwasserlabyrinth.

Berechtigungen:

- In-App Käufe
- Internetzugriff

App-Logo:

Meine Entscheidung:

Soundo

Beschreibung:
Mit Soundo kannst du nicht nur Musik hören, sondern auch Musik erkennen.

Berechtigungen:

- Mikrofon
- Internetzugriff
- Kontakte

App-Logo:

Meine Entscheidung:

WCONNECT

Beschreibung:
Die neue Messenger-App verbindet alle deine Wünsche: Chatten, Video- und Sprachnachrichten.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten

App-Logo:

Meine Entscheidung:

Style Checkas

Beschreibung:
Bist du Beauty oder Loser? Die App sagt es dir.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten
- SMS
- Speicher
- In-App Käufe

App-Logo:

Meine Entscheidung:

Smartphone- aber sicher! – Der Smartphone-Führerschein

Projekt 2	***Ziele***	*Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen.*
	Zeit	*120 min., pro Station ca. 10 min.*
	Methoden	*Stationenarbeit*
	Material	*Smartphone-Führerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys*
	Zugang Internet/PC	*Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren*

Vorbereitung

Kündigen Sie rechtzeitig an, dass die SuS ihre Handys mit in den Unterricht bringen sollen. Bereiten Sie den Raum mit 5 Stationen und den Stationenbeschreibungen vor. An jeder Station sollte ein PC oder Tablet mit Internetverbindung zur Verfügung stehen. Wenn dies nicht möglich ist, können die SuS auch an ihren Handys recherchieren und die Videos anschauen (Schul-WLAN?). Für das Quiz an Station 4 ist ein PC notwendig. Legen Sie an Station 3 Papier für die Gestaltung der Tipps für den sicheren App-Kauf aus. Kopieren Sie die Führerscheine in der entsprechenden Anzahl der SuS.

Einstieg

Steigen Sie mit den Ergebnissen einer Studie in die Stunde ein: Laut einer Studie gehören 16- bis 19-jährige Nutzer zur Gruppe der „Fatalistischen Handynutzer". Fatalistisch bedeutet schicksalsergeben. Was bedeutet das, und wie könnt ihr euch das erklären?
Quelle: *www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf,* S.22, (Abruf: 25.01.2018) Erklärung: Trotz guter Kenntnisse und hohem Gefährdungsgefühl verzichtet diese Gruppe auf Basisschutzmaßnahmen wie z. B. Passwörteränderungen.

Alternative: Abfrage in der Klasse zum Thema sicheres Handy: Wer von euch nutzt die Bildschirmsperre? Wie häufig wechselt ihr eure Passwörter? Wer hat Antiviren-Programme auf seinem Handy? Wer nutzt Privatsphäre-Einstellungen in Diensten wie WhatsApp oder Facebook?

Teilen Sie die SuS in fünf Gruppen ein und verteilen Sie die Laufzettel. Da alle Gruppen alle Stationen durchlaufen, ist es egal, an welcher Station sie beginnen. Teilen Sie daher die Gruppen den einzelnen Stationen zu. Für jede Station werden ungefähr 10 Minuten benötigt.

Erarbeitung

Kündigen Sie auf ein akustisches Signal hin den Stationenwechsel an.

TIPP: Informationen recherchieren lassen

Wenn die SuS Hintergrundinformationen benötigen, lassen Sie die Recherche in einer Suchmaschine an PC oder Tablet durchführen. Bei Handysektor finden die SuS ein Lexikon, in dem Begriffe wie IMEI erklärt werden: *www.handysektor.de/lexikon.html* Die SuS haben auch die Möglichkeit, sich gegenseitig zu helfen. So können „Experten" für bestimmte Handys und Handy-Betriebssysteme ernannt werden, die bei Fragen speziell an den Stationen 1 bis 3 gruppenunabhängig helfen.

Sicherung

Die Gruppenergebnisse sowie die „unbekannten Funktionen" (Tafelanschrieb Station 2) sollen vorgestellt und besprochen werden. Die Smartphone-Führerscheine werden bereits unterschrieben an die SuS ausgeteilt.

Station 1: Sicherheit - Schütz dein Phone!

Sicherheit für euer Smartphone ist bestimmt ein Thema für euch, oder? Dann sollten die Einstellungen an euren Geräten auch so aussehen wie in der Tabelle unten. Wenn ihr etwas nicht findet, fragt jemanden aus eurer Gruppe, der das gleiche Smartphone hat, oder gebt eure Frage zusammen mit eurem Betriebssystem in eine Suchmaschine ein. Streicht auf eurem Laufzettel durch, was ihr bereits richtig eingestellt habt.
Wenn ihr im Unterricht etwas nicht erledigen konntet, holt es zu Hause nach.

TIPP: Auf *www.handysektor.de/lexikon.html* findet ihr Erklärungen zu den Begriffen.

GPS, WLan und Bluetooth	**ausschalten** (wenn du es nicht brauchst)
Betriebssystem Update	**durchführen**
AntiVirus App (nur für Android notwendig, beim Download auf gute Bewertung im Store achten)	**installieren**
Bildschirmsperre (am Sichersten mit Passwort)	**einschalten**
IMEI (= die Seriennummer eures Handys, bei Verlust oder Diebstahl der Polizei melden)	**herausfinden und notieren**
In-App-Käufe (z.B. Zusatzkäufe in Spiele-Apps wie Münzen oder Edelsteine)	**ausschalten**
„Handy suchen“ (iPhone: schau in den Einstellungen nach; Android: schau unter android.com/devicemanager im Internet nach)	**herausfinden und aktivieren**
Roaming	**ausschalten**
Hausaufgabe: Drittanbietersperre/Mehrwertdienste sperren lassen (z.B. Premium-SMS für Casting-Shows)	**sperren lassen** beim Telefonanbieter (Eltern bzw. Vertragsinhaber anrufen lassen)

Zusatzaufgabe: Hier gibt es Videos von Handysektor, die euch bei den Aufgaben helfen können und weitere Infos liefern: Was ist eigentlich ein Bewegungsprofil?
Unter *http://bit.ly/1RxIGdo* und
Kostenfallen unter *http://bit.ly/1Rjv4oN*

Station 2: Funktionen – Check dein Phone!

Fast jede Woche kommt ein neues Handy auf den Markt, mit immer spektakuläreren Funktionen: Fingerabdrucksensor, verbesserte Spracherkennung, mobile Bezahlfunktionen und noch viel mehr.

Kennt ihr euer Handy eigentlich in- und auswendig? Wählt aus der folgenden Liste mindestens drei Aufgaben aus, am besten etwas, das ihr noch nicht gemacht habt.

- Erstellt ein Foto, das ihr direkt am Handy mit Funktionen, die euch zur Verfügung stehen, bearbeitet.
- Erstellt ein kurzes Video (max. 10 Sekunden) und zeigt es jemandem aus eurer Gruppe.
- Erstellt eine Sprachmemo, z.B. in einer Fremdsprache.
- Erstellt eine Nachricht per Spracheingabe, z.B. SMS oder WhatsApp.
- Erstellt einen Termin in eurem Kalender, z.B. die nächste Klassenarbeit.
- Denkt euch etwas Eigenes aus.

Zusatzaufgabe: Unbekannte Funktionen
Habt ihr bei eurer Reise ins Handy Funktionen entdeckt, die ihr noch nicht kanntet? Wenn nicht, dann macht euch auf die Suche! Schreibt sie an die Tafel und erklärt sie am Ende der Stunde euren Klassenkameraden und -kameradinnen.

Station 3: Apps – Alles unter Kontrolle?!

Apps kaufen und installieren ist kinderleicht, oder?
Dass man dabei aber auch einiges beachten muss, zeigt euch das Video „Appgesichert“ unter
http://bit.ly/1RfJ303



Quelle: *www.handysektor.de/mediathek/videos/erklaervideo-appgesichert.html,* (Abruf: 25.01.2018)

Notiert die vier wichtigsten Tipps aus dem Video und gestaltet sie ansprechend für eure Klassenkameraden und -kameradinnen (auf Papier, in einem Textverarbeitungsprogramm am PC oder mithilfe einer Design-App wie Pic Collage am Handy oder Tablet).

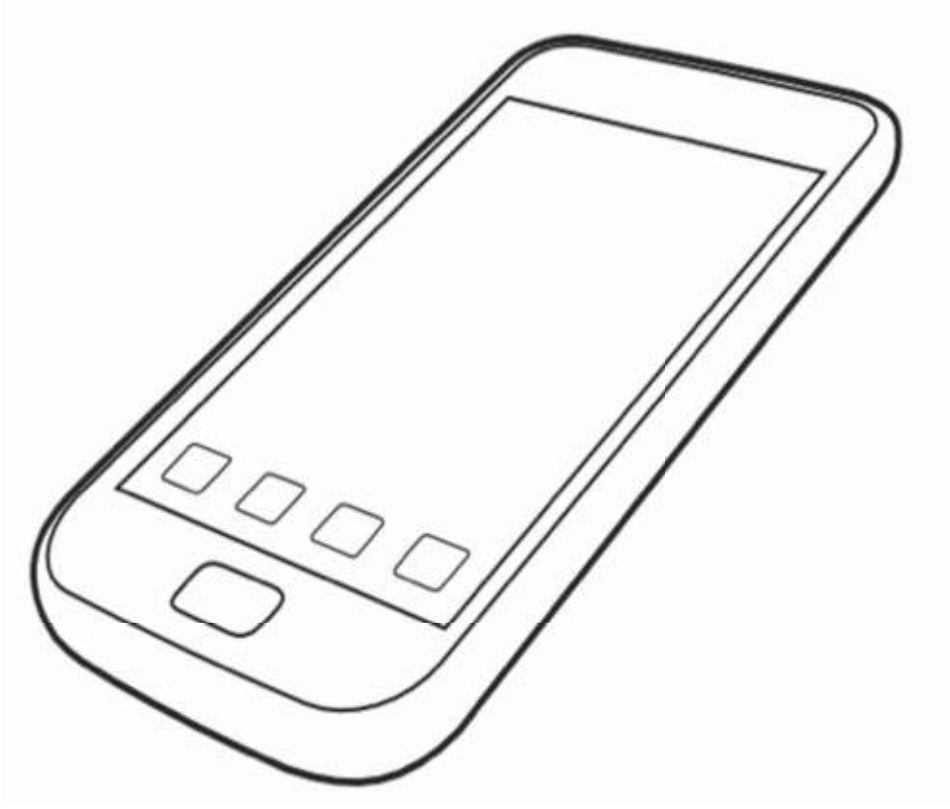
Station 4: Quiz „Smart mobil?!“

Testet euer Handywissen am Computer mit dem klicksafe- Quiz „Smart mobil“. Wählt das Quiz mit den Zusatzinfos! Habt ihr alle gut aufgepasst? Jeder merkt sich eine Frage, die er besonders schwierig fand und stellt sie am Ende des Quiz' nochmal in der Gruppe.
Quiz: www.klicksafe.de/qz/quiz11/_project

Quelle:
www.klicksafe.de/rack:qz/quiz11/_project/ (Abruf: 23.03.2016)

Station 5: Das sichere Handy der Zukunft

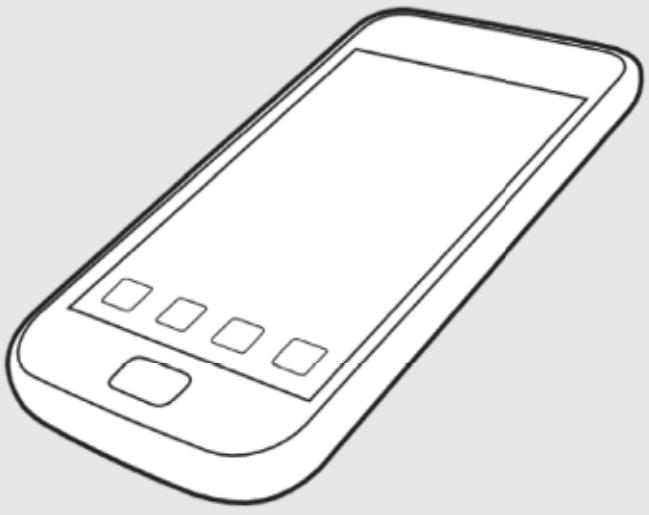
Das Handy der Zukunft liegt vor euch, allerdings nur als leere Skizze. Welche Sicherheitsfunktionen sollte es haben? Welche Apps braucht es zum Schutz? Zeichnet oder schreibt eure Ideen darauf!



Zusatzaufgabe:
Habt ihr Lust auf weitere Informationen zum Thema sicheres Handy? Recherchiert zu folgenden Begriffen: Blackphone und Kryptohandy, und notiert euch auf der Rückseite eures Laufzettels, was ihr dazu herausfindet.


YEEESS
Herzlichen Glückwunsch! Du hast Dein Handy gut unter Kontrolle!
Smartphone-Führerschein für
Datum, Unterschrift Lehrperson
WOOW
1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft


YEEESS
Herzlichen Glückwunsch! Du hast Dein Handy gut unter Kontrolle!
Smartphone-Führerschein für
Datum, Unterschrift Lehrperson
WOOW
1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft

Laufzettel: Der Smartphoneführerschein - Name:	
Station	Hake ab, was du erledigt hast:
1. Sicherheit	☐ GPS, WLan und Bluetooth ☐ Update Betriebssystem ☐ AntiVirus App ☐ Bildschirmsperre ☐ IMEI ☐ In-App- Käufe ☐ „Handy suchen“ ☐ Roaming
2. Funktionen	☐ bearbeitetes Foto ☐ kurzes Video ☐ Sprachmemo ☐ Nachricht per Spracheingabe (SMS, Whats App) ☐ Termin ☐ eigene Idee: _____ Hausaufgabe: ☐ Drittanbietersperre/Mehrwertdienste
3. Apps	Tipps für den sicheren App-Kauf: 1. _____ 2. _____ 3. _____ 4. _____
4. Handywissen	Erreichte Punktzahl: _____ von _____
5. Sicheres Handy der Zukunft	

Daten in den Wolken

Projekt 3		
	Ziele	*Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind.*
	Zeit	*45 min.*
	Methoden	*Sammlung +/- (Tafelbild), Tipps gestalten, Recherche*
	Material	*Video Cloud (3,15 min.), Kopiervorlage Wolke*
	Zugang Internet/PC	*Nein (Video downloaden)*

Einstieg

Fragen Sie das Vorwissen der SuS zum Thema ab: Ihr habt sicher schon mal von Cloud oder Clouding gehört. Wisst ihr, woher diese Bezeichnung kommt? Die Erklärung ist auf dem Arbeitsblatt und im Handysektor-Erklärvideo zu „Cloud" zu finden. Teilen Sie das Arbeitsblatt zu Projekt 3 aus und zeigen Sie das Video:
www.handysektor.de/mediathek/videos/erklaervideo-cloud.html

Erarbeitung

Die SuS tragen die Vor- und Nachteile der Datenspeicherung in einer Cloud auf dem Arbeitsblatt zusammen. Besprechen Sie die Aufgabe, vielleicht mit Unterstützung eines Tafelbildes. Die SuS ergänzen ihre Notizen.

Vorteile:

- Programme können ohne lokale Installation über das Internet genutzt werden.
- Man kann gleichzeitig mit Freunden an einem Dokument arbeiten.
- Man kann Computerspiele in guter Qualität streamen
- Die Cloud kann als Datenspeicher genutzt werden, sodass ein größerer lokaler Speicher auf den Geräten zur Verfügung steht.
- Daten können auf allen Geräten synchronisiert werden.
- Der Zugriff auf Daten ist von überall aus möglich.
- Die Cloud-Anbieter verfügen bei Handyverlust über Sicherheitskopien.

Nachteile:

Es besteht Unsicherheit in Bezug auf den Datenschutz (Wie gehen Dienste mit Daten um? Wird etwas weitergegeben/ausgewertet?)

- Die Sicherheit von Cloud-Diensten ist nur schwer überprüfbar.
- Wo stehen die Server? Welches Recht gilt?
- Ohne Internetverbindung ist kein Zugriff auf die Daten möglich.
- Was passiert mit den eigenen Daten, wenn ein Cloud-Anbieter seinen Dienst einstellt und die Daten (Filme, Musik etc.) nicht lokal gespeichert sind?

Die SuS untersuchen anhand der Tabelle die von ihnen genutzten Dienste auf Datenspeicherung in der Cloud und kommen wahrscheinlich zu dem Ergebnis, dass ein Großteil der Dienste, die sie nutzen, ihre Daten in der Cloud speichert.

Test: Sind meine Daten in der Cloud?

Idee 1:

Wenn folgende Fragen mit Ja beantwortet werden können, speichern die Dienste Daten in der Cloud:

- „Kann ich dort Daten (Texte, Bilder, Videos, Termine etc.) speichern und von anderen Geräten abrufen?“
- „Kann ich mit der App Informationen (Texte, Bilder etc.) mit anderen teilen/austauschen?“
- „Kann ich über die App auf Medien (Musik, Videos/Filme) aus dem Netz zugreifen, ohne diese Daten herunterladen zu müssen?“
- „Funktioniert die App nur mit Internetzugang?“

Idee 2:

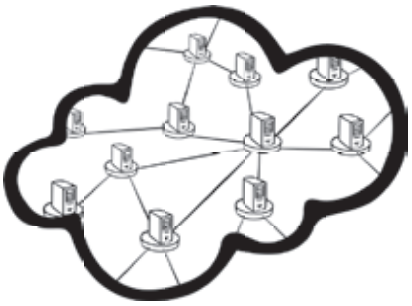
Schüler schalten ihr Smartphone in den Flugmodus. Die meisten Apps, die dann nicht mehr funktionieren – weil sie keinen Internetzugriff mehr haben –, greifen auf eine Form von Clouddienst zurück. Ausgenommen sind hiervon alle Arten von Browsern (z.B. Chrome, Safari etc.), die einfach nur Internetseiten anzeigen.

Sicherung

Die SuS lesen die Tipps auf dem Arbeitsblatt und gestalten einen ausgewählten Tipp in Form einer Wolke. Teilen Sie dazu die Kopiervorlage zu Projekt 3 aus. Sie können die Tipps auch zuteilen, sodass alle fünf Tipps ausgestaltet werden. Die Wolken werden vorgestellt. Sie können im Klassenraum aufgehängt werden. Zum Abschluss der Einheit sollen die SuS entscheiden können: Welche Cloud-Dienste will ich weiterhin nutzen, welche Daten gebe ich an die Cloud ab und welche lege ich lieber lokal ab. Sprechen Sie zum Abschluss mit den SuS über folgende Themen: Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl?

Definition: iCloud, Synchro, Clouding… Was ist eigentlich die Cloud?

Computer und Speicher sind heute auf der ganzen Welt miteinander vernetzt. Der genaue Aufbau wirkt aber wie von einer Wolke (engl. Cloud) verschleiert. Wenn Informationen nicht zentral auf einem Rechner, sondern irgendwo in einem großen Server-Netzwerk liegen, dann sind sie in der Cloud.



Aufgaben:

1. Schaut euch das Handysektor-Erklärvideo „Was ist eigentlich die Cloud?“ an.
Notiert, welche Vor- und Nachteile sich aus der Speicherung von Daten in der Cloud ergeben.
Video: *www.handysektor.de/mediathek/videos/erklaervideo-cloud.html*

_____ _____

_____ _____

_____ _____

2. Tom aus dem Video nutzt bereits Cloud-Dienste: Seine E-Mails liegen in der Cloud, und er streamt Musik und Filme. Welche Cloud-Dienste nutzt du selbst bereits? Schreibe sie auf.

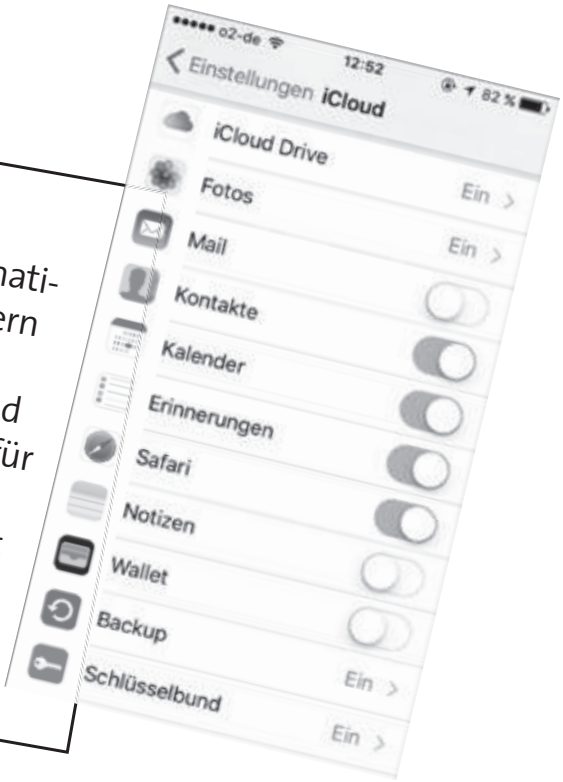
Kategorie	Ja/Nein	Name des Dienstes
E-Mails		
Smartphone> Kalender, Musik, Fotos etc. (z.B. iCloud, Google Drive)		
Musik-Streaming (z.B. Spotify)		
Video-Streaming (z.B. Netflix)		
Cloud Gaming (z.B. OnLive)		
Textverarbeitung (z.B. Google Docs)		
Datenspeicher (z.B. Dropbox)		

3. Lies die folgenden Tipps von Handysektor durch. Such dir einen der Tipps aus und schreibe ihn in die Wolkenvorlage. Du kannst die Vorlage auch noch schön gestalten.

Damit du Cloud-Dienste gefahrlos nutzen kannst,
hier die wichtigsten Tipps:

1. Speichere sensible private Daten wie intime Fotos oder geheime Dokumente nicht in der Cloud.

2. Deaktiviere den automatischen Upload von Bildern oder Dokumenten von deinem Smartphone und entscheide stattdessen für jede Datei, ob du diese in die Cloud laden möchtest (Bild Beispiel iCloud, Quelle: klicksafe, iOS 9.3.1).



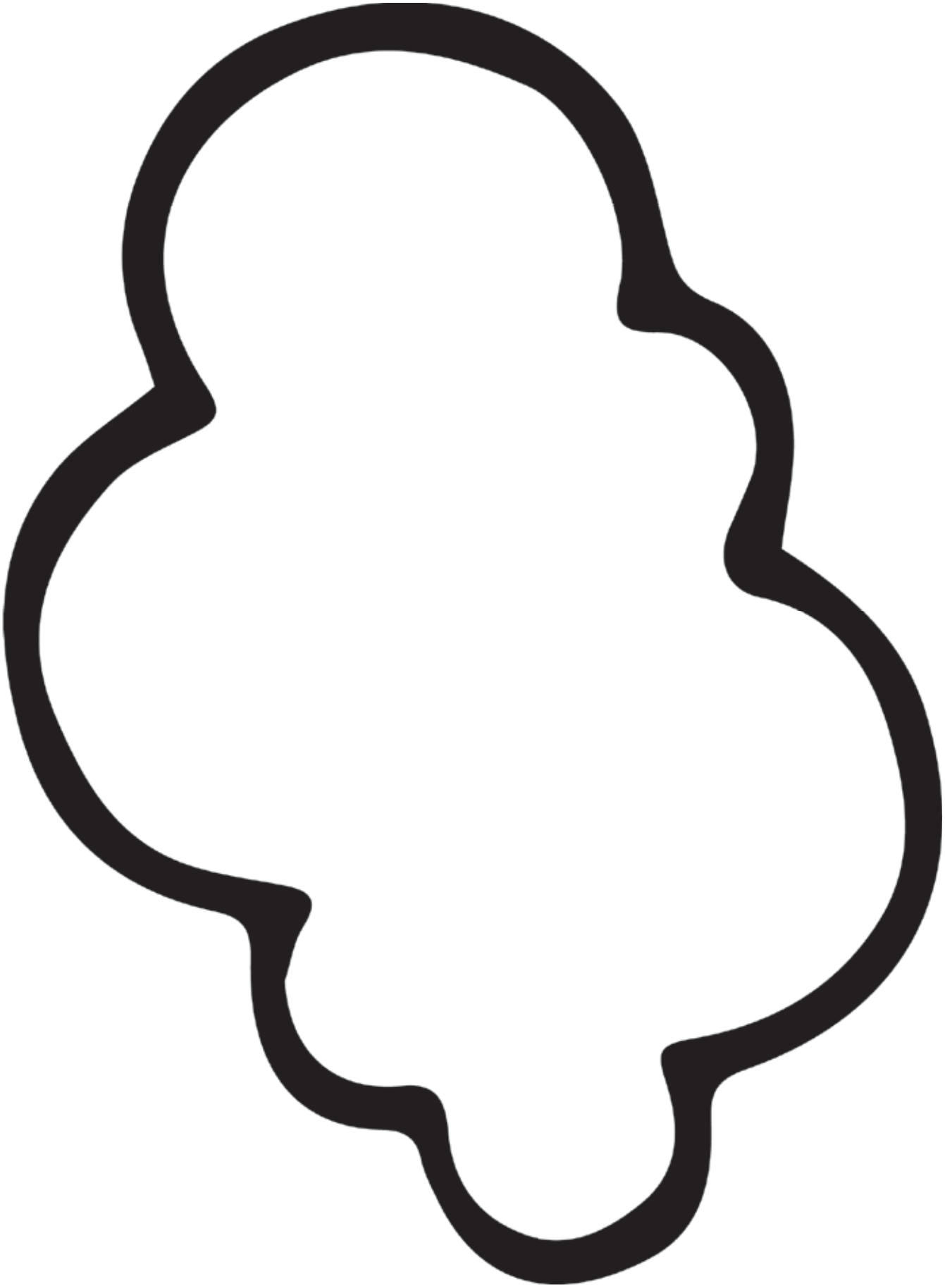
Quelle: *www.handysektor.de/themenmonate/detailansicht/article/safer-cloud-datenschutz-in-der-wolke.html*

3. Verwende ein sicheres Passwort, um deinen Cloud-Zugang zu schützen. Verwende dieses Passwort nirgendwo sonst.

4. Nutze, wenn möglich, die Zwei-Wege-Authentifizierung*, um deinen Zugang zur Cloud zusätzlich abzusichern.

5. Speichere alle Dateien zusätzlich bei dir, z.B. auf einer externen Festplatte. Die Gefahr ist gering, dass Daten in der Cloud verloren gehen, aber so gehst du auf Nummer sicher!

** Zwei-Wege-Authentifizierung bedeutet, dass dir dein Anbieter einen Einmalcode per SMS auf dein Handy schickt, den du zusätzlich zu deinem Passwort beim Anmelden eingeben musst. Da der zweite Code über einen anderen „Weg" verschickt wird, müsste ein Krimineller sowohl dein Passwort knacken als auch an dein Handy gelangen, um Zugang zu deinen Daten zu erhalten.*





2_2 WhatsApp & Co – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Apps für jeden und alles!**	**Der App-Check für Fortgeschrittene**
Kompetenzen	Die Schülerinnen und Schüler beschreiben mit eigenen Beispielen die grundlegenden Funktionen von Handys im Alltag Heranwachsender	Die Schülerinnen und Schüler werten anhand eines vorgegeben „App-Checks" einzelne Apps aus und vergleichen die Ergebnisse miteinander.
Methoden	Internetrecherche	App-Check
Material	Arbeitsblatt	Arbeitsblatt, eigenes Handy
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Apps für jeden und alles!	Die Schülerinnen und Schüler sollen sich in einem ersten Schritt gegenseitig ihre Lieblings-Apps zeigen und dies begründen. Hier wird es sicherlich viele Überschneidungen geben, was ein Indiz dafür sein kann, dass die Handy-Nutzung auch starken Peer-Gruppen-Prozessen ausgesetzt ist bzw. davon bestimmt wird. In einem zweiten Schritt sollen sie die Funktionen von Handys kennenlernen und App-Beispiele dafür finden. Zum Schluss steht die Frage nach der Finanzierung, die im Einzelfall ohne tiefere Recherche nicht einfach zu beantworten ist. Grundsätzlich kann man unterscheiden zwischen „Bezahlung mit Werbung" oder „Bezahlung in der Währung Daten".
AB 2: Der App-Check für Fortgeschrittene	Die Schülerinnen und Schüler sollen mit Hilfe des „App-Checks" eine App analysieren im Hinblick auf Datensicherheit, Werbung, Berechtigungen. Auf dem Arbeitsblatt finden sich bereits technische Hinweise. Viele Funktionen sind gut im Internet zu finden und müssen für die Betriebssysteme und Modelle immer aktuell recherchiert werden, sind aber integriert (wie die Darstellung des Energieverbrauchs oder des Speicherbedarfs der App). Der anschließende Vergleich dient der Präsentation der Ergebnisse und nicht einem qualitativen Vergleich der Apps, der die Schülerinnen und Schüler für die genannten Problematiken sensibilisieren soll. Die Aufgaben h-j eignen sich auch als Hausaufgabe.

Lust auf mehr?

- In modernen Smartphones verstecken sich noch viele andere Funktionen, die missbraucht werden können, z. B. durch sogenannte „Spy-Apps", die unbemerkt Kamera oder Mikrofon aktivieren. Hier lohnt es sich, interessierte Schülerinnen und Schüler etwas tiefer eintauchen zu lassen.
- Ein Trend der Zukunft, oder eher der Gegenwart, wird als das „Internet der Dinge" bezeichnet. Darunter versteht man die Vernetzung von z. B. Haushaltsgeräten und Autos mit dem Internet, gesteuert über Apps auf dem Smartphone. Ein Arbeitsblatt dazu finden Sie auf:
  www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/Zusatz_AB_Internet_der_Dinge.pdf, Lösungen dazu im Bereich
  www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/

Apps für jeden und alles!

Es gibt eine **Biertrinker-App** und eine **Schlafüberwachungs-App** oder auch die **Helium-Stimme-App** und zahllose andere **mehr** oder **weniger sinnvolle Apps** für das Smartphone. Sicherlich hast du selbst viele Apps installiert und nutzt sie intensiv. Hier darfst du Beispiele für Apps finden und diese nach wissenschaftlichen Aspekten sortieren.

Arbeitsaufträge:

1. Bildet Gruppen von max. vier SchülerInnen. Stellt euch gegenseitig eure drei Lieblings-Apps vor und erklärt, warum ihr sie mögt/häufig benutzt! Gebt euch dann einen Gruppen-Namen, der etwas mit euren Lieblings-Apps zu tun hat!
2. Bitte findet Beispiel-Apps für folgende Funktionen, die Wissenschaftler zusammengestellt haben. Erklärt die Beispiele!

Funktion mit Erläuterung	Beispiel-App
Sicherheit, Freunde und Eltern benachrichtigen zu können.	
Organisation des Alltags: Zum Vereinbaren von Abholdiensten mit den Eltern bis hin zu Kontakten zu Freunden und Bekannten.	
Beziehung/Kommunikation mit Freunden und Freundinnen. Das Handy kann als **Schaltzentrale** des sozialen Netzwerkes verstanden werden.	
Identität. Das Handy wird dazu genutzt, sich selbst nach außen darzustellen..	
Unterhaltung durch die Nutzung von Video/Audio und Spielen.	
Information mittels Apps, die Informationen bereitstellen.	
Transaktion wie der Kauf von Kinokarten, Fahrkarten u.v.a.	
Sozialisation durch Fotos von FreundInnen, deren Weitergabe, Social Communities.	
Empowerment mit Anwendungen, die eine Erweiterung eigener Fähigkeiten bedeuten, bspw. Unterstützung körperlich eingeschränkter Kinder und Jugendlicher.	

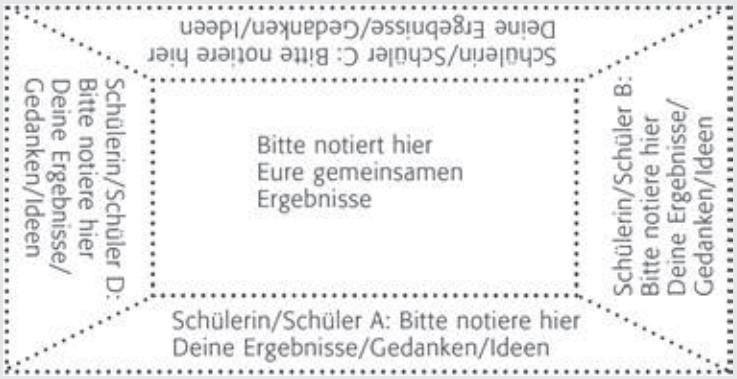
Quelle: Verändert nach: Nicola Döring: „Handy-Kids: Wozu brauchen sie das Mobiltelefon" (2006)

3. Mit Apps lässt sich ein großes Geschäft machen. Recherchiert in der Gruppe wie sich kostenlose Apps finanzieren.



App-Alarm *Du bist dir nicht sicher, ob die App, die du dir herunterladen möchtest, wirklich sicher ist? Dann lasse die App vom Handysektor-Team testen und löse den App-Alarm aus! Auf* ***www.handysektor.de/apps-upps/app-alarm.html***

Beschreibung zum Online-Projekt „Das Internet der Dinge“

Kompetenzen	**Die SuS erkennen die technischen Möglichkeiten des „Internet der Dinge“.**
Zeit	45 Minuten
Methoden	Placemat, Bildergeschichte
Material	Papier (Placemat), Schere + Klebestift (evtl.)
Zugang Internet/PC	Nein
Einstieg	Schreiben Sie „Internet der Dinge“ an die Tafel. Was ist überhaupt das „Internet der Dinge“? Die SuS erstellen in Gruppen ein „Placemat“. **Methode „Placemat“:** Die SuS bilden 4-er Gruppen und legen ein Blatt Papier (DIN A3) in die Mitte. Danach zeichnen sie einen Kasten in die Mitte und verbinden die Ecken des Blattes, so dass außen vier Felder entstehen. Jeweils ein/e Schüler/in setzt sich vor ein Feld und notiert seine/ihre Gedanken (jeder für sich alleine!). Danach drehen die SuS das Blatt um 90°. Die SuS lesen stumm, was die anderen geschrieben haben (schriftliches Kommentieren ist erlaubt). Die SuS wiederholen diesen Vorgang, bis wieder alle vor ihrem ursprünglichen Feld sitzen. Jetzt dürfen die SuS miteinander reden und sollten sich auf eine gemeinsame Aussage einigen, die in der Mitte notiert wird.  Erklärung zum Internet der Dinge siehe Informationskasten Kapitel 2.1 in den Sachinformationen. Zeigen Sie ein Beispiel aus der Sammlung „Internet der Dinge Produktbeispiele 1 und 2“ (PDF), zu finden auf www.klicksafe.de/medienethik.

Erarbeitung

Die SuS bekommen das Arbeitsblatt ausgeteilt. *Wir denken uns ins Jahr 2030. Die Technik ist allgegenwärtig…* Ein Tag im Leben von Paul und seiner Familie soll in einer Bildergeschichte beschrieben werden. Die Beschreibung der Protagonisten wird vorgelesen.
Aufgabe: Findet einen passenden Text und schreibt ihn in die Kästchen.
Lösungsvorlagen finden Sie auf www.klicksafe.de/medienethik.
Quelle Bildergeschichte + Produktbeispiele: Think Tank Medienethik Studierende der HDM Stuttgart.

TIPP
Sie können die ausgeschnittenen Texte aus den Textfeldern den Situationen zuordnen lassen. Teilen Sie dazu das Arbeitsblatt mit den Textkästen aus.

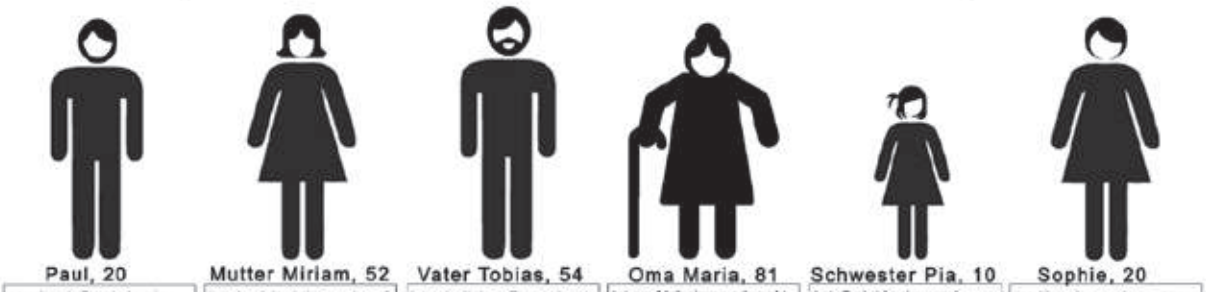
Sicherung

Vorstellung der Bildergeschichten. Auswertung: Könnt ihr euch eine solche Zukunft vorstellen?

Zusatzaufgabe/Hausaufgabe
Fluch oder Segen? Pro/Contra-Sammlung oder Erörterung zum Thema „Internet der Dinge".

Online-Artikel vom 14.01.2014 zur Übernahme des Thermostatherstellers *Nest Labs* durch *Google*: „Google will in Ihr Schlafzimmer": www.spiegel.de/netzwelt/gadgets/nest-uebernahme-google-will-in-ihr-schlafzimmer-a-943406.html

Alltagsszenario 2030



Paul, 20

studiert Soziologie an der Universität Stuttgart. Er ist Single und wohnt noch zu Hause bei seinen Eltern. Neuen Technologien und dem Internet der Dinge steht er sehr offen gegenüber – Paul genießt den Komfort, den ihm die Geräte ermöglichen.

Mutter Miriam, 52

ist Architektin und auf die Gestaltung und Einrichtung von Smart Homes spezialisiert. Durch die schnelle Entwicklung verändert sich ihr Job ständig – um immer auf dem aktuellen Stand zu bleiben, stattet sie das Zuhause der Familie daher stets mit den neuesten Technologien aus.

Vater Tobias, 54

ist arbeitslos. Der gelernte Speditionskaufmann war in einem großen Logistikunternehmen angestellt. Durch die wachsende Vernetzung und den Einsatz neuester Technologien in der Logistik wurden bundesweit die Stellen etlicher Speditionskaufleute eingespart. Tobias ist daher skeptisch im Umgang mit dem Internet der Dinge.

Oma Maria, 81

ist an Alzheimer erkrankt. Vor einiger Zeit musste sie wegen ihrer zunehmenden Demenz aus ihrer Wohnung in eine altersgerechte Wohnanlage umziehen. Ihr Appartment ist mit individuell auf ihre Bedürfnisse ausgerichteten Technologien ausgestattet. So können Senioren trotz Pflegekräftemangel bestmöglich betreut werden.

Schwester Pia, 10

ist Schülerin und gehört der Generation der Smart Life Natives an – ein Leben ohne die Vorteile des Internets der Dinge ist für Pia fast nicht mehr vorstellbar. Nachmittags lernt sie in einem virtuellen Lernraum.

Sophie, 20

ist Krankenschwester in der Smart Clinic Stuttgart West und Single. Paul und Sophie teilen viele Interessen und Charakterzüge.

Morgens um halb 9 in Deutschland im Jahr 2030.

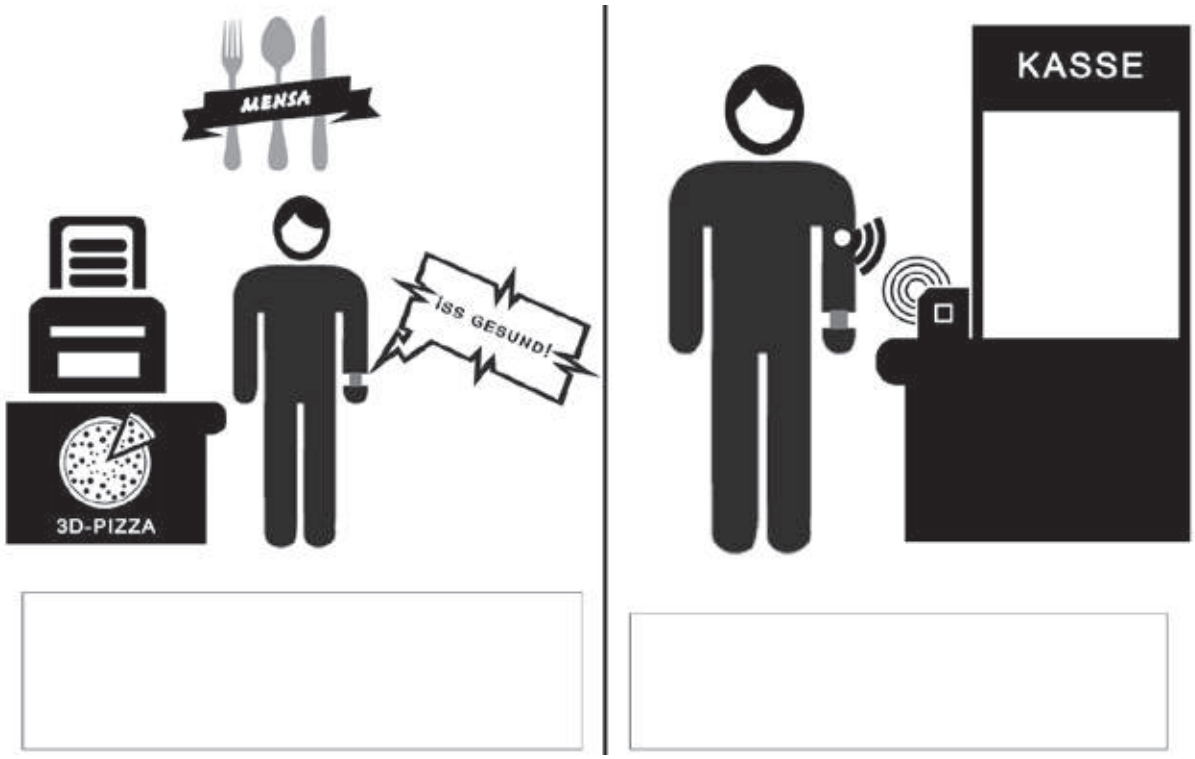


Pauls Wecker klingelt heute automatisch eine Stunde später. Seine erste Vorlesung fällt aus. Der Wecker meldet dem Smart Car, dass es eine Stunde später kommen muss und gibt der Kaffeemaschine Bescheid, damit sie Pauls Kaffee kocht. Der Kühlschrank meldet, dass die Milch leer ist und fragt Paul, ob er eine neue bestellen möchte.

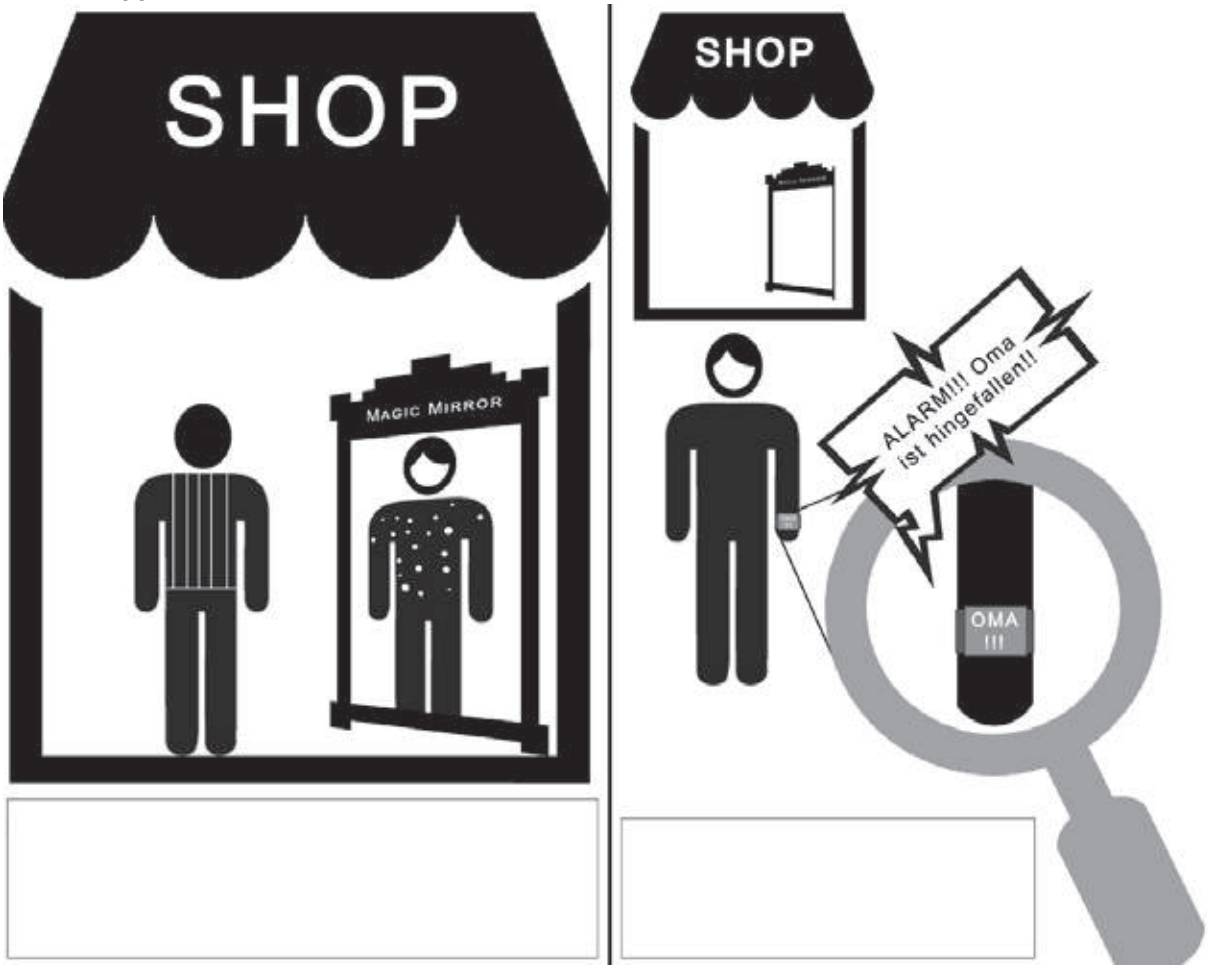
Auf dem Weg zur Uni



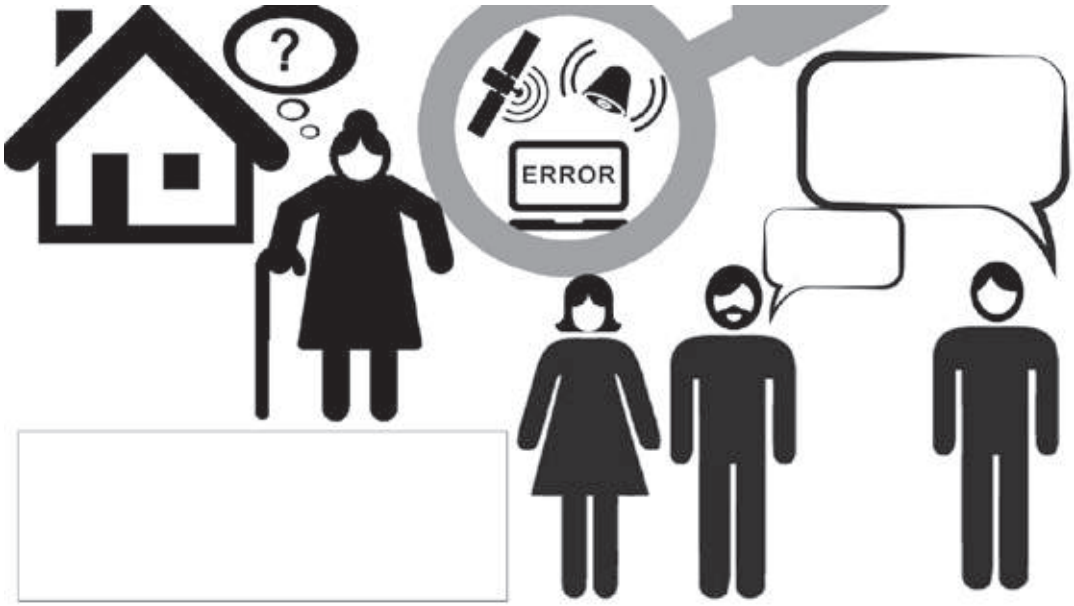
In der Mensa



Beim Shoppen



Oma ist gestürzt? Nur ein Fehlalarm…



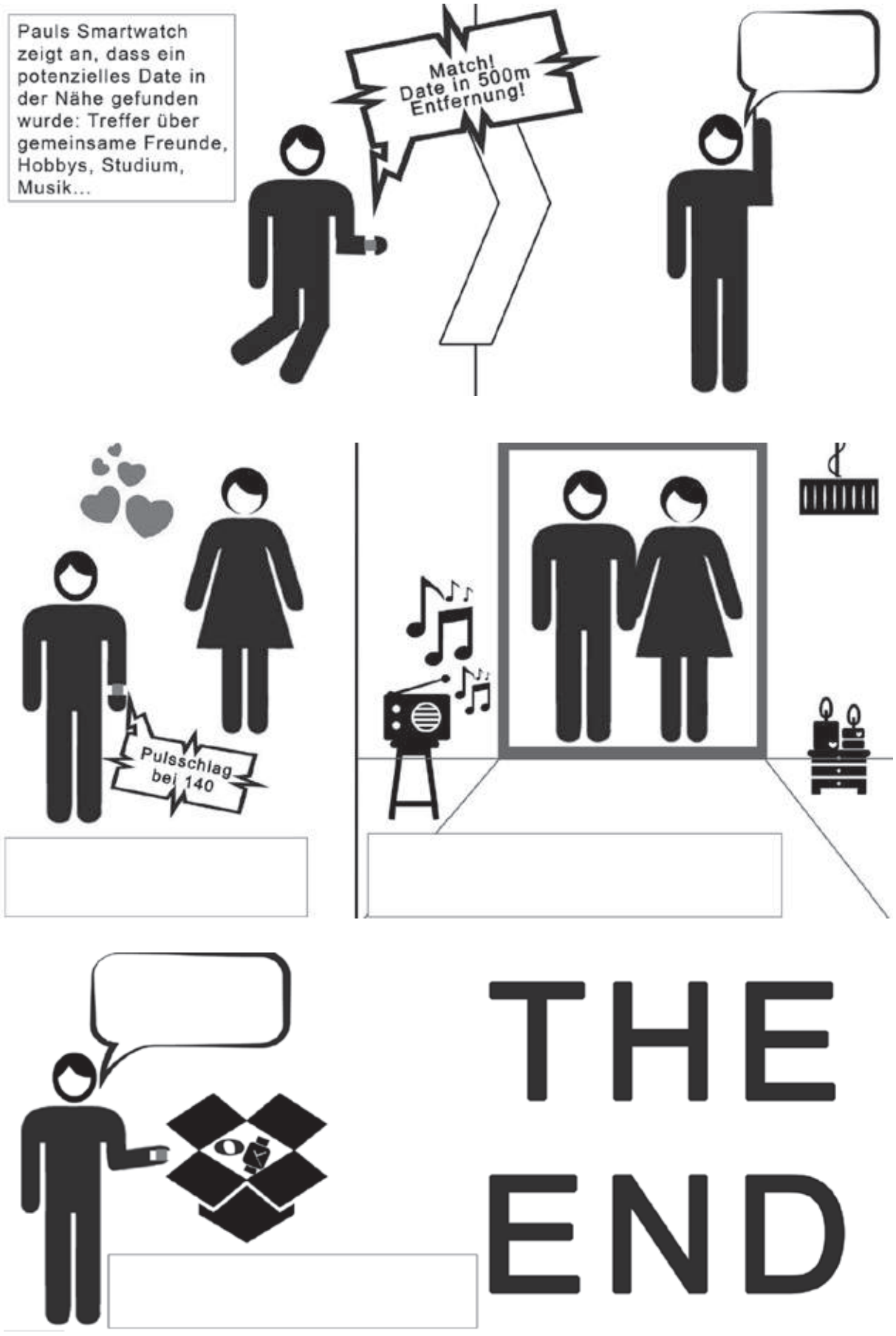
Pia muss nicht alleine daheim sein.



Paul bekommt eine Nachricht von seiner Smartwatch



Liebe 3.0…


Pauls Smartwatch zeigt an, dass ein potenzielles Date in der Nähe gefunden wurde: Treffer über gemeinsame Freunde, Hobbys, Studium, Musik…
Match! Date in 500m Entfernung!
Pulsschlag bei 140
THE END

Paul nimmt seine neue Bekanntschaft mit nach Hause. Das Smart-Home stellt automatisch romantische Musik an, dimmt das Licht und zündet elektrische Kerzen an.

So viel Komfort ist doch super!

Beim Einkaufen wird Paul über seine Smartwatch darüber informiert, dass etwas mit seiner Oma nicht stimmt.

Paul und seine Eltern haben den Alarm erhalten, dass Oma gestürzt ist. Alle treffen bei Oma ein. Doch bei dem Alarm handelte es sich um einen Systemfehler. Cyberkriminelle haben sich in das System gehackt und es lahmgelegt.

Ihr seid auch schon da? Das System hat schon wieder einen Fehler?!

Und Oma ist doch nichts passiert!

Typisch deutsch – German Angst

An der Kasse muss Paul nicht lange anstehen. Er zahlt per RFID-Chip in seinem Arm. Der Betrag wird so direkt von seinem Konto abgebucht.

Ob ich lerne oder nicht, entscheide immer noch ICH.

Lernen verschiebe ich auf morgen!

Auf dem Rückweg von seiner Oma macht Pauls Smartwatch ihn darauf aufmerksam, dass er die Zeit jetzt am besten zum Lernen nutzen sollte.

Pauls Smartwatch zeigt an, dass ein potenzielles Date in der Nähe gefunden wurde: Treffer über gemeinsame Freunde, Hobbys, Studium, Musik…

Paul trifft Sophie. Die beiden verstehen sich auf Anhieb! Pauls Fitnessarmband meldet einen erhöhten Pulsschlag.

Voll Weltraum was mit unseren Daten so alles passiert!

Mir reicht's mit der Überwachung!

Mutter Miriam bekommt eine Nachricht von ihrer Smartwatch, dass Pia von ihrer Interactive-Jacke zu einer Freundin geschickt wurde, da niemand zu Hause ist. Über die Vernetzung mit der Smartwatch schickt sie Pia eine Umarmung an die Jacke.

Um mit Sophie ungestört zu sein, legt Paul alle technischen Geräte ab. Die Nacht gehört nur den Beiden…

Am Nachmittag hat Paul frei und geht einkaufen. Er probiert ein T-Shirt an und kann es im Magic Mirror mit verschiedenen Mustern ausprobieren. Über soziale Medien fragt er seine Freunde, ob er das T-Shirt kaufen soll.

In der Mensa gibt es frische Pizza aus dem 3D-Drucker. Pauls Fitness-Armband alarmiert ihn, auf die Pizza zu verzichten und gesünder zu essen.

Paul fährt mit dem Smart Car zur Vorlesung. Während der Fahrt kann er sich das Skript der vorigen Woche noch einmal durchlesen – oder einfach entspannen. Das Auto ist selbstgesteuert.

Paul besucht an der Universität eine Vorlesung zum Thema Medienethik.

2_3 Internet der Dinge – Arbeitsblätter
Lösungsblatt

Alltagsszenario 2030



Paul, 20

studiert Soziologie an der Universität Stuttgart. Er ist Single und wohnt noch zu Hause bei seinen Eltern. Neuen Technologien und dem Internet der Dinge steht er sehr offen gegenüber – Paul genießt den Komfort, den ihm die Geräte ermöglichen.



Mutter Miriam, 52

ist Architektin und auf die Gestaltung und Einrichtung von Smart Homes spezialisiert. Durch die schnelle Entwicklung verändert sich ihr Job ständig – um immer auf dem aktuellen Stand zu bleiben, stattet sie das Zuhause der Familie daher stets mit den neuesten Technologien aus.



Vater Tobias, 54

ist arbeitslos. Der gelernte Speditionskaufmann war in einem großen Logistikunternehmen angestellt. Durch die wachsende Vernetzung und den Einsatz neuester Technologien in der Logistik wurden bundesweit die Stellen etlicher Speditionskaufleute eingespart. Tobias ist daher skeptisch im Umgang mit dem Internet der Dinge.



Oma Maria, 81

ist an Alzheimer erkrankt. Vor einiger Zeit musste sie wegen ihrer zunehmenden Demenz aus ihrer Wohnung in eine altersgerechte Wohnanlage umziehen. Ihr Appartment ist mit individuell auf ihre Bedürfnisse ausgerichteten Technologien ausgestattet. So können Senioren trotz Pflegekräftemangel bestmöglich betreut werden.



Schwester Pia, 10

ist Schülerin und gehört der Generation der Smart Life Natives an – ein Leben ohne die Vorteile des Internets der Dinge ist für Pia fast nicht mehr vorstellbar. Nachmittags lernt sie in einem virtuellen Lernraum.



Sophie, 20

ist Krankenschwester in der Smart Clinic Stuttgart West und Single.
Paul und Sophie teilen viele Interessen und Charakterzüge.



Pauls Wecker klingelt heute automatisch eine Stunde später. Seine erste Vorlesung fällt aus. Der Wecker meldet dem Smart Car, dass es eine Stunde später kommen muss und gibt der Kaffeemaschine Bescheid, damit sie Pauls Kaffee kocht.
Der Kühlschrank meldet, dass die Milch leer ist und fragt Paul, ob er eine neue bestellen möchte.

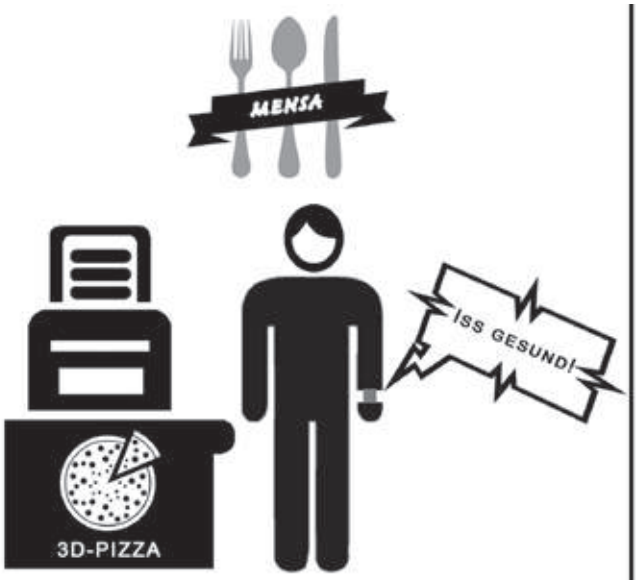


Paul fährt mit dem Smart Car zur Vorlesung. Während der Fahrt kann er sich das Skript der vorigen Woche noch einmal durchlesen - oder einfach entspannen. Das Auto ist selbstgesteuert.



Paul besucht an der Universität eine Vorlesung zum Thema Medienethik.

2_3 Internet der Dinge – Arbeitsblätter
Lösungsblatt



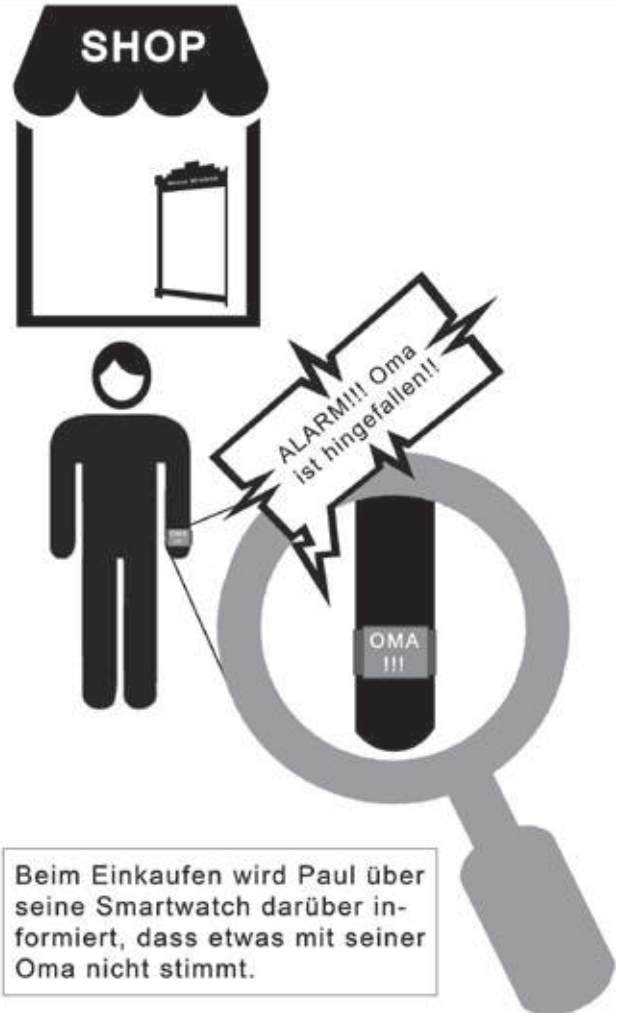
In der Mensa gibt es frische Pizza aus dem 3D-Drucker.
Pauls Fitness-Armband alarmiert ihn, auf die Pizza zu verzichten und gesünder zu essen.



An der Kasse muss Paul nicht lange anstehen. Er zahlt per RFID-Chip in seinem Arm. Der Betrag wird so direkt von seinem Konto abgebucht.

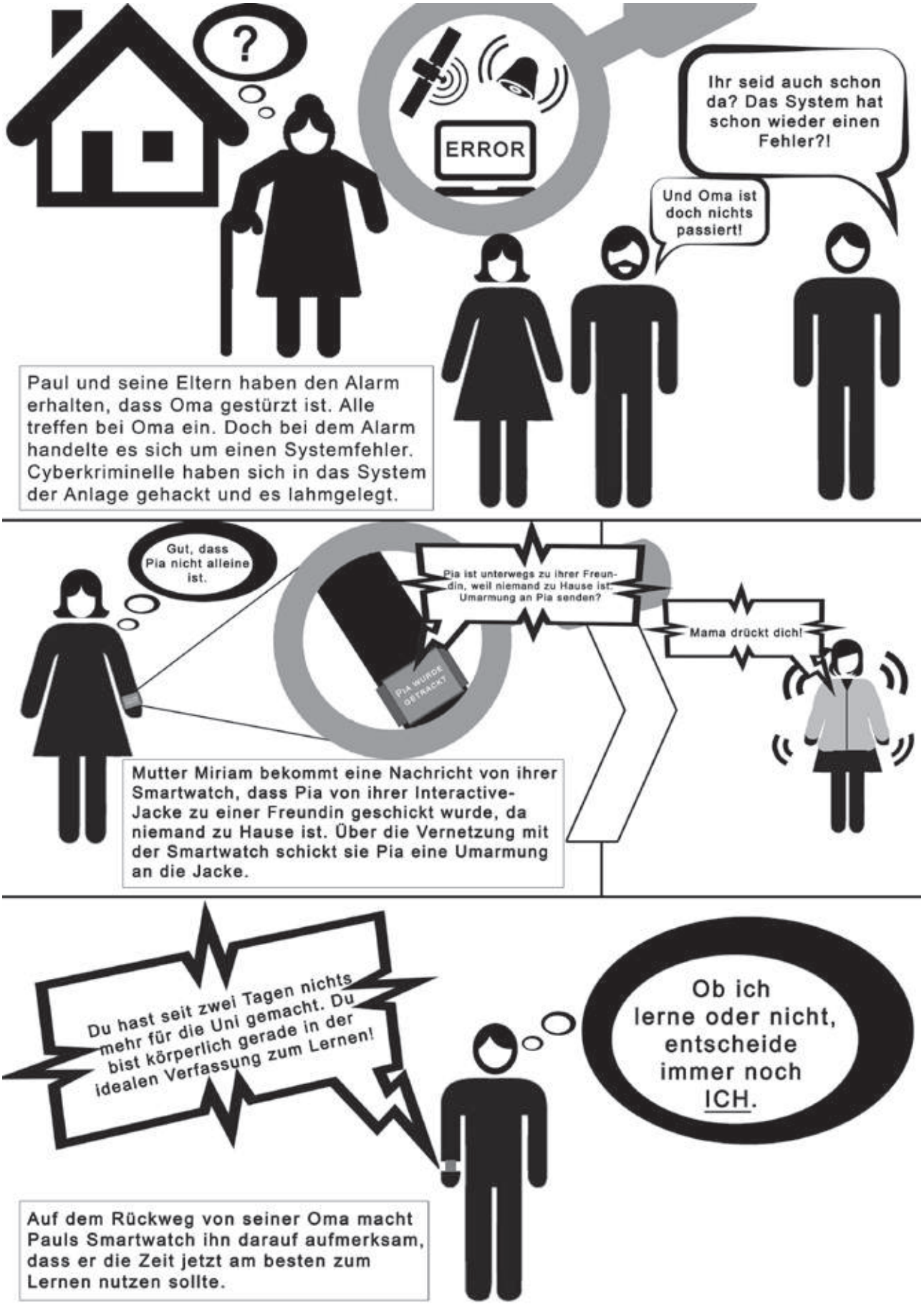


Am Nachmittag hat Paul frei und geht einkaufen. Er probiert ein T-Shirt an und kann es im Magic Mirror mit verschiedenen Mustern ausprobieren. Über soziale Medien fragt er seine Freunde, ob er das T-Shirt kaufen soll.

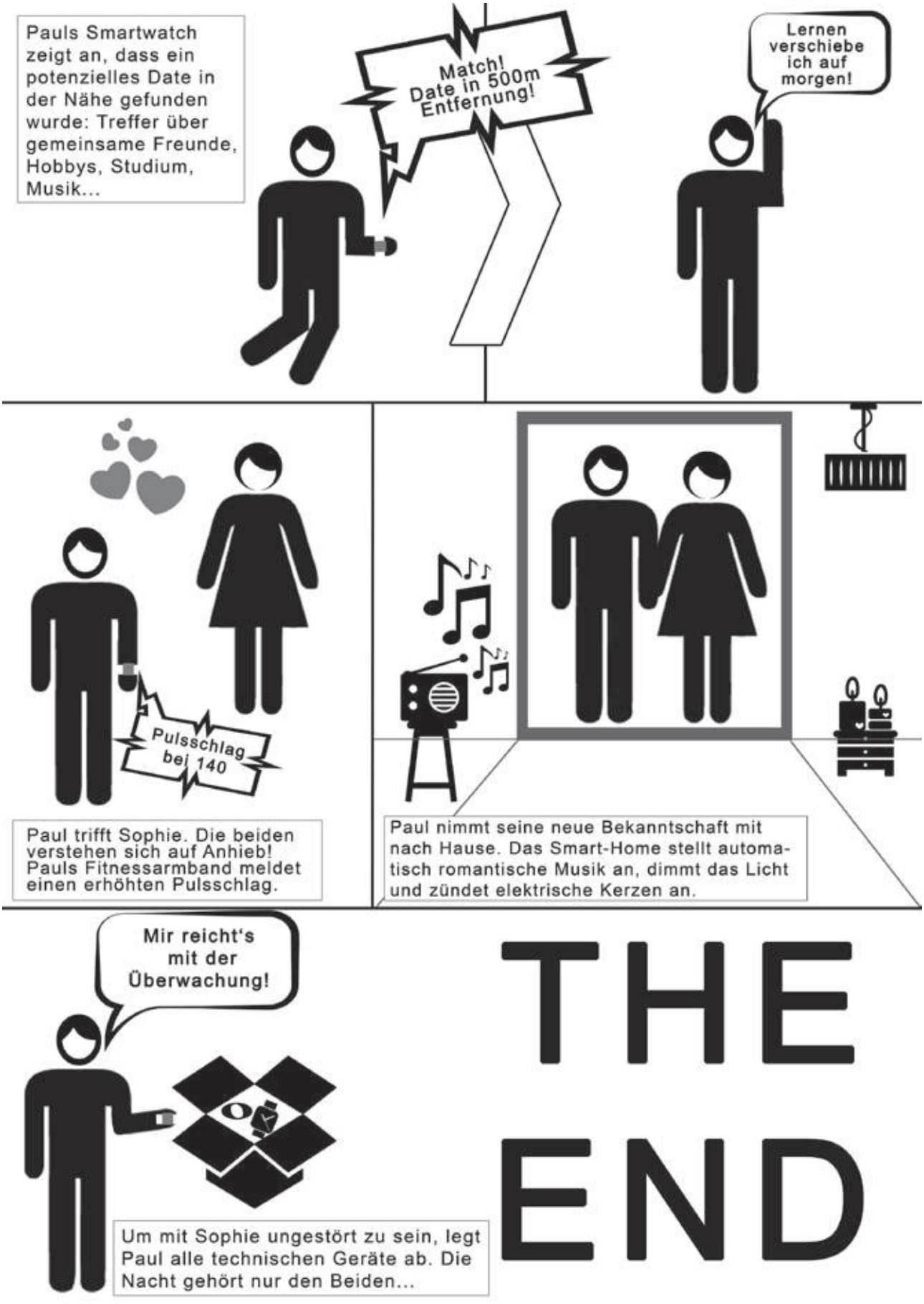


Beim Einkaufen wird Paul über seine Smartwatch darüber informiert, dass etwas mit seiner Oma nicht stimmt.

2_3 Internet der Dinge – Arbeitsblätter
Lösungsblatt



2_3 Internet der Dinge – Arbeitsblätter
Lösungsblatt



Internet der Dinge – Produktbeispiele

Kategorie 1: Fernbedienung via Netz

Good Night Lamp

Bei der „Good Night Lamp" handelt es sich um ein Set bestehend aus mehreren Lampen. Wird eine Lampe aktiviert, so aktivieren sich über die „Lightning"-Netzwerkverbindung automatisch auch andere Lampen, auch über große Distanzen hinweg. Per Smartphone-App können die Lampen aus der Ferne kontrolliert und gesteuert werden.



Tado

„Tado" ist ein Heizungsthermostat, das via Smartphone-App ferngesteuert werden kann. Im Automatikmodus übernimmt das Thermostat selbständig die Temperaturregelung, je nach dem, wie weit der Nutzer mit seinem Smartphone von seinem Haus entfernt ist.



Kategorie 2: Messung und Sammlung von Daten

Athos

„Athos" besteht aus einem Set an Fitnessbekleidung, in das Sensoren integriert werden können. Die Sensoren erfassen während des Trainings Daten zur Aktivität einzelner Muskelgruppen und der Pulsfrequenz des Trägers. Über die zugehörige Smartphone-App kann so der Trainingsfortschritt getrackt werden.



Mothers

„Mothers" besteht aus einem Set von kompakten Sensoren, die auf unterschiedliche Weise einsetzbar sind. So kann ein Kind bspw. einen Sensor an der Kleidung tragen. "Mothers" erkennt dann, wann das Kind das Haus betritt. Die gesammelten Daten können per Computer oder Mobile Device abgerufen und überprüft werden.



VeriChip

Der „VeriChip" ist ein RFID-Transponder, der unter die Haut implantiert wird. Wird der Chip auf der richtigen Frequenz angesprochen, antwortet er mit einer eindeutigen sechzehnstelligen Nummernfolge, die den Träger des Chips in einer Datenbank eindeutig identifiziert.



Kategorie 3: Profiling und Vorschläge

Koubachi

„Koubachi" ist ein Sensor, der in Pflanzkübeln angebracht wird. Er misst Feuchtigkeit und Dünger in der Erde sowie Temperatur- und Lichtverhältnisse. Aus den gesammelten Daten erstellt die „Koubachi"-App eine Pflegeanleitung und schlägt dem Nutzer vor, wie er seine Pflanzen am besten versorgen kann.



Connected Car von BMW und SAP

Hierbei handelt es sich um ein Forschungsprojekt von SAP in Zusammenarbeit mit BMW. Lokalitäten in der Umgebung des Fahrers stellen ihre Angebote per SAP Cloud zur Verfügung. BMW Connected Drive gleicht das Angebot mit den Nutzungspräferenzen des Fahrers ab und unterbreitet ihm Vorschläge. Dieser kann sich direkt zum gewünschten Ziel navigieren lassen.



Kategorie 4: Daten sammeln und Aktivität

The Dash

„The Dash" sind kabellose In-Ear-Kopfhörer. Beim Sport erfassen sie Körperfunktionen, wie etwa Pulsfrequenz und Körpertemperatur. Sollte sich bspw. die Herzfrequenz des Sportlers außerhalb des optimalen Bereichs bewegen, gibt das Gerät durch eine entsprechende Musikauswahl automatisch Feedback. Durch Musik mit mehr Beats per Minute wird er animiert, sich mehr anzustrengen bzw. umgekehrt, sich etwas mehr zu schonen. Daneben werden Daten zum Trainingsfortschritt erhoben.



Canary

„Canary" ist ein Gerät, das die Sicherheit zu Hause erhöhen soll. Die Sensoren umfassen eine HD-Kamera, Mikrofon, Thermometer, Bewegungsmelder sowie einen Beschleunigungssensor. Die Anlage kann per Smartphone scharf gestellt werden. Sie warnt dann automatisch, falls etwa die Temperatur im Haus rasant ansteigt. Im Falle eines Stromausfalls sendet „Canary" automatisch ein Video der letzten Sekunden vor dem Ausfall auf das Smartphone des Nutzers.



Kategorie 5: Daten suchen und Produktion

MakerBot

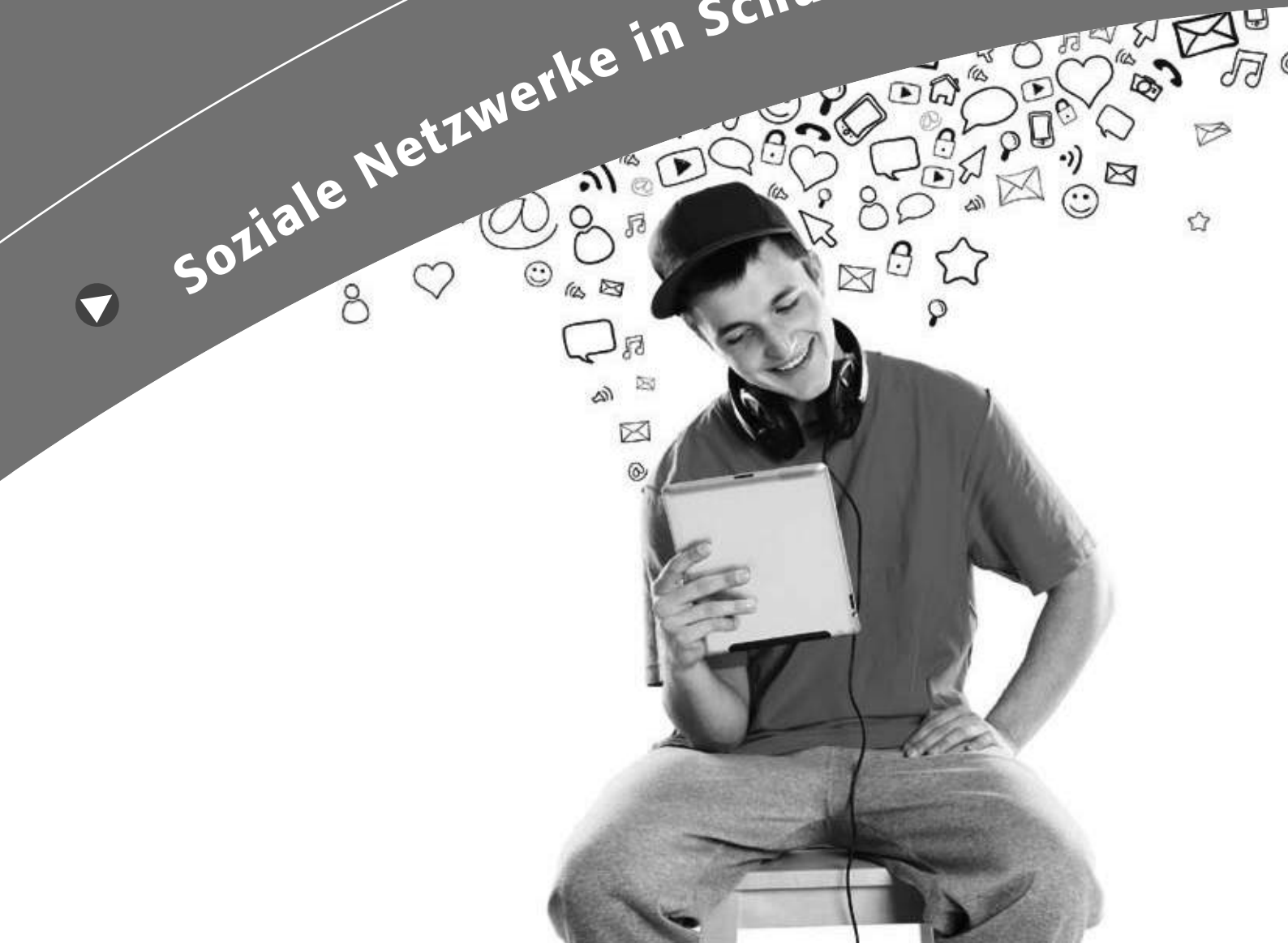
Der „MakerBot" ist ein 3D-Drucker, der auf dem Open-Source-Prinzip beruht. Sowohl die Software, als auch die Hardware des Druckers sind Open-Source-basiert. Das heißt, jeder Besitzer eines „MakerBot" kann mit diesem einen neuen „MakerBot" produzieren. Baupläne von selbst designten Objekten können im „MakerBot Thingiverse" für alle zugänglich geteilt werden.



3|1 Soziale Netzwerke
3|2 Schule und Arbeit

3

Soziale Netzwerke in Schule und Arbeit



Übersicht der Bausteine:

- **Soziale Netzwerke** | **Arbeitsblätter**
- **Schule und Arbeit** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Datenschutz_klicksafe.pdf

Soziale Netzwerke in Schule und Arbeit



Freunde

Freunde, Freunde, Freunde – was für eine Menge an „Freunden" hat man doch bei Facebook, WhatsApp, Instagram, Twitter, Snapchat und und und und. Dabei sollten „Freunde" doch etwas ganz Besonderes und Kostbares sein, oder? Hier sollst du darüber nachdenken, was ein Freund für dich ist.

Arbeitsaufträge:

1. Was ist ein Freund/eine Freundin? Findet euch z.B. in 4er-Gruppen zusammen. Überlege bitte zunächst alleine (vielleicht mithilfe eines „Placemats") und diskutiert danach in eurer Gruppe darüber. Stellt eure Ideen danach den anderen Gruppen vor!

2. Worin besteht der Unterschied zwischen „Freunden", „Kumpels" und „Bekannten"? Vergleiche sie und fülle folgende Tabelle aus:

Das würde ich mit ihnen tun/ihnen erzählen:	**Mit echten Freunden: „Freunde"**	**Mit anderen, die ich persönlich kenne: „Kumpels"**	**Mit Menschen, die ich nur aus dem Internet kenne: „Bekannte"**
A. Meine heimliche Liebe verraten			
B. Über den Streit mit meinen Eltern berichten			
C. Ins Kino gehen			
D. Einen Blick in das Tagebuch werfen lassen			
E. Meinen Spitznamen verraten			
F.			
G.			
H.			
I.			
J.			

3. Vergleicht eure Ergebnisse und sprecht darüber! Erstellt danach an der Tafel eine gemeinsame Tabelle!

3_1 Soziale Netzwerke – Arbeitsblätter methodisch-didaktische Hinweise

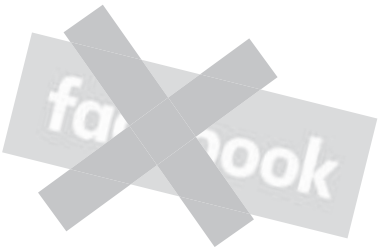
Arbeitsblatt	**AB 1** ▷●	**AB 2** ▷▷
Titel	**Facebook-Verbot für Laura**	**Welche Nutzungsmotive gibt es für Facebook?**
Kompetenzen	Die Schülerinnen und Schüler setzen sich in einem Rollenspiel mit den Vor- und Nachteilen von Social Communitys auseinander.	Die Schülerinnen und Schüler vergleichen Zitate zur Beschreibung von Facebook-Nutzungsmotiven und setzen sie in Bezug zu ihren eigenen Erfahrungen.
Methoden	Rollenspiel	Textarbeit, Stufenleiter
Material	Arbeitsblatt, Kärtchen	Arbeitsblatt
Zeit (in Minuten)	90 (evtl. länger)	45
Zugang Internet/PC	ja	nein

Hinweise für die Durchführung

AB 1: Facebook-Verbot für Laura	Die Schülerinnen und Schüler sollen in Form eines Rollenspiels die Vor- und Nachteile von Social Communitys wie Facebook diskutieren. Dazu nutzen sie in einem ersten Schritt die Stichworte aus der Tabelle, die einige Nutzungsmotive und Herausforderungen darstellen. Die fünf Rollen sollten etwa gleich groß besetzt sein. Wenn es innerhalb der Gruppe keine Einigung auf den „Rollenspieler" bzw. die „Rollenspielerin" gibt, sollten Sie den Zufall entscheiden lassen (dies aber vorher kommuniziert haben!). Wichtig bei dieser Methode ist die Reflexion im Anschluss, bei der alle Beteiligten ein methodisches und inhaltliches Feedback geben dürfen, aber auch die Distanzierung der Spieler von ihren Rollen ist enorm wichtig. Achten Sie darauf, dass die Spielerinnen und Spieler nicht „Ich" sagen, sondern „Die Mutter war der Meinung…" o. ä.
AB 2: Welche Nutzungsmotive gibt es für Facebook?	Einige Begriffe wie „Teilhabe" oder „Identitätsbildung" werden Sie erläutern müssen. Trotzdem bietet das Arbeitsblatt mit diesen sechs Zitaten einen guten und knappen Überblick über die Nutzungsmotive einer Social Community wie Facebook. Die Stufenleiter dient der eigenen Beurteilung der Motive und ihrer Gewichtung, der Zeitungsartikel im letzten Arbeitsauftrag soll eine kreative Form der Darstellung ermöglichen. Schülerinnen und Schüler, die selbst kein Facebook nutzen, übertragen die Aufgabe auf WhatsApp oder stellen sich vor, sie würden Facebook nutzen! **Quellenangaben:** [1] Schmidt, J-H. et al. (2010). *Heranwachsen mit dem Social Web.* Aufgerufen am 30.10.2014 unter http://www.hans-bredow-institut.de/de/node/2482 [2] mekonet kompakt. (2010). *Intimität im Netz auf einen Blick.* Aufgerufen am 30.10.2014 unter http://www.mekonet.de/t3/uploads/media/mekonet_kompakt_intimitaet-im-netz2012.pdf [3] Sloterdijk, P. (2009). *Fremde Freunde – Vom zweifelhaften Wert digitaler Beziehungen.* Der Spiegel, 10 [4] Wippermann, P. im Interview (k. A.). (2012, 1. Februar). *heute-Journal* [Nachrichtenmagazin]. Mainz: Zweites Deutsches Fernsehen. [5] Laird, S. (2012). *Why do People use Facebook?* [6] Bauer, J. (2010). *Interview-Titel „Lob der Schule"*

Lust auf mehr?
Beide Arbeitsblätter lassen sich mit wenigen Anpassungen auf weitere Angebote anwenden, so zum Beispiel auf Dienste wie Instagram, Snapchat, Ask.fm usw.

Facebook-Verbot für Laura!



„Oh je! Jetzt ist es passiert!“ stöhnt Laura morgens in der Schule in Richtung ihrer besten Freundin Zehra. „Meine Mutter verbietet mir Facebook! Die ist total unter schlechten Einfluss geraten und hat gestern so eine Fernsehsendung gesehen, wo Jugendliche als Kommunikationszombies auf Droge ‚Internet‘ dargestellt wurden! Dazu kam noch mein Onkel – der ist so voll der Datenschützer! Zehra tippt weiter auf ihrem Handy herum, während sie sagt: „So ein Unsinn! Mache ihr klar, wie sehr unser Bewusstsein erweitert und unsere Freundschaft durch Facebook vertieft wird!“ und muss dabei laut lachen.

Stelle dir vor, es kommt am Nachmittag zu einem Gespräch zwischen Laura, ihren Eltern, Zehra und dem Onkel.

Arbeitsaufträge:

1. Bitte teilt euch in etwa gleich große Gruppen auf:

Laura	Zehra	Mutter	Vater	Onkel

2. Überlegt euch innerhalb der Rollen, wie ihr sie spielen wollt.
   Erstellt euch eine kurze Rollenkarte, auf die ihr die grundlegende Meinung zur Facebook-Nutzung von Jugendlichen schreibt.
   Bei Mutter, Vater und Onkel dürft ihr euch Vornamen und Berufe ausdenken, bei Laura und Zehra könnt ihr Hobbies / Lieblingsbeschäftigungen notieren.

3. Erstellt euch neun Kärtchen zu folgenden Stichworten. Notiert darauf, was es bei jedem Stichwort Positives und Negatives zu sagen gibt (nur so könnt ihr in der Diskussion auf diese Argumente reagieren!). Dazu müsst ihr vielleicht einige der Themen noch genau im Internet nachschauen.

Dabei sein wollen / Gruppenzwang	Der LIKE-Button und Kommentare	Cyber-Mobbing (zum Beispiel Beleidigungen)
Weitergabe persönlicher Daten / Sicherheitseinstellungen	Freunde und Freundschaften	Unterhaltung und Freizeitbeschäftigungen
Chronik mit privaten Fotos	Kommunikation mit den Klassenkameraden	Werbung auf Facebook

4. Wählt in der Gruppe eine Person aus, die die Rolle spielt (dabei ist es egal, ob Junge oder Mädchen). Führt das Rollenspiel durch!

5. Bitte macht danach unbedingt eine Runde, bei der jede Rolle sagen darf, wie sie sich gefühlt hat und das Publikum sagen kann, ob das Spiel realistisch war.

6. Wertet das Spiel danach aus: Welche Argumente wurden gebracht?
   Wie wurde Facebook dargestellt? Was ist das Schöne daran?
   Was ist problematisch für Jugendliche an Facebook?

Welche Nutzungsmotive gibt es für facebook ?

Jan-Hinrik Schmidt[1]:
Soziale Netzwerke werden vor allem aus folgenden Gründen genutzt:
- Selbstdarstellung
- Teilhabe und Beziehungspflege durch Vernetzung

Mekonet[2]:
Der „Nutzen- und Belohnungsansatz": Medien werden zur Befriedigung von Wünschen und Bedürfnissen genutzt, nach:
- Unterhaltung
- Orientierung, Identitätsbildung
- Teilhabe, Zugehörigkeit und Soziale Unterstützung
- Selbstdarstellung und Anerkennung

Sam Laird[5]:
Wir alle wollen ein Teil von etwas sein!

Peter Sloterdijk[3]:
„Der Rückzug von den anderen, das Alleinseindürfen, das ist eine große Errungenschaft. Aber der Mensch ist auch ein Stammeswesen. Diese Netzwerke können beides glücklich vereinen: Man bleibt vom lästigen, vom aufsässigen anderen verschont, und doch ist der ganze Stamm immer anwesend."

Peter Wippermann[4]:
„Es dreht sich um mediales „Kraulen". Nicht was ich jemandem erzähle ist wichtig, sondern dass ich etwas erzähle ... dass ich noch wahrgenommen werde von meiner Umwelt"

Joachim Bauer[6]:
Menschen haben Bedeutungshunger.

Arbeitsaufträge:

1. Ihr dürft in Partnerarbeit arbeiten. Bitte erklärt euch gegenseitig kurz die sechs Aussagen der sechs Autoren. Belegt sie mit eigenen Beispielen!

2. Übertrage – zunächst alleine – die drei (für dich!) wichtigsten Aussagen in eine Stufenleiter, wobei das Wichtigste oben steht. Erklärt euch dann gegenseitig warum diese Nutzungsmotive so wichtig sind!

3. Macht eine kurze Umfrage in der Klasse und erstellt eine Übersicht an der Tafel: Welches der Motive ist für die meisten am wichtigsten / am unwichtigsten?

4. Diskutiert diese Übersicht in der Klasse!

5. Weshalb nutzen über eine Milliarde Menschen Facebook? Kläre das Phänomen mit eigenen Worten in Form eines Zeitungsartikels über Facebook und baue (wenn es passt) die Nutzungsmotive der Autoren ein.
Hast du noch eigene Gründe (= Nutzungsmotive), die noch nicht genannt wurden? Wenn ja, erkläre sie bitte!

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Broadcast yourself**	**Google, Google, Google**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Möglichkeiten von YouTube für das schulische Lernen.	Die Schülerinnen und Schüler ermitteln die kostenlosen Angebote des Google-Konzerns und hinterfragen sie kritisch auf Finanzierung und Datenschutz.
Methoden	Video-Analyse, Präsentation	Internet-Recherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Broadcast yourself	YouTube ist eine unter Pädagogen manchmal unterschätzte Möglichkeit für das schulische Lernen. Zu sehr vielen Unterrichtsthemen gibt es sehr gute Erklär-Videos, die von engagierten Menschen, oftmals auch Lehrerinnen und Lehrern, hergestellt und (kostenlos) veröffentlicht werden. Ein Blick lohnt sich also. Aber… wie immer bei der Fülle im Netz, muss hier der kritische Blick bleiben und eine Video-Analyse, vor allem auch inhaltlich zur Überprüfung der Richtigkeit der Informationen, ist notwendig. Nach der Pflicht könnten Sie eine Kür einbauen und die Schülerinnen und Schüler selbst ein Erklär-Video erstellen lassen. Die Technik ist über die Kameras und Schnitt-Möglichkeiten in den Schüler-Handys sowie YouTube-interne Schnittmöglichkeiten vorhanden.
AB 2: Google, Google, Google	Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler einen Blick hinter die Kulissen von Google werfen. Vielleicht aktualisieren Sie die vorhandene Liste mit einem Blick auf die Google-Seiten, denn der Konzern ist eine dynamische Technologie-Firma mit immer neuen Ideen. Über all diesen Angeboten steht immer wieder die Frage, wie sie kostenlos sein können und gleichzeitig für Google so gewinnbringend. Dazu dienen die Fragen, die in der Präsentation beantwortet werden sollen. Gleichzeitig sollen die Fragen eine rein technische und vielleicht allzu unkritische Darstellung verhindern.

Lust auf mehr?

- YouTuber als Berufsmodell? Wie man mit YouTube Geld verdienen kann erfahren die Schüler in dem Video des hauptberuflichen TechChanel-YouTubers Felix Bahlinger (Chanel Felixba):
  www.youtube.com/watch?v=eCLvx-KfVZw
  Sammlung: Welche problematischen Aspekte werden genannt?
- Themenspecial über YouTube und Kommerzialisierung unter
  www.klicksafe.de/themen/kommunizieren/youtube/
- Google arbeitet ständig an neuen Produkten und gibt dies auf der Seite
  http://research.google.com/ bekannt. Hier könnten die Schülerinnen und Schüler weiterarbeiten und einen Blick in die Zukunft werfen.

Broadcast yourself

Bestimmt kennt ihr das Videoportal YouTube und andere Portale wie MyVideo, Daily Motion, Vimeo oder Clipfish. Aber wusstet ihr, dass ihr diese Videoportale auch für die Schule nutzen könnt?

Arbeitsaufträge:

1. Partnerarbeit: Sucht euch zwei Videos aus, die euch interessieren, und schaut sie euch an.

- Geschichte/Kleinstaaten in Europa:
  http://tinyurl.com/7cup9lc
- Biologie/Mendelsche Regeln:
  http://tinyurl.com/nqua5xj
- Sport/Parcours im Sportunterricht:
  http://tinyurl.com/cjq62rl
- Hauswirtschaft/Stricken lernen:
  http://tinyurl.com/yz467rl
- Mathe/Winkel messen und zeichnen:
  http://tinyurl.com/ck65l4d
- Musik/Gitarre lernen:
  http://tinyurl.com/cjxncsj
- Erste Hilfe:
  http://tinyurl.com/nmzkn25
- ITG/Computer: Einrichten von Lesezeichen am Beispiel des Browsers Mozilla Firefox:
  http://tinyurl.com/c2fywg3
- Und noch etwas Witziges:
  http://tinyurl.com/cfucxhr
  http://tinyurl.com/63427z

2. Sucht nach folgenden Fragen. Findet ihr Erklärungen auf YouTube?
   a) Was ist der Satz des Pythagoras?
   b) Wie ist das Herz des Menschen aufgebaut?
   c) Wie wird das Past Perfect Simple im Englischen gebildet?
   d) Wie wird das Komma bei Aufzählungen gesetzt?

Projektvorschlag:
Produziert selbst in Gruppen ein Lernvideo und stellt es den anderen Schülern zur Verfügung. Ihr könnt es auch bei YouTube online stellen. Dann müsst ihr aber auf folgende Dinge achten:

- die Bildrechte der Beteiligten (haben alle, die im Video vorkommen, ihr Einverständnis und ggf. das der Eltern gegeben?)
- ein sinnvolles Tagging (die Auswahl von Begriffen, die den Inhalt eurer Videos beschreiben, damit sie über die Suchfunktion zu finden sind)
- überlegt euch, ob ihr das Video unter Creative-Commons-Lizenz veröffentlichen wollt – Informationen über Creative Commons: **http://de.creativecommons.org/**

Google, Google, Google

Schon längst ist Google viel mehr als eine einfache Suchmaschine. Der Konzern **Google Incorporated** mit Sitz in Kalifornien wurde 1998 von Larry Page und Sergey Brin gegründet und hat sich seitdem zu einem weltweiten Motor für Internet-Technologien entwickelt.

Hier kannst du Google etwas besser kennenlernen … und auch einen kritischen Blick auf das Unternehmen werfen.

Arbeitsaufträge:

1. Google hat zahllose Anwendungen entwickelt, die in der Regel kostenlos für den Nutzer sind. Bitte sucht euch jeweils zu zweit eine Google-Anwendung aus und recherchiert dazu.

Suchmaschine Google	Google Chrome	Google Maps	Gmail
YouTube	Google+	Google Books	Google Earth
Google Alerts	Google Kalender	Google Docs	Google Übersetzer
Hangouts	Google Groups	Google Keep	?
?	?	?	?

Bei den Fragezeichen in der Liste könnt ihr ein Produkt auswählen, das noch nicht genannt wurde. Die Produkte findet ihr unter: **www.google.de/intl/de/about/products**

2. Erstellt eine kurze Präsentation für die anderen und beantwortet darin folgende Fragen: Ist diese Anwendung kostenlos? Wenn nein, wie teuer ist sie? Wenn ja, wird Werbung eingeblendet?

   a) Wozu dient die Anwendung?

   b) Ist sie kostenlos? (Wenn nein, wie teuer ist sie?)

   c) Wie wird sie finanziert?

   d) Ist eine Anmeldung mit persönlichen Daten notwendig? (Wenn ja, mit welchen?)

   e) Was erfährt Google über mich bei der Nutzung?

3. Google verlangt von seinen Nutzern, ein Konto einzurichten, das dann für alle Anwendungen genutzt werden kann. Macht folgendes Gedankenexperiment: Willi ist ein Google-Fan und nutzt fast ausschließlich Google-Anwendungen. Erstellt – zunächst in Partnerarbeit, dann an der Tafel – eine Liste mit Daten, die Google möglicherweise über Willi erfahren kann.

4. Diskutiert in der Klasse die Frage, welche Macht Google dadurch erlangt und inwieweit dies problematisch sein könnte.

Tipp:
Es gibt Alternativen zu Suchmaschinen mit Datenhunger: Zum Beispiel Startpage:
https://startpage.com/deu/
und DuckDuckGo
https://duckduckgo.com/

3_1 Soziale Netzwerke – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Zwitschern mit Larry**	**Twitter für Newbies**
Kompetenzen	Die Schülerinnen und Schüler beschreiben eine Statistik zur Nutzung von Twitter aus der JIM-Studie und ermitteln im Gespräch die Unterschiede zur Nutzung bei Jugendlichen und Erwachsenen.	Die Schülerinnen und Schüler übertragen die Tabelle mit typischen Begriffen zur Benutzung von Twitter auf Plakate.
Methoden	Statistik-Analyse	Museumsgang
Material	Arbeitsblatt	Arbeitsblatt, Plakate (mind. DIN A3), dicke Stifte
Zeit (in Minuten)	45	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Zwitschern mit Larry	Twitter ist noch immer ein Erwachsenen-Phänomen, was sich aber leicht ändern kann. Die Schülerinnen und Schüler sollen hier Zahlen zur Nutzung von Twitter bei Jugendlichen kennenlernen und auswerten. In einem zweiten Schritt soll analysiert werden, warum bislang Erwachsene Twitter eher nutzen als Jugendliche. Die Twitter-Integration der Live-Stream-App Periscope ist für jugendliche Nutzer wahrscheinlich interessant. Über Periscope können Nutzer ihr Smartphone dazu nutzen, um selbst Live-Videoaufnahmen direkt ins Netz zu streamen. Über Vor- und Nachteile soll nach einer kurzen Internet-Recherche diskutiert werden. Abschließend haben die Schüler, die Twitter nutzen, die Möglichkeit, Lieblings-Hashtags oder Lieblings-Twitterer vorzustellen.
AB 2: Twitter für Newbies	Dieses Arbeitsblatt ist im Prinzip eine Fleiß-Recherchearbeit zu Twitter und den wichtigsten Begriffen rund um dieses Angebot. Vielleicht lassen Sie die Schülerinnen und Schüler selbst aus den sechs Möglichkeiten wählen und steigern so die Motivation. Die Methode Museumsgang beinhaltet, dass die Plakate alle in einem Raum aufgehängt werden. Der Präsentator / die Präsentatorin der jeweiligen Gruppe steht vor dem Plakat und erläutert – wie ein Museums-führer – das Plakat.

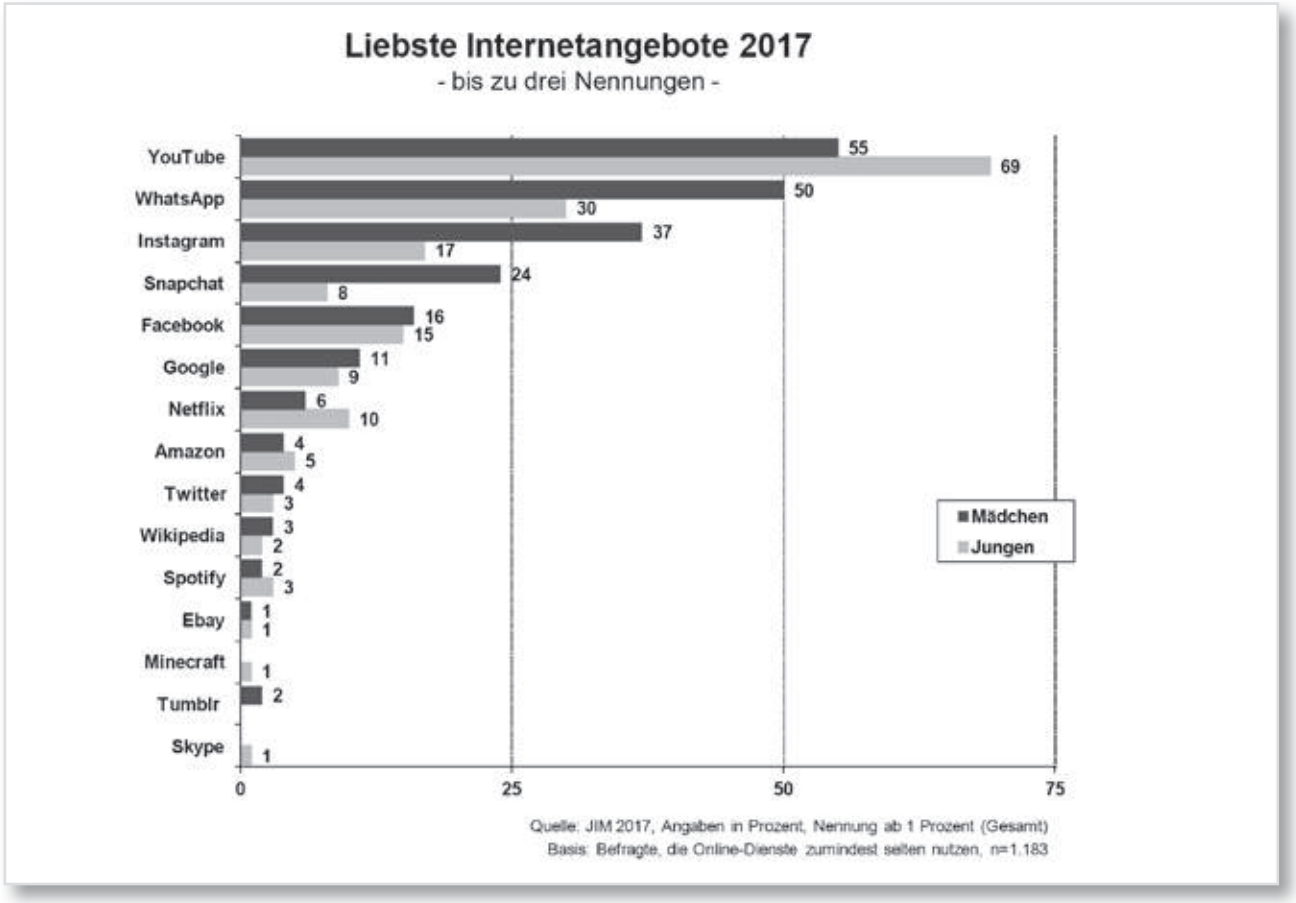
Lust auf mehr?

Die Zahlen rund um die Angebote wie Twitter werden auch immer in Form von nett aufbereiteten Statistiken dargeboten. Schauen Sie doch mal unter „Internet-Minute" in einer Bildersuche (bei Google oder Bing bspw.) nach. Hier könnten die Schülerinnen und Schüler die Zahlen überprüfen oder selbst eine ähnliche Darstellung anfertigen.

Zwitschern mit Larry

Jeder kennt den kleinen blauen Vogel, doch kaum einer weiß, dass er „Larry" heißt und seinen Namen dem ehemaligen Basketballspieler Larry Bird verdankt. Die Rede ist natürlich von dem Symbol des Dienstes **Twitter,** der 2006 gegründet wurde. Der Name Twitter kommt von dem englischen Verb „to twitter", das im Deutschen mit „zwitschern" übersetzt wird.

Unter deutschen Jugendlichen ist Twitter noch nicht so verbreitet, wie folgende Statistik aus der JIM-Studie 2015 zeigt:



MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.). (2017).
JIM-Studie 2017, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.

Arbeitsaufträge:

1. Bitte beschreibt das Diagramm aus der JIM-Studie möglichst genau. Fasst die wichtigsten Ergebnisse zusammen!
2. Unter Erwachsenen ist Twitter beliebt. Warum nicht auch bei Jugendlichen? Notiert Ideen dazu an der Tafel und diskutiert sie. Könnt ihr hier zustimmen?
3. Über die Live-Stream-App Periscope können Twitter-Nutzer Live Streams senden und empfangen. Informiert euch über Vor- und Nachteile dieser Anwendung.
4. Kennt ihr Twitterer oder auch Hashtags #, die ihr besonders toll findet? Stellt sie den anderen vor.

Twitter für Newbies

Twittern gehört unter Prominenten mittlerweile zum guten Ton. Viele Fußballspieler der deutschen Nationalelf twittern, viele Schauspieler und Politiker ebenso. Insgesamt hat Twitter etwas über 300 Millionen aktive Nutzer (Stand: 2015), die ihre Nachrichten verbreiten oder solche empfangen.

Hier kannst du Twitter etwas besser kennenlernen.

Arbeitsaufträge:

1. Bitte sucht euch mithilfe der Leitfragen und Arbeitsaufträge eines der folgenden Themen aus. Ihr dürft ganz nach Eurem Interesse auswählen!

2. Stellt das Thema auf einem Plakat dar!

	Begriffe	Beliebtheit	AGB	Datenschutz	Twitaholics	Politik
Leitfragen	Was bedeutet „Tweet", „Hashtag" und die anderen Twitter-Begriffe.	Wer nutzt Twitter und wie oft?	Was steht unter „Ihre Rechte" in den Allgemeinen Geschäftsbedingungen?	Welche Daten speichert Twitter über mich? Was sind „Geotags"?	Wer sind die fleißigsten Twitterer mit den meisten Followern?	Wann und für wen spielte Twitter eine große politische Rolle?
Arbeitsaufträge	Erstellt ein kleines Twitter-Glossar!	Recherchiert die aktuellen Nutzungszahlen und stellt sie anschaulich dar!	Stellt die Nutzungsbedingungen mit eigenen Worten kurz dar!	Fasst die Ergebnisse in einer Liste zusammen und erklärt sie!	Erstellt eine Auflistung mit maximal 10 Namen!	Nehmt zwei Ereignisse der letzten Jahre und zeigt die Bedeutung von Twitter!

3. Bereitet euch in der Gruppe auf einen **Museumsgang** vor. Dabei hängen alle Plakate im Klassenraum. Alle dürfen reihum die Plakate besuchen und die Erläuterungen hören (wechselt euch an eurem Plakat ab, jeder soll mindestens einmal erläutern!).

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Falschmeldungen – nicht immer harmlos**	**Shitstorm**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Strukturmerkmale von Falschmeldungen, die als „Hoaxes" bekannt sind.	Die Schülerinnen und Schüler erkennen Merkmale des Internet-Phänomens „Shitstorm" und Möglichkeiten der Bewertung. Sie beurteilen die Legitimität solcher Aktionen.
Methoden	Gruppenarbeit, versch. Präsentationsmöglichkeiten	Gruppenarbeit, Internet-Recherche, Mind-Map
Material	Arbeitsblatt (je nach Präsentationsform versch. Materialien wie Papier, Stifte, Kleber)	Arbeitsblatt, (evtl. großes Papier für große Mind-Map)
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Falschmeldungen – nicht immer harmlos	Hoaxes laden für den aufgeklärten Betrachter oft zum Schmunzeln ein, trotzdem darf man ihre Bedeutung nicht unterschätzen. Die Schülerinnen und Schüler sollen hier einige der modernen Sagen („urban legends") aus dem Internet unter dem Begriff der „Hoaxes" kennenlernen und sich mithilfe der Internet-Adresse der Technischen Universität Berlin über den aktuellen Stand informieren. Hier könnten Sie eine Phase einbauen, in der die Schülerinnen und Schüler über ihre eigenen Erfahrungen berichten, aber auch über ihre Ängste sprechen können. Gerade jüngere Schülerinnen/Schüler können von bspw. Gewaltandrohung sehr verängstigt sein. Wie immer bei diesen Themen gilt es, sensibel zu reagieren. Mit dem letzten Arbeitsauftrag sollen die Schülerinnen und Schüler ihre Erkenntnisse kreativ umsetzen und damit das Gelernte festigen.
AB 2: Shitstorm	Sascha Lobo bezeichnet sich selbst als Autor, Blogger, Microblogger und Strategieberater und ist vielfach in den Neuen (wie auch in den alten) Medien präsent. Seine Definition eines Shitstorms ist nicht wissenschaftlich, kennzeichnet aber trotzdem sehr anschaulich das Phänomen. Auf der Grundlage der Beaufort-Skala zur Einteilung von Windstärken (die den Erdkunde-Kolleginnen und -Kollegen geläufig sein dürfte) versuchen Schwede und Graf eine Einteilung der Shitstorms. Hier dürfen Sie sehr leistungsstarke Schülerinnen und Schüler gerne zum kritischen Hinter-fragen einer solchen Einteilung auffordern. Sie soll dazu dienen, den Shitstorm nicht pauschal zu verurteilen, sondern auch qualitativ zu bewerten. In der Mindmap sollen die Schülerinnen und Schüler ihre Erkenntnisse darstellen und sie sich gegenseitig präsentieren. Im letzten Arbeitsauftrag gehen die Schülerinnen und Schüler noch einen Schritt weiter mit der Frage, ob ein Shitstorm nicht auch positive Seiten haben kann, zum Beispiel als demokratisches Instrument der Meinungsäußerung. **Quellen** Definition: Lobo, S. (2012, 21. April). *How to survive a shitstorm* [Video]. Aufgerufen am 02.12.2014 unter ⓘ **https://www.youtube.com/watch?v=-OzJdA-JY84** **Bildquelle:** „Sascha Lobo" von Matthias Bauer (flickr: Matthias Bauer) - originally posted to Flickr as Sascha Lobo. Lizenziert unter CC BY-SA 2.0 über Wikimedia Commons - ⓘ **https://commons.wikimedia.org/wiki/File:Sascha_Lobo.jpg#/media/File:Sascha_Lobo.jpg**

Lust auf mehr?
Moderne Mythen oder urban legends sind ein schier unerschöpfliches Thema, das sich im Internet kongenial unterbringen lässt. Dazu gehören ganze Gebilde von Verschwörungstheorien, die früher in Büchern und Zeitschriften nur ein kleines Publikum fanden, nun aber weltweit ausgebreitet werden.
Für historisch interessierte Schülerinnen und Schüler könnte als Beispiel hier die These von der „Nicht-Mondlandung" der Amerikaner kritisch hinterfragt werden.

Falschmeldungen – nicht immer harmlos

Hoaxes nennen Experten die vielen Falschmeldungen, die im Internet kursieren. Beliebte Hoaxes sind u. a.:

- Personen mit bestimmte Blutgruppe für einen Leukämie-Kranken gesucht
- Vorsicht! Handy explodiert beim Aufladen!
- Spritzen-Nadeln von HIV-Infizierten im Kinositz versteckt!
- Die Flugnummer Q33NY einer der Maschinen, die am 11.09.2011 ins World Trade Center flog, ergibt in der Schriftart **Wingdings** folgende Botschaft:

Q33NY

▽

Wingdings

▽



Quelle: The Museum of Hoaxes (www.hoaxes.org)

Die meisten Hoaxes sind schlicht witzig oder nervig. Einige jedoch spielen ganz bewusst mit Emotionen wie der Angst vor Tod oder Krankheit, Rachegefühlen etc. Unter folgender Adresse kannst du eine ständig aktualisierte Liste von Hoaxes finden, die von der Technischen Universität Berlin betreut wird:
http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Arbeitsaufträge:

1. Teilt euch in 4er-Gruppen auf. Zwei von euch informieren sich über Hoaxes allgemein. Die anderen beiden informieren sich über Kettenbriefe, die per E-Mail, über Soziale Netzwerke oder Messenger-Apps verschickt werden. Sucht jeweils 2-3 Beispiele heraus, die ihr besonders interessant findet.

2. Tauscht euch in der Gruppe aus und stellt euch die Ergebnisse gegenseitig vor!

3. Denkt gemeinsam darüber nach, warum diese Hoaxes und Kettenbriefe in Umlauf gebracht werden und welche Folgen sie haben können.

4. Überlegt und recherchiert, wie man sich schützen kann! Erstellt Tipps zum Schutz für jüngere SchülerInnen. Ihr dürft eine der folgenden Präsentationsformen wählen:

   A einen Aufkleber
   B max. zehn einfache Sätze
   C ein Symbol / Piktogramm
   D ein Werbeplakat
   E einen Reim / ein Gedicht
   F ein Maus-Pad

Shitstorm

„Als Shitstorm wird ein Internet-Phänomen bezeichnet, bei dem innerhalb eines kurzen Zeitraums eine subjektiv große Anzahl kritischer Äußerungen getätigt wird, von denen sich zumindest ein Teil vom ursprünglichen Thema entfernt und stattdessen aggressiv, beleidigend oder bedrohend sind"

(nach Sascha Lobo, 2012).



Foto: Matthias Bauer

Die Wissenschaftler Barbara Schwede und Daniel Graf versuchten gar eine Skala zu beschreiben für die Stärke eines Shitstorms: Von 0 (keine kritischen Rückmeldungen) über 4 (Herausbildung einer vernetzten Protestgruppe. Wachsendes, aktives Follower-Publikum auf allen Kanälen) bis Stufe 6 (ungebremster Schneeball-Effekt mit aufgepeitschtem Publikum. Tonfall mehrheitlich aggressiv, beleidigend, bedrohend.).

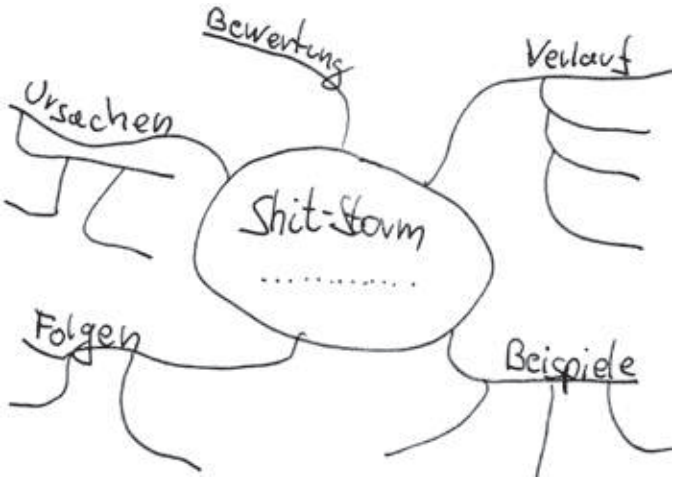
Arbeitsaufträge:

1. Informiert euch über einen Shitstorm aus dem vergangenen Jahr. Versucht herauszufinden, warum und wie er entstanden ist, wie er verlaufen ist was die Folgen waren. Versucht, den ausgewählten Shitstorm in der Skala von Schwede und Graf zu verorten. Diese ist zu finden unter

   ① **http://www.barbaraschwede.ch/blog.html** bzw.

   ① **http://tinyurl.com/038ug8g**

2. Stellt eure Ergebnisse in Form einer Mind-Map dar:



3. Shitstorms können auf der einen Seite für Einzelpersonen, Unternehmen, Verbände etc. problematisch sein und sie schädigen. Auf der anderen Seite können Shitstorms durch ihr Machtpotenzial auf Missstände hinweisen und sogar darauf hinwirken, diese zu beheben. Diskutiert diese zwei Seiten eines Shitstorms in der Klasse. Versucht, Regeln aufzustellen, wann ein Shitstorm in Ordnung wäre.



3_2 Arbeit und Schule – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 6**
Thema	**Motive von Jugendlichen**
Zeitangabe (Unterrichtsstunden à 45 min.)	1
Ziele	Mit der Methode „Strukturierte Kontroverse“ sollen die Schülerinnen und Schüler darüber reflektieren, warum Jugendliche viele Daten (leichtsinnig) veröffentlichen.
Methodische Hinweise	Für Jugendliche im Internet-Zeitalter reicht es nicht aus, die gesetzlichen Regelungen und die Gefahren von Missbrauch zu kennen. Viele breiten ihre Daten freiwillig vor einer Öffentlichkeit aus, von einer „Datenaskese zu einer Datenekstase“, wie ein Journalist mal schrieb. Hier geht es um die Gründe, die naturgemäß sehr individuell sein können. Trotzdem gibt es immer wiederkehrende Motive (s. Sachinformationen), die aufgearbeitet und reflektiert werden sollten. In der Studie „Heranwachsen mit dem Social Web“ der Landesanstalt für Medien NRW werden folgende Schlagworte bei den Gründen für die Nutzung genannt: ■ Selbstdarstellung ■ Partizipation ■ Vernetzung ■ Beziehungspflege Sicherlich lassen sich viele der Antworten von Schülerinnen und Schülern hier einordnen. Mit der Methode „Strukturiere Kontroverse“ (darin übernehmen Schülerinnen und Schüler abwechselnd auch die Gegen-Positionen) sollen sie, in Form eines Rollenwechsels, die Gründe dafür und dagegen nicht nur kennen, sondern auch argumentativ vertreten.
Methoden und Material	Arbeitsblatt, Strukturierte Kontroverse
Organisationsformen	Einzelarbeit, Gruppenarbeit
Zugang Internet / PC	nein

Arbeitsblatt	**AB 7**
Thema	**Karrierebremse Internet**
Zeitangabe (Unterrichtsstunden à 45 min.)	2
Ziele	Die Schülerinnen und Schüler sollen eine eigene Personensuche im Internet und durch ein Rollenspiel zum Thema „Private Daten im Internet und Bewerbung“ durchführen. Dadurch sollen sie zu einer kritischen Auseinandersetzung darüber kommen.
Methodische Hinweise	Das „Googlen“ der eigenen Person bzw. die Eingabe des eigenen Namens in die bekannten Personen-Suchmaschinen (s. Arbeitsblatt) birgt gewisse Risiken durch ein unvorhersagbares Ergebnis. Auf jeden Fall sollten Sie als Lehrkraft dies vorher für Ihren Namen gemacht haben, denn sicherlich kommen Schülerinnen und Schüler auf diese Idee. Ein Tipp, den man aus Sicht des Datenschutzes geben kann, ist, solch eine Eigen-Recherche regelmäßig durchzuführen. Legen Sie sich ein Handlungsmuster zurecht, falls es bei der Recherche durch Schülerinnen und Schüler zu negativen Ergebnissen kommt (Was tun, wenn man ein blödes Bild von sich findet?). In den Sachinformationen und auf dem Arbeitsblatt Nr. 9 finden Sie Hinweise dazu. Alternativ ist im ersten Arbeitsauftrag angegeben, die Suche mit einem Prominenten-Namen durchzuführen. An dieser Stelle sollen die Schülerinnen und Schüler diese Möglichkeiten der Suche lediglich kennenlernen und ausprobieren können. Eine Reflexion findet mit dem zweiten Arbeitsauftrag statt. Das Rollenspiel schließlich problematisiert den Umgang mit Daten im Internet und der Tatsache, dass diese Daten auch bei einer Bewerbung um einen Job eine Rolle spielen könnten. Denken Sie beim Rollenspiel an folgende Phasen:

Geht das? Ein Tag ohne Datenspuren?

Der Wecker klingelt. Es ist 6:45 Uhr. Zeit zum Aufstehen, aber da war doch was? Mein Gehirn arbeitet fieberhaft und kämpft gegen den letzten Traum und den Wunsch weiterzuschlafen … ach ja … heute ist der Tag, an dem ich keine Datenspuren hinterlassen möchte. Ich stehe auf. Darf ich das Radio einschalten? Ja, denn niemand erfährt, ob ich es eingeschaltet habe. Darf ich Kaffee kochen? Ja, ein Glück! Ich möchte gerne meine E-Mails abrufen vor dem Gang ins Büro, aber … das darf ich heute nicht, denn mein Login ins Internet wird von meinem Anbieter protokolliert mit Uhrzeit und der Nummer des Computers, der IP-Nummer. Also los, auf ins feindliche Leben draußen. Ach … M i s t … ich darf das Auto nicht benutzen! Das hatte ich ganz vergessen. Dann werde ich zu spät kommen. Auf den Straßen gibt es Überwachungskameras für den Verkehr und ich möchte ja heute keine Datenspuren in Form von Videos hinterlassen. Und außerdem sendet das Auto ja über die Blackbox Infos über mein Fahrverhalten an meine Kfz-Versicherung. Ich hätte auch nicht auf die Autobahn fahren dürfen – unter Mautbrücken werden die Nummernschilder fotografiert, von jedem Auto! Und das Auto selbst erfasst auch eine ganze Menge Informationen. Ich schleiche mich also mit meinem Fahrrad aus dem Haus. Am Bahnhof darf ich nicht vorbeifahren, dort hängt eine Kamera. Endlich im Büro darf ich die Zeitstempeluhr nicht benutzen (Datenspuren, wann ich wo war!), ich sage später, ich hätte es vergessen.
Den Computer darf ich anmachen … oder? Nein, besser nicht, denn auch dort gibt es Protokolldateien im Netzwerk der Firma. Darf ich telefonieren? Auch nicht … M I S T … natürlich weiß die Telefongesellschaft, von welchem Apparat aus wohin wann und wie lange angerufen wird! Mein Handy? SMS? Keine Chance! Derselbe Datenspeicherwahn. Besser, ich melde mich sofort krank, denn arbeiten kann ich sowieso nicht. Ich schleiche also wieder zurück nach Hause, mit Angst davor, gefilmt zu werden. Eigentlich wollte ich noch einkaufen, aber … Kameras in jedem Laden … ich bräuchte auch noch Geld vom Automaten … Daten, Daten, Daten, die gespeichert werden. Meine Kreditkarte? Ein einziger Daten-Horror! Und ich zücke tatsächlich immer die Kunden-Karte, wenn ich in meinem Drogeriemarkt Shampoo und Seife kaufe – wenn ich jetzt daran denke, wird mir schwindlig. Die wissen, was ich wie oft einkaufe! Kein Risiko heute. Ich hole mir noch eine Flasche Cola am Kiosk und zahle in bar. Hatte der Besitzer einen Fotoapparat an der Wand? Oder fange ich schon an zu spinnen?
Zu Hause angekommen, schalte ich den Fernseher ein (darf ich …? Bei Satellitenempfang ja, bei Kabelempfang nein – zum Glück habe ich eine Schüssel), ziehe die Vorhänge zu und setze mich auf meine Couch. Ein toller Tag, so ganz ohne Datenspuren, oder?

Arbeitsaufträge:

1. Bitte lies den Text genau durch und führe danach ein Partnerinterview durch.

> Methode „Partnerinterview"
> Zu zweit mit Partner A und Partner B.
> Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt.
> Dann Wechsel der Rollen – aber Vorsicht!
> Jeder darf zwei Fehler beim Nacherzählen des Tagesablaufs einbauen, die der andere finden muss!

2. Liste auf, wo der Autor des Textes Datenspuren hinterlassen hätte.
3. Geht es dir als Schüler/Schülerin eigentlich auch so? Welche Datenspuren hinterlässt du an einem normalen Tag? Werde ein Daten-Detektiv und spüre auf, wo du Datenspuren hinterlässt. Erstelle auch dazu eine Liste und vergleiche sie mit dem Text!

> **Idee für eine Hausaufgabe:**
> Kannst du einen Tag verbringen, ohne Datenspuren zu hinterlassen? Schreibe einen Bericht über einen solchen Tag!

Warum ich mich öffentlich zeige? Lust an der Gemeinschaft

Datenschutz sollte doch eigentlich eine Selbstverständlichkeit sein, oder? Und trotzdem gibt es viele Menschen, die sich im Internet präsentieren und viel über sich preisgeben. Vor allem in Social Communities wie facebook. Warum? Und welche Meinung hast du dazu? Mithilfe dieses Arbeitsblattes sollt ihr darüber nachdenken.

„(…) Es mag schwer zu glauben sein, aber offenbar ist studiVZ für viele Mitglieder ein privaterer Ort als das eigene Zuhause. Sie erleben das Netzwerk als eine Stätte, an der man ganz unter sich ist und sich für nichts auf der Welt genieren muss. (…) Den wenigsten ist klar, dass kaum ein Ort so wenig privat ist wie das Internet. (…)"

Quelle: Nackt unter Freunden DER SPIEGEL 10/2009 vom 02.03.2009, Seite 118, online unter http://www.spiegel.de/spiegel/print/d-64385862.html

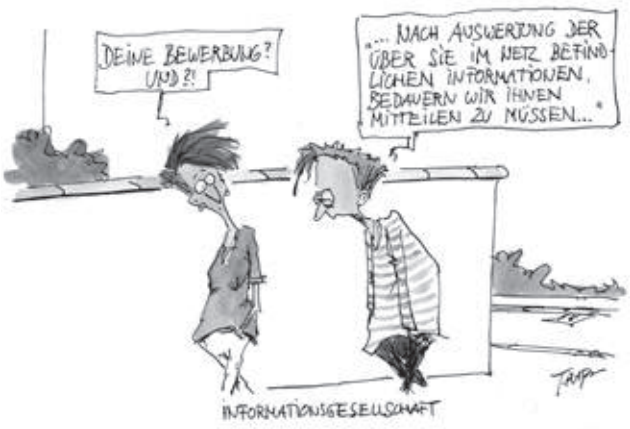
Verhaltensforscher erklären diese Leichtsinnigkeit mit alten Verhaltensweisen. Wir saßen schon in der Steinzeit gerne am Feuer und mit unserem Rudel zusammen. Dort waren wir sicher. Diese Gefahreneinschätzung fehlt am Computer, anders als im Angesicht des Säbelzahntigers oder heute auf einer belebten Straßenkreuzung oder in dunklen Gassen. Wir fühlen uns sicher, sind es aber nicht.

Arbeitsaufträge:

1. Bitte schreibe drei Gründe auf, warum Jugendliche sich im Internet mit persönlichen Daten wie privaten Fotos, Vorlieben, Hobbys, Alter, Adresse, usw. präsentieren.
2. Vergleicht diese Gründe in der Klasse und schreibt die wichtigsten an die Tafel.
3. Wie findest du das? Ist das o.k. oder eher bedenklich? Mit der Methode „strukturierte Kontroverse" sollt ihr euch darüber austauschen, diskutieren und vor allem die Positionen wechseln.

Strukturierte Kontroverse:
Bildet Vierergruppen! In jeder Gruppe arbeiten zwei Paare zusammen an einem Thema. Das eine Paar sammelt Argumente für die These und das andere Paar sammelt in der Diskussion Argumente für die Gegenthese.
Nun präsentieren sich die Paare gegenseitig ihre gefundenen Argumente.
Anschließend wechseln die Paare ihre Rollen (Pro wird zu Contra und Contra zu Pro) und führen erneut eine Diskussion. Einigt euch zum Schluss auf eine Position und begründet diese!
Nun stellen verschiedene Gruppen ihre Ergebnisse vor.

Was weiß das Netz über mich?



„Karrierebremse Internet" – das stand als Überschrift in der Westdeutschen Allgemeinen Zeitung vom 22.9.2009. In dem Zeitungsartikel steht beschrieben, dass Arbeitgeber das Internet gezielt nach Informationen absuchen, wenn sich jemand für einen Job bewirbt. Und auch der Zeichner Thomas Plassmann hat das Problem in seiner Karikatur „Informationsgesellschaft" beschrieben.

Und diese Suche ist ganz einfach: Du kannst einen Namen „googlen" oder in eine der Personensuchmaschinen wie www.yasni.de oder www.spock.com eingeben. Und schon erfährst du, was das Netz über denjenigen weiß! In diesem Arbeitsblatt darfst du es mal ausprobieren. Du brauchst dafür einen Internetzugang.

Arbeitsaufträge:

1. *Du darfst Detektiv spielen: Finde heraus, was das Internet über dich weiß. Suche nach Informationen zu deiner Person. Fasse die wichtigsten Daten auf einem Steckbrief zusammen. Wenn du nichts über dich findest (gut!), dann suche dir einen Prominenten heraus, vielleicht eine Schauspielerin oder einen Fußballer!*
2. *Welche der gefundenen „personenbezogenen Daten" findest du problematisch, wenn sie im Internet veröffentlicht werden? Suche dir drei Beispiele heraus und erläutere sie deinem Nachbarn!*
3. *Spielt folgendes Rollenspiel: Große Krisensitzung bei Familie Müller. Paula / Paul muss sich in drei Monaten für eine Ausbildungsstelle bewerben. Und Onkel Willi hat sich als Personalchef der Firma Meier mal im Internet umgeschaut ... und Paula / Paul hat eine Menge Datenspuren hinterlassen!*

Paula / Paul	Mutter	Vater	Freundin Jana	Onkel Willi
Du gehst recht sorglos mit deinen Daten im Internet um. Deine facebook-Chronik ist öffentlich komplett einsehbar, gegründet hast du die Gruppe „Wir trinken nur Bier an Tagen die mit ‚g' enden. Und Mittwochs." und du hast auch tolle Fotos der letzten Partys und von deinen Freunden veröffentlicht. Außerdem bist du regelmäßig im Blog „Arbeit – Nein Danke!" und schreibst dort Kommentare und, und, und …	Natürlich kennst du Soziale Netzwerke, schließlich brauchst du es für deinen Beruf. Du bist selbst Mitglied bei facebook und du hast dort auch viele Daten von dir veröffentlicht. Dir war nie so ganz klar, dass das auch problematisch werden kann, auch wenn du eigentlich vorsichtig warst bei der Veröffentlichung.	„Was soll nur aus dem Kind werden?" Du bist der Meinung, dass Paula / Paul ohnehin zuviel vor dem Computer hockt. Und du verstehst auch nicht recht, was man dort alles machen kann. Dieses facebook war dir sowieso immer unheimlich.	Du bist ganz vorsichtig mit dem, was du im Netz veröffentlichst und was nicht. Du hast vielleicht 2–3 harmlose Fotos von dir in facebook und bestimmt keine blöden Sachen und auch keine wichtigen persönlichen Daten. Du wusstest schon immer, dass Datenschutz wichtig ist. Aber Paula / Paul wollte ja nie auf dich hören!	Du bist Personalchef bei der Firma Meier. Und du hast in den letzten Jahren immer wieder Job-Bewerber, die alles über sich im Internet stehen haben. Normalerweise lädst du solche Leute gar nicht erst ein – was für ein Bild macht das denn für die Firma? Aber du möchtest deiner Nichte/ deinem Neffen natürlich helfen!

Sicherer werden: Privatdaten-Management

Du hast bis hierhin schon ganz viel über „personenbezogene Daten" gelernt und weißt, was an deren Veröffentlichung problematisch sein kann. Du kennst die Gesetzeslage und weißt, dass das Internet nichts vergisst und auch Arbeitgeber surfen. Doch wie kannst du dich – aus Sicht des Datenschutzes – richtig verhalten? Hier sollst du dir einige Tipps erarbeiten.

TIPPS

	Was ist das Problem?	Tipp
E-Mail	Viele sagen: „E-Mails sind Postkarten, die mit Bleistift geschrieben sind." Das Problem sind die „Authentizität" (ist der Absender echt?) und die Integrität (ist der Inhalt verändert?)	a) Ich schreibe nichts wirklich Privates in E-Mails. b) Ich benutze eine Verschlüsselungs-Software.
WhatsApp	WhatsApp nutzt Handynummern zur Identifizierung und greift deshalb auf das Adressbuch deines Smartphones zu. Die Sicherheit der über WhatsApp übermittelten Daten steht in der Kritik.	a) Ich schreibe nichts wirklich Wichtiges in WhatsApp wie Bankverbindung oder ähnliches. b) Ich gebe meine Handynummer nicht leichtfertig weiter, um mit neuen Bekanntschaften WhatsApp nutzen zu können. c) Ich respektiere die Privatsphäre meiner Freunde im Adressbuch und nutze WhatsApp nicht, wenn diese ihre Daten nicht weitergeben möchten.
facebook	Profilfoto und Titelbild ist für jeden sichtbar. Die Standardeinstellung bei facebook entsprechen nicht den sichersten Optionen. Öffentliche Beiträge können tatsächlich von jedem gesehen werden.	a) Ich überlege mir sehr genau, welche Profil- und Titelbilder ich wähle. b) Ich ändere die Voreinstellungen und wähle immer einen möglichst kleinen Personenkreis als Publikum aus. c) Ich überlege mir sehr genau was ich schreibe und wähle „öffentlich" nur, wenn es wirklich notwendig sein sollte.
Eigene Fotos und Filme	Fotos oder Filme können von deinem Profil oder deiner Seite kopiert und woanders gespeichert werden. Jeder kann sie sehen.	a) Ich veröffentliche keine / nur harmlose Fotos von mir. b) Ich suche regelmäßig in www.yasni.de (und anderen Suchhilfen) nach Fotos von mir. c) Ich schaue die Fotoalben meiner Freunde durch.
Flash-Cookies	Die so genannten Flash-Cookies werden nicht im Browser gespeichert, sondern im Adobe Flash Player.	Ich kontrolliere und lösche diese Supercookies im Einstellungsmanager für den Flash Player.
Internet-Telefonie	Der Inhalt des Telefonats kann abgehört werden.	Ich bespreche nichts wirklich Wichtiges per Internet-Telefonie.
Browser	Deine besuchten Seiten, die Cookies und andere Daten werden gespeichert.	a) Ich ändere die Browser-Einstellungen. b) Ich lösche diese Daten nach jeder Benutzung.
Chat	Alle Daten sind von allen Nutzern einsehbar, du weißt nie genau, wer dein Gegenüber wirklich ist.	a) Ich melde mich mit einem anonymen Nickname an. b) Ich gebe keine Daten (z. B. Adresse, Telefon- oder Handynummer) weiter.
Anmeldungen Websites	Du musst personenbezogene Daten angeben, damit du dich anmelden kannst.	a) Ich gebe nur unwichtige Daten weiter. b) Ich lüge und benutze eine zweite E-Mail-Adresse.
Passwörter	„Schwache" Passwörter können leicht erraten oder geknackt werden.	a) Ich denke mir ein eigenes System für Passwörter aus. b) Ich geben sie nie weiter.
Blogs und Foren	Deine Veröffentlichungen in Blogs und Foren können von allen gelesen werden.	a) Ich schreibe ohne meinen richtigen Namen. b) Ich bin sehr sorgfältig mit dem, was ich schreibe.

Ein kleiner Zusatzauftrag für ganz Schnelle:
Wer noch weitermachen möchte: Auch zu folgenden Stichwörtern findet man Datenschutz-Probleme: Handy, Online-Banking, Gesichtserkennung, W-LAN.

Auch das solltest du bedenken … je mehr über dich im Netz zu finden ist … desto mehr finden auch Bösewichter!

Arbeitsaufträge:

1. Lies die Tipps sorgfältig durch. Frage nach, wenn du etwas nicht kennst oder nicht verstehst.

2. Welche der Tipps findest du besonders gut und wichtig für dich persönlich? Lege dir eine TOP-5 Liste an und redet in der Klasse darüber!

3. Erstelle dir eine Mind-Map mit den Tipps. Schreibe sie so auf ein großes Blatt Papier, dass du eine gute Übersicht hast. Du darfst die einzelnen Punkte auch mit Bildern verdeutlichen!



Unter **www.watchyourweb.de** findest du nette Video-Clips zum Thema



Eine Aufgabe zum Weiterdenken Zuhause:
Veröffentlichte Daten werden manchmal mit einem Tattoo verglichen. Stimmt der Vergleich? Was glaubst du?

Arbeitsblatt	**AB 4**
Thema	**(Digitale) Datenspuren im Alltag**
Zeitangabe (Unterrichtsstunden à 45 min.)	1
Ziele	An einem Text, der einen Selbstversuch schildert, einen Tag ohne Datenspuren verleben zu wollen, sollen die Schülerinnen und Schüler erfahren, wie wir alltäglich (digitale) Datenspuren hinterlassen. Danach sollen sie dies auf ihre eigene Situation übertragen.
Methodische Hinweise	Das Beispiel aus der Berufswelt eines Erwachsenen enthält einige Merkmale, die für Kinder und Jugendliche (noch) nicht relevant sind, so Zeiterfassungssysteme, Mautbrücken oder Kreditkarten. Nichtsdestotrotz ist es ein alltägliches Beispiel, das in dieser Form vielleicht den Eltern passieren kann. Auch das Auto selbst erhebt zahlreiche Daten. S. Presseerklärung des TLfDI: ⓘ **http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_das_auto_-_black_box_au__er_kontrolle.pdf** Das Partnerinterview soll sicherstellen, dass der Text von allen verstanden wurde und wiedergegeben werden kann. Die Auflistung der Datenspuren fällt sicherlich leicht, eine genaue Auflistung der erhobenen Daten finden Sie in den Sachinformationen (so werden beim Handy die Verbindungsdaten, aber nicht die Inhalte gespeichert, ebenso beim E-Mailing oder SMS). Die Übertragung auf die eigene Alltagssituation im Arbeitsauftrag Nr. 3 soll deutlich machen, inwieweit auch Kinder und Jugendliche Datenspuren im Alltag hinterlassen. Die Idee für eine Hausaufgabe ist als Vorschlag für interessierte Schülerinnen / Schüler zu verstehen und mit einem positiven Ergebnis nur sehr schwierig zu realisieren (es ist fast unmöglich, keine Datenspuren zu hinterlassen!).
Methoden und Material	Arbeitsblatt, Partnerinterview
Organisationsformen	Einzelarbeit, Partnerarbeit
Zugang Internet / PC	nein

Arbeitsblatt	**AB 5**
Thema	**Gesetzeslage zum Datenschutz**
Zeitangabe (Unterrichtsstunden à 45 min.)	2
Ziele	Durch eine Anwendung von einigen grundlegenden Gesetzen zum Datenschutz auf (fiktive) Fallbeispiele aus der Schule sollen wesentliche Elemente im Datenschutzrecht gelernt werden.
Methodische Hinweise	Gesetzestexte sind von Natur aus von Juristen für Juristen formuliert und dem Normalbürger nicht immer sofort zugänglich. So natürlich auch die Bestimmungen zum Datenschutz aus DSGVO, aus Bundes- und Landes-Datenschutzgesetz, Kunsturheberrechtsgesetz und Strafgesetzbuch. Die kurzen Erläuterungen in dem Text sollen helfen, können aber nur einen ersten Einstieg liefern. Die fiktiven Fallbeispiele des unbedarften Lehrers Dr. Tafel – oder sollte man besser Dr. Whiteboard schreiben – sollen die Gesetze veranschaulichen. Die Lösungen, hier kommentiert, sind folgende:

	Darf er das?	**ja**	**nein**
A.	Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b. Ja, denn die Schule darf (auf gesetzlicher Grundlage) Daten verarbeiten, ohne eine Klassenliste wäre sein Job als Lehrer nicht möglich.	×	
B.	Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis. Nein, das „Recht am eigenen Bild" gilt auch und besonders für Minderjährige, gerade wenn das Bild veröffentlicht werden soll. Aber Vorsicht: Es schützt eigentlich nur vor Veröffentlichung, nicht vor der Fotografie an sich! Wenn man aber Befürchtungen hat, das Bild könnte veröffentlich werden, kann man die Löschung vorab verlangen.		×
C.	Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis. Ja, aber hier gilt auch eine Altersgrenze: Wenn vorausgesetzt werden kann, dass die Minderjährigen den Sinn und Zweck verstehen, müssen sie und die Eltern zustimmen. Oft wird die Grenze bei 12 oder 14 Jahren (14 ist die Regel) gesehen. Bei jüngeren Kindern genügt die Zustimmung der Eltern.	×	

	D.	Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage. Nein, natürlich nicht. Niemand darf die Fotos ohne Einverständnis veröffentlichen, auch nicht zu privaten (und nicht-kommerziellen) Zwecken.		×
	E.	Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage. Nein, auch das nicht. Es sei denn, es liegt das Einverständnis vor – der Schülerinnen und Schüler bzw. bei Minderjährigen: der Eltern!		×
	F.	Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag. Nein, das kostet ihn wahrscheinlich den Job!		×
	G.	Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt. Nein, die Weitergabe von Daten ist strikt verboten, auch an Bekannte, Freunde oder Verwandte. Schulsekretärinnen dürfen bspw. auch am Telefon keine Auskunft über einzelne Schülerinnen / Schüler geben.		×
	H.	Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop. Hierfür braucht er die Genehmigung der Schulleitung; das gilt i.ü. nicht nur für Fotos, sondern auch für sonstige personenbezogenen Schülerdaten; außerdem muss sich Dr. T. damit einverstanden erklären, dass sein Laptop so wie dienstliche Geräte kontrolliert werden können; und den Belangen des Datenschutzes muss ebenfalls Rechnung getragen werden.		×
	I.	Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören. Nein! (Kein Kommentar!) Das Recht am eigenen Bild und dann noch heimlich!		×
	J.	Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich. Nein, auch hierfür würde er wohl seinen Job verlieren.		×
	K.	Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er ihn filmen dürfe. Ja, natürlich nur, wenn auch alle Eltern (und Kinder) ihr Einverständnis geben.	×	
	L.	Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er? Es ist umstritten, ob und unter welchen Voraussetzungen eine Zustimmung widerrufen werden kann. Gerichte haben hierzu unterschiedliche Entscheidungen getroffen. Nach einer Ansicht ist die Zustimmung wie ein Vertrag zu behandeln und daher rechtsverbindlich und nur unter den gesetzlich vorgesehenen Voraussetzungen rückgängig zu machen. Nach anderer Ansicht ist eine Zustimmung zwar generell widerruflich, allerdings nur, wenn ein gewichtiger Grund vorliegt. Deshalb sollte Dr. Tafel die Sorgen der Mutter ernst nehmen und versuchen, mit ihr eine gute Lösung zu finden. Für datenschutzrechtliche Zustimmungserklärungen gilt das wiederum nicht, die können tatsächlich frei widerrufen werden.	×	×
	Die beiden letzten Arbeitsaufträge sollen wiederum eine Anwendung des Erlernten ermöglichen. Die Gesetze haben – selbstverständlich – viel mit dem Leben von Kindern und Jugendlichen zu tun und sollen sie schützen. Nur die Kenntnis dieser Rechtsnormen ermöglicht eine Anwendung im Einzelfall.			
Methoden und Material	Arbeitsblatt			
Organisationsformen	Einzelarbeit, Klassengespräch, Gruppenarbeit			
Zugang Internet / PC	nein			

Recht und Gesetz und meine Daten

Selbstverständlich gibt es in Deutschland viele Gesetze, die festlegen, wie man mit persönlichen Daten umgehen muss. Hier lernst du einige wichtige kennen.

Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Die DSGVO und das Bundesdatenschutzgesetz regeln die Datenverarbeitung der öffentlichen Stellen des Bundes (z. B. Bundesbehörden, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts usw.) sowie der nicht öffentlichen Stellen (z. B. Händler, Dienstleister, Einzelfirmen, Selbständige, Rechtsanwälte, Ärzte usw.). Alle Länder haben darüber hinaus für ihre öffentlichen Stellen (z. B. Landesbehörden, Landesanstalten, Landeskörperschaften usw.) eigene Landesdatenschutzgesetze erlassen.

Bundesdatenschutzgesetz und Landesdatenschutzgesetze dürfen aber nur das regeln, was ihnen über die DSGVO erlaubt wird. Die DSGVO ist die Basisgrundlage des Datenschutzes in Europa. Aufgrund europarechtlicher Zuständigkeiten gelten für die Verarbeitung von Daten bei der Strafverfolgung durch Polizei und Justiz allerdings Ausnahmen, die aber auch die Europäische Grundrechtecharta beachten müssen und über reine europäische Richtlinie abgebildet werden.

Daneben können die Mitgliedsstaaten der Europäischen Union über die DSGVO auch weitere Regelungen zur Datenverarbeitung treffen, wenn diese Verarbeitung zur Erfüllung öffentlich-rechtlicher Aufgaben dient, wie z. B. in den Schulgesetzen der Bundesländer. Diese regeln beispielsweise den Umgang mit den Schüler-, Eltern- und Lehrerdaten in der Schule. So dürfen nur die zur Aufgabenerfüllung der Schulen erforderlichen Daten erhoben werden und nur für diesen Zweck verarbeitet und genutzt werden. Wichtig ist, dass das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten (vgl. Artikel 4 Nr. 2 DSGVO) nur zulässig ist, wenn dies entweder ausdrücklich durch ein Datenschutzgesetz oder eine andere Rechtsvorschrift erlaubt bzw. angeordnet ist oder der Betroffene zuvor hierin eingewilligt hat.

In den Datenschutzgesetzen sind auch die Rechte der betroffenen Personen beschrieben. Jede Person hat ein Auskunftsrecht, d. h. sie darf nachfragen, was über sie gespeichert ist. Sie hat auch einen Anspruch auf Richtigstellung oder in bestimmten Fällen einen Anspruch auf Einschränkung oder sogar Löschung seiner Daten. Ebenfalls kann die betroffene Person eine erteilte Einwilligung jederzeit widerrufen. Schließlich kann sich jedermann an den zuständigen Bundes- bzw. Landesdatenschutzbeauftragten wenden, wenn er sich durch den Umgang mit seinen personenbezogenen Daten in seinen Datenschutzrechten beeinträchtigt sieht.

Kunsturheberrechtsgesetz

§ 22 „Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Dies nennt man auch Recht am eigenen Bild. Es bedeutet, du alleine bestimmst, welche Fotos von dir veröffentlicht werden. Ganz wichtig: Wer ohne dein Einverständnis Bilder von dir ins Netz stellt, macht sich strafbar! Es gibt übrigens Ausnahmen für berühmte Persönlichkeiten wie Sportler, Schauspieler oder Politiker.

Strafgesetzbuch

§ 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
„(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."
Wer also heimlich Fotos in einer Umkleidekabine macht, der macht sich strafbar!

Und leider gibt es – wahrscheinlich überall – Menschen, die sich nicht an die Gesetze halten. Dr. Tafel ist so einer, der es nicht ganz genau nimmt mit dem „Datenschutz": Kreuze an, ob er das darf (ja) oder nicht (nein)

	Darf er das?	ja	nein
A.	Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b.		
B.	Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis.		
C.	Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis.		
D.	Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage.		
E.	Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage.		
F.	Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag.		
G.	Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt.		
H.	Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop.		
I.	Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören.		
J.	Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich.		
K.	Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er den Versuch filmen dürfe.		
L.	Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er?		

Wer wissen möchte, wie und welche Daten in Social Communities wie facebook „verarbeitet" werden, der schaut mal in die „Datenschutzerklärung" und in die „Allgemeinen Geschäftsbedingungen" (AGB)

Arbeitsaufträge:

1. Bitte vergleicht eure Antworten in der Klasse.
2. Redet darüber, warum Dr. Tafel das eine darf und das andere nicht.
3. Was haben diese Gesetze mit euch zu tun? Erstellt eine Liste der wichtigen Punkte der Gesetze und schreibt – möglichst mit Beispielen – auf, worauf ihr ein Recht habt! Denkt dabei auch an facebook, YouTube, Knuddels oder ähnliche Plattformen.
4. Teilt euch in Gruppen auf und malt zu jedem der wichtigen Punkte ein Plakat „Das Gesetz und ich".

Arbeitsblatt	**AB**
Titel	**Recht und Gesetz / Berufsgeheimnisträger**
Kompetenzen	Die Schülerinnen und Schüler erfahren, dass es für bestimmte Berufe besondere Anforderungen an die Vertraulichkeit und Geheimhaltung für die bei der Ausübung der Tätigkeit erlangten Informationen und Daten gibt. Es wird verdeutlicht, wie der eigene Beruf einzuordnen ist, und ob dieser von speziellen Vorschriften erfasst ist.
Methoden	Partnerinterview
Material	Arbeitsblatt
Zeit (in Minuten)	45
Zugang Internet/PC	nein

Hinweise für die Durchführung

Die Schülerinnen und Schüler lesen den Text „Informationen für Berufsgeheimnisträger" und überlegen hierbei schon, welche Informationen für sie relevant sind, und ob sie davon betroffen sind. Anschließend führen immer zwei Schülerinnen und Schüler ein Partnerinterview durch, um das Gelesene abzufragen. Hierbei können Inhalte oder die vorbereiteten Leitfragen helfen. Die beiden Aufgaben sollen gemeinsam gelöst werden und hierbei eine Diskussion darüber ermöglichen.

Übersicht über Gesetze und Regelungen

- § 203 Abs. 1 Nr. 3 und Abs. III Satz 2 StGB StB (Stand Oktober 2016) und deren berufsmäßig tätigte Gehilfe
  => umfasst auch Daten von Unternehmen, schützt auch die bloße Angabe des Mandatsverhältnisses Strafbar nur nach Antrag (Strafmaß bis 1 Jahr) Gilt auch nach Beendigung des Mandats und Tod des Betroffenen!
- § 203 Abs. 3 Satz 2 beschreibt den Rechtfertigungsgrund, dass Berufsgeheimnisträger und deren Gehilfen fremde Geheimnisse gegenüber sonstigen Personen, die an ihrer beruflichen Tätigkeit mitwirken, offenbaren dürfen, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist.
- § 57 Abs. 1 StBerG für Steuerberater
- § 62 StBerG für Gehilfen
- UWG, dort §§ 17, 18
- Verpflichtung zur Geheimhaltung und Vertraulichkeit
- Arbeitsvertrag

Lösungen

Darfst Du vertrauliche Informationen unverschlüsselt per E-Mail versenden?

Nein, vertrauliche, bzw. geheime Informationen müssen bei der Kommunikation und Übermittlung geschützt sein. Dies muss auch beim Versenden von vertraulichen Informationen per E-Mails beachtet werden.

Kann ein Geheimnisverrat mit Gefängnis bestraft werden?

Ja, im Strafgesetzbuch (StGB) § 203 „Verletzung von Privatgeheimnissen" Absatz (1) steht:

> Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als …. *(hier folgt die Aufzählung der betroffenen Berufe)* anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Sind auch „Gehilfen besonderer Berufsgruppen und mitwirkende Personen" zur Verschwiegenheit verpflichtet?

Ja, im Strafgesetzbuch (StGB) § 203 „Verletzung von Privatgeheimnissen" Absatz (3) steht:

> Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.
>
> Gehilfe ist, wer im Rahmen seiner beruflichen Tätigkeit für eine in § 203 Abs. 1 StGB genannte Berufsgruppe eine Unterstützung ausübt, welche die Kenntnis fremder Geheimnisse mit sich bringt.
>
> Sonstige mitwirkende Personen (z. B. externe Dienstleister), die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken, sind ebenfalls zur Verschwiegenheit zu verpflichten.

Endet die Verschwiegenheitsverpflichtung mit dem Ausscheiden aus dem Unternehmen?

Nein, fast immer besteht diese auch nach dem Ausscheiden aus dem Unternehmen fort. Oftmals unbefristet, jedoch mindestens zwei Jahre.

Welche Paragraphen im Strafgesetzbuch (StGB) regeln die Verschwiegenheitsverpflichtung?

Dies sind § 203 (Verletzung von Privatgeheimnissen) und ggf. § 206 (Verletzung des Post- oder Fernmeldegeheimnisses).

Bin ich mit meinem Beruf auch betroffen?

Eine Aufzählung der meisten betroffenen Berufe findest Du im Strafgesetzbuch (StGB) § 203.

Recht und Gesetz / Berufsgeheimnisträger

Aufgabe 1:

Lies den Text mit der Methode Partnerinterview. Du kannst folgende Leitfragen verwenden:

Leitfragen

- Darfst Du vertrauliche Informationen unverschlüsselt per E-Mail versenden?
- Kann ein Geheimnisverrat mit Gefängnis bestraft werden?
- Sind auch „Gehilfen besonderer Berufsgruppen und mitwirkende Personen" zur Verschwiegenheit verpflichtet?
- Endet die Verschwiegenheitsverpflichtung mit dem Ausscheiden aus dem Unternehmen?
- Welcher Paragraph im Strafgesetzbuch (StGB) regelt die Verschwiegenheitsverpflichtung?
- Bin ich mit meinem Beruf auch betroffen?

Informationen für Berufsgeheimnisträger

Unabhängig davon, welcher Beruf oder welche Tätigkeit ausgeübt wird, gibt es rechtliche Rahmenbedingungen, welche dafür sorgen, dass die hierbei erlangten Informationen vertraulich zu behandeln sind. Dies bezieht sich beispielsweise auf Angaben zu eigenen Mitarbeitern, Arbeitskollegen, Kunden, Mandanten, Patienten oder auch Geschäftspartnern. Diese Vertraulichkeit wird auch Verschwiegenheitsverpflichtung oder Schweigepflicht genannt. Diese Verschwiegenheitsverpflichtung begründet sich in aller Regel durch entsprechende Vereinbarungen im Arbeitsvertrag oder über die Regelungen im Gesetz gegen den unlauteren Wettbewerb zu Geschäfts- und Betriebsgeheimnissen im §§ 17, 18 UWG.

Darüber hinaus gibt es für bestimmte Berufsgruppen berufsrechtliche Regelungen, welche die Verschwiegenheit vorschreiben. Die Verpflichtung auf diese berufsrechtliche Verschwiegenheit ergibt sich aus dem jeweiligen Gesetz direkt, wie z. B. aus § 57 Abs. 1 Steuerberatungsgesetz (StBerG), so dass Steuerberater aufgrund dieser Regelung einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Bei Steuerberatern sind dann z. B. die bei ihm beschäftigten Personen auf die Verschwiegenheit zu verpflichten, § 62 Satz 1 StBerG.

Zudem wird über strafrechtliche Regelungen im Strafgesetzbuch das unbefugte Offenbaren von Informationen, die bestimmte Berufsträger bei der Ausübung ihrer Tätigkeit erhalten, unter Strafe gestellt (z.B. für Ärzte, Rechtsanwälte, Steuerberater etc. in § 203 StGB und bei für Post- und Fernmeldegeheimnisse in § 206 StGB). Umso wichtiger ist es für jeden, informiert zu sein und zu wissen, inwieweit man bei der Ausübung seines Berufes betroffen ist. Für Berufseinsteiger oder Auszubildende und Praktikanten trifft dies erst recht zu, da diese in der Regel noch keine Erfahrung haben. Wichtig ist hierbei auch, dass nicht nur die Personen, welche die Berufe ausüben, durch Gesetze und Vorschriften erfasst werden, sondern auch deren Gehilfen und sonstige Personen wie z.B. externe Dienstleister welche zur Ausübung der beruflichen Tätigkeit in Anspruch genommen werden und auf die Verschwiegenheit verpflichtet wurden.

Methode „Partnerinterview“ – zu zweit mit Partner A und Partner B. Beide lesen, danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt mit den Worten: „Habe ich dich richtig verstanden, dass …?“ Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler einbauen, die der andere finden muss!

Beispiele hierfür sind Steuerfachgehilfen, Buchhalter, Rechtsanwaltsgehilfen oder Arzthelferinnen oder z. B. auch Laborkräfte. Sonstigen mitwirkenden Personen wie z.B. externen Dienstleistern dürfen Geheimnisse offenbart werden, soweit dies für die Inanspruchnahme der Tätigkeit erforderlich ist und sie auf die Verschwiegenheit verpflichtet wurden. Schaut man sich nun die Daten an, um die es geht, gibt es offensichtliche Informationen, bei denen jedem klar ist, dass diese der Verschwiegenheit unterliegen. Etwa Bilanzen oder Steuererklärungen, Patientendiagnosen oder Laborbefunde, die wirtschaftliche Situation eines Unternehmens oder die Vertretung eines Mandanten in einer Strafsache und auch bei der Verarbeitung von Daten durch Steuerberater, Ärzte oder Rechtsanwälte. Hinzu kommen jetzt noch Informationen, welche auf den ersten Blick belanglos scheinen, jedoch auch geheim zu halten sind, da dem Betroffenen bei Bekanntwerden des Sachverhaltes u.U. Nachteile entstehen. Allein die Tatsache, dass jemand Patient in einer Praxis ist oder Mandant in der Kanzlei, sagt noch nichts darüber aus, an welcher Krankheit der Patient leidet, oder welche Dienstleistungen der Mandant in Anspruch nimmt, oder ob es dem Unternehmen des Mandanten z.B. wirtschaftlich gut oder schlecht geht. Der Betroffene soll aber selbst entscheiden können, ob bekannt wird, zu welchem Arzt er geht oder durch welche Kanzlei er betreut wird. Auch scheinbar belanglose Informationen ermöglichen es, in Verbindung mit weiteren Daten durchaus aussagekräftige Rückschlüsse zu ziehen. In der Praxis bedeutet dies für berufsmäßige Gehilfen ein Bewusstsein dafür zu entwickeln mit vertraulichen Informationen sensibel umzugehen und zu gewährleisten, dass das „Geheimnis“ geheim bleibt. Viele Dienstleistungen würden nicht in Anspruch genommen werden, wenn man sich nicht darauf verlassen könnte, dass die Umstände und die hierbei erlangten Informationen vertraulich sind. Beispiele hierfür sind Besuche beim Arzt oder Psychologen. Besondere Beachtung finden hierbei Tätigkeiten, wenn es um die Kommunikation, die Speicherung oder den Transport von Daten geht.

Unverschlüsselte Kommunikation von vertraulichen Daten über einen unsicheren Kommunikationsweg sollte daher nicht erfolgen, wenn dadurch eine unbefugte Offenbarung droht. Problematisch kann es daher sein, unverschlüsselte E-Mails zu senden, Daten unverschlüsselt in eine öffentliche Cloud zu speichern, bzw. bei Cloud-Diensten abzulegen. Auch bei Messanger-Diensten oder Chat-Kommunikation sollte geprüft werden, ob dabei nicht doch unbefugt offenbart wird und diese daher für vertrauliche Informationen ausscheiden. Selbst wenn die inhaltlichen Kommunikationsdaten verschlüsselt übertragen werden, sind dem Dienste Anbieter die sog. Metadaten, also wer kommuniziert wie oft und wann mit wem, u.U. zugänglich und bekannt. Besonders problematisch können auch Telefongespräche sein, in welchen es um vertrauliche Inhalte geht. Der Anrufer kann sich mit einer falschen Identität melden und auf diesem Weg vertrauliche Informationen erhalten, die er nicht bekommen sollte. Als Angerufener kann man sich nicht immer davon überzeugen, dass der Anrufer auch wirklich der ist, für den er sich ausgibt. Wenn man sich also nicht 100% sicher ist, mit wem man spricht, sollten am Telefon keine vertraulichen Informationen genannt werden. Auch dann nicht, wenn es noch so dringend oder wichtig erscheint (z. B. Polizei, Staatsanwaltschaft, Krankenkasse, Schule, …). Es empfiehlt sich hier, die Berechtigung des Anrufers zu überprüfen oder sich den Sachverhalt schriftlich zusenden zu lassen oder den Anrufer über eine vorher bereits hinterlegte, bzw. bekannte Telefonnummer zurückzurufen. Damit kann man sicherer sein, dass man tatsächlich mit einem Berechtigten kommuniziert. Nach Feierabend, in der Familie, unter Freunden oder Online auf sozialen Medien endet die Verschwiegenheit natürlich nicht. Besonders hier muss man darauf achten, dass vertrauliche Informationen nicht „herausrutschen“. An dieser Stelle noch einmal der Hinweis, dass auch belanglose Informationen, wie etwa „ wir haben jetzt die Fa. XYZ als Kunden“ oder „die Fa. ABC zieht um nach …“ vertraulich sind.

Aufgabe 2:

Stelle Dir vor, die Sekretärin eines Mandanten ruft Dich an und bittet Dich darum, Dir die letzte betriebswirtschaftliche Auswertung zu faxen. Hierzu nennt sie Dir die Faxnummer.

- *Welche Probleme können sich hier ergeben?*
- *Würdest Du das Fax an die am Telefon genannte Faxnummer senden?*
- *Wie würdest Du in diesem Fall vorgehen?*

Aufgabe 3:

Ordne die verschiedenen Daten der jeweiligen Datenart zu.

Tabelle: Verschiedene Arten von Daten

Datenart	Daten
Geschäftsgeheimnis, Personenbezogene Daten, Berufsrechtliche Verschwiegenheit	Gehalt, Umsatz, Gesundheitsdaten, Adresse, Steuerdaten beim Steuerberater, Konstruktionspläne, Mandatsverhältnis, Source-Code (Software), Rezept beim Arzt oder Apotheker

Aufgabe 4:

Welche Berufsgruppen aus Tabelle A sind nicht im StGB § 203 genannt?

Tabelle

Berufsgruppen	
■ Ärzte, Zahnärzte, Tierärzte ■ Psychologen ■ Anwälte, Notare, Wirtschaftsprüfer ■ Buchprüfer, Steuerberater ■ Ehe-, Familien-, Erziehungsberater ■ Sozialarbeiter, Sozialpädagogen	■ Mitarbeiter von Kranken-, Unfall- oder Lebensversicherungen ■ Selbstständige Versicherungsvertreter ■ Mitarbeiter von privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstellen ■ Datenschutzbeauftragte



Das Recht am eigenen Bild

4|1 **Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild**

4

Übersicht der Bausteine:

- **Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Nicht alles, was geht, ist auch erlaubt! Downloaden, tauschen, online stellen – Urheberrecht im Alltag
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Urheberrecht_klicksafe.pdf

4 Das Recht am eigenen Bild



4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter

Übersicht über die Arbeitsblätter

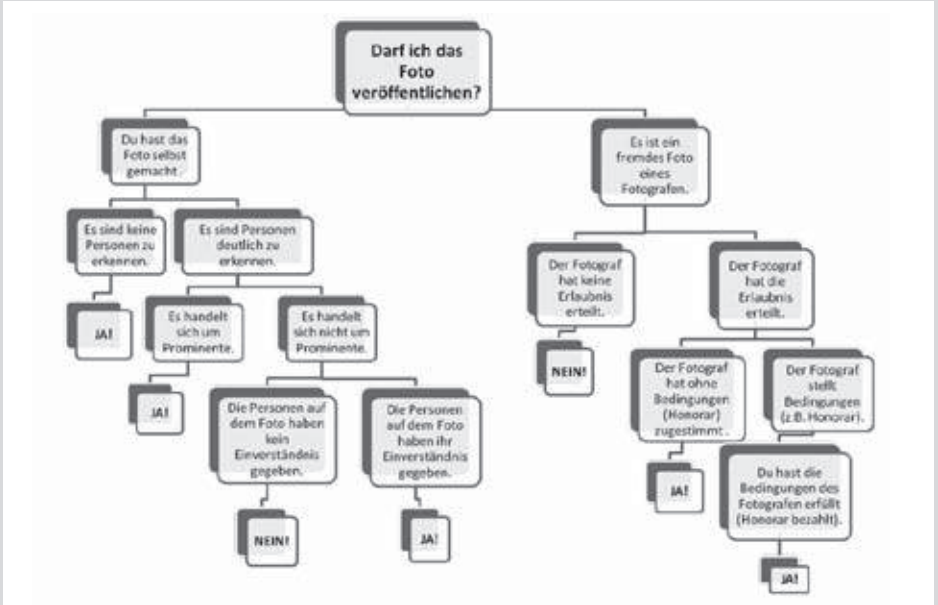
Titel	Inhalt/Lernziel	Arbeitsblätter
Urheberrecht – Was ist das?	Die Schüler sollen anhand eines Beispiels das Urheberrecht in seinen Grundzügen kennenlernen und seine Bedeutung reflektieren.	AB 1
Fotos und das Urheberrecht	Die Schüler sollen aus einem Informationstext eine Visualisierung in Form eines „Entscheidungsbaums" erstellen und damit die rechtlichen Grundlagen zur Veröffentlichung von Fotos wiedergeben können.	AB 2
Open Content	Die Schüler sollen das Modell Creative Commons kennenlernen und anwenden können.	AB 3
Abmahnungen	Die Schüler sollen das Rechtsinstrument der Abmahnung und eine angemessene Reaktion darauf kennenlernen.	AB 4
Urheberrecht im Unterricht	Am Beispiel eines schulischen Referats sollen die Schüler ihre Kenntnisse aus dem Urheberrecht anwenden können und das Zitatrecht kennenlernen.	AB 5
Videos anschauen und hochladen	Die Schüler sollen anhand von zehn Fragen – jeweils als Fallbeispiel – die rechtlichen Fragen der Nutzung von Videoportalen kennenlernen.	AB 6
Urheberrecht offline	In sechs Gruppen sollen die Schüler verschiedene Offline-Anwendungsszenarien des Urheberrechts durchspielen und anhand von Leitfragen in einem Stationenlernen umsetzen können.	AB 7
Streaming – Was und wo du schauen darfst	Die Schüler sollen technische und rechtliche Aspekte des Streamings und Embeddings im Ansatz verstehen.	AB 8
Up- und Downloads – Was ist legal, was illegal?	Die Schüler recherchieren über die beiden Nutzungsszenarien „Zum Download bereitstellen" und „Dateien selbst downloaden". Sie können urheberrechtliche Probleme erkennen und denken über legalen und nicht legalen Einsatz der unterschiedlichen Dienstleistungen sowie deren technisch-funktionale Unterschiede (Vergleich Tauschbörse – Filehoster) nach.	Projekt
Quiz Urheberrecht	Die Schüler können das erworbene Wissen anhand eines Quiz' überprüfen und festigen.	Quiz

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**
Thema	**Urheberrecht – Was ist das?**
Inhalt	**Grundlagen des Urheberrechts**
Ziele	Die Schüler sollen anhand eines kurzen Beispiels (das Foto eines Sportlers aus dem Internet) das Urheberrecht in seinen Grundzügen kennenlernen und seine Bedeutung reflektieren.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	2
Methodische Hinweise	Der Einstieg erfolgt über ein alltägliches Problem in Zeiten des Internets und die Frage: Darf ich ein Foto ohne CC-Lizenz aus dem Netz veröffentlichen? Die Antwort lautet in diesem Fall eindeutig Nein. Mit der Blitzumfrage im 1. Arbeitsauftrag können Sie ein Meinungsbild in der Klasse erstellen und den Kenntnisstand der Schüler einschätzen. Arbeitsaufträge 2 (a, b) und 3 sind zugegebenermaßen recht knifflig, was an der juristischen Materie liegt. Geben Sie Ihren Schülern für Arbeitsauftrag 2 a kurz Zeit (2–3 Minuten), um alleine über die Bedeutung des Satzes nachzudenken, rufen Sie erst danach die Meldungen ab. Die Methode Placemat (Aufgabe 2 b) für eine einfachere Formulierung des Urheberrechts soll ermöglichen, in Ruhe diese anspruchsvolle Aufgabe zu bearbeiten, im Schonraum einer Schülergruppe zu diskutieren und dann erst ein Gruppenergebnis präsentieren zu müssen. Die Fixierung an der Tafel soll ermöglichen, dass im Weiteren mit dieser (hoffentlich einfacheren) Definition des Urheberrechts weitergearbeitet werden kann. Am Schluss schließlich steht die Diskussion über den Sinn des Urheberrechts, den viele Schüler infrage stellen. Es lohnt sich eine Diskussion über eine Gesellschaft, die dieses Recht nicht wahrt …
Lösungen	Aufgabe 2 b: Das Urheberrecht ist eine Art Eigentumsrecht. Deshalb spricht man auch von geistigem Eigentum. Der Urheber eines Werkes kann über jede Form der Verwertung seines Werkes im Prinzip frei entscheiden, anderen z. B. verbieten, seinen Text zu veröffentlichen oder sein Musikstück auf CDs zu verkaufen bzw. für die Erlaubnis hierfür Geld verlangen. Er hat auch das Recht, als Autor, Komponist oder Softwareentwickler genannt zu werden, wenn sein Werk verwertet wird.

Lösungen	Aufgabe 3: 1. Sprachwerke sind alle Werke, deren Ausdrucksmittel die Sprache ist. Hierzu gehören sowohl die „Schriftwerke", deren Festlegung die Schrift ist, als auch Reden, Vorlesungen und Vorträge. Mögliches weiteres Beispiel für Sprachwerke: Songtexte! 2. Werke der Musik: die neue CD von Lady Gaga 3. Werke der Tanzkunst: die Choreografie in einem Musical 4. Werke der bildenden Künste: die Comics in diesem Heft 5. Lichtbildwerke: die Fotos, die man bei der letzten Klassenfahrt gemacht hat 6. Filmwerke: Kinofilme, Fernsehfilme etc. 7. Darstellungen wissenschaftlicher oder technischer Art: die Deutschlandkarte (aus dem Lehrmittelraum)
Methode/n und Material	Umfrage, Placemat, Tafel, Klassengespräch
Organisationsformen	Plenum Gruppenarbeit, Einzelarbeit
Zugang Internet/PC	Nein

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 2**
Thema	**Fotos und das Urheberrecht**
Inhalt	**Das Recht am eigenen Bild und die Möglichkeiten zur Veröffentlichung eigener und fremder Fotos**
Ziele	Die Schüler sollen aus einem Informationstext eine Visualisierung in Form eines Entscheidungsbaums erstellen und damit die rechtlichen Grundlagen zur Veröffentlichung von Fotos wiedergeben können.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	1–2
Methodische Hinweise	Der Einstieg erfolgt über einen kurzen Text, der erläutert, was das Recht am eigenen Bild ist (jeder hat das Recht zu bestimmen, ob er fotografiert wird und ob dieses Bild veröffentlicht wird – allerdings gibt es Ausnahmen wie „Beiwerk"). Die Schüler sollen diesen Text lesen und anschließend mithilfe des 1. Arbeitsauftrages als Entscheidungsbaum visualisieren. Für die Gestaltung eines solchen Entscheidungsbaumes gibt es verschiedene Möglichkeiten. Ermuntern Sie Ihre Schüler zu einer kreativen Umsetzung. Vielleicht gibt es sogar (urheberrechtsfreie!) Fotos, die dies veranschaulichen können. Bei dem Lösungsvorschlag wird davon ausgegangen, dass die Persönlichkeitsrechte, wie das Recht am eigenen Bild, mit dem Fotografen geklärt sind.
Lösungen	
Methode/n und Material	AB, Plakate, Schere, Klebstoff
Organisationsformen	Plenum, Einzelarbeit
Zugang Internet/PC	Nein

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 3**
Thema	**Open Content**
Inhalt	**Das Lizenzmodell Creative Commons**
Ziele	Die Schüler sollen das Modell Creative Commons kennenlernen und anwenden können.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	1–2 (mit Zusatzaufgabe ca. 3)
Methodische Hinweise	Creative Commons bietet die Möglichkeit – gerade für Schüler und Studenten –, kostenlos und legal Bilder, Fotos, Texte, Videos und Musik zu nutzen. Im Gegenzug könnten auch Schüler ihre Werke als CC-Lizenz zur Verfügung stellen und somit der Allgemeinheit (legal) zugänglich machen. Mit den ersten beiden Arbeitsaufträgen sollen sie die Feinheiten der CC-Lizenzen kennenlernen. Der 1. Arbeitsauftrag verursacht sicherlich etwas kreatives Chaos im Klassenraum. Die Schüler sollen sich als Symbole für die Regeln (by, nc, nd und sa) zu möglichen Kombinationen mit einem Schild vor der Brust aufstellen und die Kombination erläutern. Stehen beispielsweise die Schüler nc und sa zusammen, darf der Name des Urhebers weggelassen und das Werk verändert werden. Das Werk darf aber nicht für kommerzielle Zwecke genutzt werden, und nach einer Veränderung muss es unter nc/sa-Lizenz stehen. Vielleicht lassen Sie nach einer Gruppenphase die beste dieser Performances vor der Klasse darstellen?! Die praktische Anwendung der Lizenzbestimmungen soll in Aufgabe 3 gefestigt werden (s. Lösungen). Aufgabe 4: Durch die Erstellung eines Handyvideos, das mit lizenzfreier Musik von Netlabels unterlegt werden soll, können die Jugendlichen das Netlabel-Angebot kennenlernen und praktisch nutzen. **Tipps zur Umsetzung eines Handyprojektes:** In der Broschüre „taschenfunk“ ab S. 25 **http://tinyurl.com/zyhzgz3**
Lösungen	**Aufgabe 3:** Thomas Claveirole: Nennung des Namens, Weitergabe mit gleicher Lizenz (Namensnennung) affnpack: Nennung des Namens, keine kommerzielle Nutzung und Weitergabe mit gleicher Lizenz (Namensnennung, keine kommerzielle Nutzung) vince42: Nennung des Namens, keine Veränderung des Werks
Methode/n und Material	Erstellen von Symbolschildern, Internetrecherche, Stichwortzettel, Handyclip
Organisationsformen	Plenum, Gruppenarbeit, Einzelarbeit
Zugang Internet/PC	Ja

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 4**
Thema	**Abmahnungen**
Inhalt	**Die rechtlichen Möglichkeiten einer Abmahnung und eine Reaktion darauf**
Ziele	Die Schüler sollen das Rechtsinstrument der Abmahnung und eine angemessene Reaktion darauf kennenlernen.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	2–3

Methodische Hinweise

Es ist sinnvoll, dass Jugendliche Abmahnungen kennenlernen und wissen, wie man angemessen darauf reagiert. Wichtig ist dennoch, dass mit den Jugendlichen besprochen wird, dass mit dem Erhalt einer Abmahnung in den meisten Fällen ein eindeutiges Fehlverhalten in Form einer Urheberrechtsverletzung einhergeht.



Die einzige wirklich empfehlenswerte Reaktion ist, einen Rechtsanwalt um Rat zu fragen. Das sollten (und können!) Jugendliche nicht alleine tun, sondern mit Unterstützung ihrer Eltern.

In einem ersten Schritt sollen die Schüler das Fallbeispiel von Cemre kennenlernen und den Text zur Erläuterung von Abmahnungen lesen.

Etwas anspruchsvoller ist der 1. Arbeitsauftrag, der eine Internetrecherche zum Stichwort Abmahnung beinhaltet. Die Schüler sollen eine Liste mit Tätigkeiten erstellen, für die sie eine Abmahnung erhalten könnten.
Die Rechercheaufgaben in Arbeitsauftrag 2 sollen zeigen, dass es auch Jugendliche leicht treffen kann. Sicherlich finden sich im Netz eindrucksvolle Beispiele, in denen Jugendliche für einen Urheberrechtsverstoß eine teure Abmahnung erhielten.

Auch die Diskussion um die Abmahnwellen lohnt sich. Hierzu kann es unterschiedliche Meinungen geben. Auf der einen Seite ist das Abmahnen zu begrüßen, weil so teure und langwierige Gerichtsverfahren vermieden werden können (durch die Zahlung eines festgelegten Betrages an die abmahnende Anwaltskanzlei). Auf der anderen Seite werden viele Jugendliche sicherlich der Meinung sein, es sei unverhältnismäßig und lediglich lukrativ für einige Anwälte. Vielleicht moderieren Sie diese Diskussion und geben Impulse für beide Standpunkte. Stößt dieses Thema auf großes Interesse, bieten sich die Methoden Rollenspiel oder Podiumsdiskussion an. Auch hier ist die Sozialform offen, es bietet sich wiederum Einzel- oder Kleingruppenarbeit an.

Mustervorlage für eine Fristverlängerung bei einer Abmahnung (Konsultation eines Anwaltes wird unbedingt empfohlen!):

https://www.verbraucherzentrale.de/sites/default/files/migration_files/media227663A.pdf

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Methodische Hinweise	Die Zusatzaufgabe beschäftigt sich mit dem theoretischen Modell „Kulturflatrate", einer gesetzlich geregelten Pauschalabgabe an Urheber. Damit verbunden wäre eine freie Nutzung von Inhalten, z. B. auf Filesharing-portalen. Diese Aufgabe bietet den Schülern die Möglichkeit, eigene Konzepte der Nutzung von bislang urheberrechtlich geschützten Inhalten zu entwickeln. Eine Herausforderung dabei wird es sein, die Interessen sowohl der Nutzer, als auch die Interessen der Urheber zu berücksichtigen.
Lösungen	1. Schritt: Ich informiere meine Eltern und erzähle ihnen alles. 2. Schritt: Ich prüfe sorgfältig, ob bei der Abmahnung wirklich alles stimmt. 3. Schritt: Ich bitte meine Eltern, einen Rechtsanwalt einzuschalten.
Methode/n und Material	Klassengespräch, Internetrecherche, Kurzpräsentation
Organisationsformen	Einzelarbeit, Gruppenarbeit
Zugang Internet/PC	Ja

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 5**
Thema	**Urheberrecht im Unterricht**
Inhalt	**Das Urheberrecht bei Referaten und das Zitatrecht**
Ziele	Am konkreten Beispiel eines schulischen Referats sollen die Schüler ihre Kenntnisse aus dem Urheberrecht anwenden können und das Zitatrecht kennenlernen.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	1
Methodische Hinweise	In einem ersten Schritt sollen die Schüler nach dem Lesen des Informationstextes in Eigenarbeit notieren, worauf sie bei einem Referat achten müssen (s. Lösungen). Dabei sollen die Fallbeispiele helfen. Dieses Ergebnis sollen die Schüler nun mit der Methode Kugellager präsentieren. Räumen Sie die Tische zur Seite und lassen Sie zwei Kreise bilden (Innenkreis und Außenkreis), wobei sich jeweils zwei Stühle gegenüberstehen. Signalisieren Sie den Beginn (Außenkreis beginnt) und lassen Sie eine Minute Zeit für die Präsentation des ersten Schülers. Danach wechseln die Rollen und die im Innenkreis sitzenden Schüler berichten eine Minute lang. Nach zwei Minuten wechseln die Partner (der Außenkreis rutscht im Uhrzeigersinn zwei Stühle weiter). Wiederholen Sie dies insgesamt dreimal. Was sich auf den ersten Blick etwas unübersichtlich anhört, ist mit einer methodisch geübten Lerngruppe schnell organisiert. Der Vorteil der Methode Kugellager: Jeder berichtet, jeder muss zuhören und dies gleich dreimal.
Lösungen	**Aufgabe 1:** Lösungswort: SCANNEN
Methode/n und Material	Kugellager
Organisationsformen	Einzelarbeit, Partnerarbeit
Zugang Internet/PC	Nein

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 6**
Thema	**Videos anschauen und hochladen**
Inhalt	**Rechtliche Fragen rund um die Nutzung von Videoportalen**
Ziele	Die Schüler sollen anhand von zehn Fragen – jeweils als Fallbeispiel – die rechtlichen Aspekte der Nutzung von Videoportalen kennenlernen.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	1
Methodische Hinweise	Nach dem schon bekannten Schlagabtausch unserer Helden Therese und Konrad sollen die Schüler die Fragen alleine beantworten bzw. eine Antwort mit Begründung formulieren. Wenn die Unterrichtsreihe bis hierhin durchgeführt wurde, fallen einige der Fragen sicherlich leicht (s. Lösungen), andere bleiben trotzdem schwierig. An dieser Stelle ist keine Internetrecherche vorgesehen, Sie können aber eine einbauen (als erste Adressen für das Thema seien ⓘ **www.irights.info** und ⓘ **www.klicksafe.de** empfohlen). Der erste Austausch mit einem Partner in Arbeitsauftrag 1 soll ermöglichen, die Antworten und Begründungen kurz zu reflektieren. Bei der Sammlung der Antworten an der Tafel sollten Sie darauf achten, gegebenenfalls falsche Antworten zu korrigieren.
Lösungen	A. Darf ich mir Videos bei YouTube anschauen? *Ja. (Es gibt bei YouTube eine Alterseinstufung. Bei manchen Videos muss man sich zumindest einloggen, um sie sehen zu können. Allerdings gibt es keine Altersverifikation bei YouTube.)* B. Darf ich mir Videos anschauen, die offensichtlich rechtswidrig bei YouTube hochgeladen wurden? *Die Antwort ist leider kompliziert, s. Sachinformationen zu „Streaming in Kapitel 2.1.4".* C. Gibt es einen Unterschied zwischen Streaming und Download? Wenn ja, welchen? *Der Unterschied zu Downloads ist, dass beim Streaming keine dauerhaften Kopien auf dem Rechner des Nutzers entstehen. Dennoch werden die Dateien zumindest flüchtig in Zwischenspeichern, dem Arbeitsspeicher oder im Browser-Cache des Empfängerrechners gespeichert. Auch derart vorübergehende Speicherungen gelten grundsätzlich als Vervielfältigungen, die dem Urheberrecht unterfallen. Dafür gelten jedoch grundsätzlich auch die Privatkopieschranke und eine andere Ausnahmeregelung, die flüchtige Kopien generell erlaubt. Unter dem Strich ist die Rechtslage in dieser Frage noch im Fluss und nicht eindeutig einzuschätzen.* D. Darf ich mir Videos auch herunterladen und dauerhaft auf meinem Rechner speichern? *Ja, das ist durch das Recht auf eine Privatkopie gedeckt.*

Lösungen	E. Darf ich mir (illegale) Videos auch herunterladen und dauerhaft auf meinem Rechner speichern? *Leider gibt es hierzu keine eindeutige Antwort, s. Sachinformationen zu der komplizierten Materie in Kapitel 2.1.4, Abschnitt „Videos anschauen auf illegalen Plattformen wie kinox.to". Generell sollte man, z. B. wegen der Gefahr durch Schadprogramme, von nicht vertrauenswürdigen Quellen abraten.* F. Darf ich eigene (selbst gedrehte) Videos auf YouTube hochladen? *Ja, aber ich muss das Persönlichkeitsrecht wahren.* G. Darf ich fremde Videos, z. B. einen Mitschnitt aus dem Fernsehen, hochladen? *Nein, diese sind urheberrechtlich geschützt.* H. Darf ich ein Video in mein Profil bei Facebook einbinden? *Ja. Weitere Informationen dazu in Kapitel 2.1.4, Abschnitt „Videos einbetten".* I. Darf ich fremde Videos, die ich bearbeitet und mit fremder Musik unterlegt habe, hochladen? *Nein, sowohl die Videos als auch die Musik sind urheberrechtlich geschützt. Mit dem Einverständnis der jeweiligen Urheber ist das erlaubt.* J. Darf ich fremde Videos, die ich bearbeitet und mit eigener Musik oder CC-Lizenz-Musik unterlegt habe, hochladen? *Nein, es sei denn, ich habe die Erlaubnis der Videoproduzenten dazu erhalten.* *Informationen zum Urheberrecht bei YouTube:* **http://www.youtube.com/t/howto_copyright**
Methode/n und Material	AB, Tafel
Organisationsformen	Einzelarbeit, Partnerarbeit
Zugang Internet	Ja

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 7**
Thema	**Urheberrecht offline**
Inhalt	**Anwendungsszenarien des Urheberrechts bei Offline-Nutzungen:** A. CDs brennen B. MP3s erstellen C. Musik tauschen D. Spiele und Filme kopieren E. Filmabende F. Öffentliche Partys veranstalten
Ziele	In sechs Gruppen sollen die Schüler verschiedene Offline-Anwendungsszenarien des Urheberrechts durchspielen und anhand von Leitfragen in einem Stationenlernen umsetzen können.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	2–3
Methodische Hinweise	Zu jedem der einzelnen Themen ließen sich hier sinnhaft eigene Unterrichtsstunden durchführen. Mit der Einteilung in Expertengruppen soll die Möglichkeit eröffnet werden, die verschiedenen Anwendungsszenarien (Nutzungsmöglichkeiten) in einer Einheit zu erarbeiten. Dies bedarf sicherlich mehr als einer Unterrichtsstunde und sollte möglichst in einer Doppelstunde (bei 45-Min.-Rhythmus) begonnen werden. Eine weitere Einzelstunde sollte für die Präsentation der Ergebnisse zur Verfügung stehen. Im strengen Sinne handelt es sich nicht um ein Stationenlernen, sondern um einen Lernzirkel, denn es müssen alle Stationen besucht werden. Die Schüler sollten auch Sorgfalt bei der Darstellung der Ergebnisse walten lassen und benötigen dazu vielleicht Ihre Hilfe.
Lösungen	Die Antworten in Kurzform: **CDs brennen** Was ist eine Privatkopie? *Das Speichern eines Inhalts (Audio-, Bild-, Video-Datei oder auch Texte) auf dem eigenen Rechner, um sie rein privat (im Familien-, Freundeskreis, zu Hause) zu nutzen.* Darf ich jede legal erworbene Musik-CD kopieren? *Nein, nur solche ohne Kopierschutz.* Darf ich einen Kopierschutz umgehen? *Nein.* Was ist mit einer Fernsehsendung, die ich vom Festplattenrekorder auf eine CD brenne? *Das ist durch die Privatkopieregelung gedeckt, wenn ich die Sendung privat nutzen will.* **MP3s erstellen** Darf ich eine legal erworbene Original-Musik-CD rippen? *Ja, es sei denn, sie ist kopiergeschützt.* Darf ich die MP3-Dateien der gerippten CD weiterverkaufen? *Nein.* Ich habe drei MP3-Player. Darf ich meine Musik auf alle drei aufspielen? *Ja.* Darf ich einen Kopierschutz umgehen? *Nein.*

Lösungen	**Musik tauschen** Darf ich eine legal erworbene Musik-CD kopieren und an meinen besten Freund weitergeben? *Ja. (Tatsächlich! Aber nur an echte Bekannte und in geringem Umfang!)* Darf ich diese kopierte CD 100 fach auf dem Schulhof verteilen? *Nein.* Verstoße ich gegen das Urheberrecht, wenn ich ein Lied per E-Mail-Anhang erhalte und speichere? *Nein.* Wenn wir uns als Geschwister nur eine CD kaufen, dürfen wir dann die Musik auf alle unsere MP3-Player übertragen? *Nur dann, wenn ich insgesamt nur einige Kopien mache (maximal sieben).* **Spiele und Filme kopieren** Gilt die Privatkopieregelung auch für eine Computerspiel-DVD? *Nein.* Oder eine Video-DVD? *Ja, es sei denn, sie ist kopiergeschützt.* Darf ich einen Kopierschutz umgehen? *Nein.* Darf ich ein kopiertes Computerspiel weitergeben? *Nein.* Darf ich einen kopierten Film weitergeben? *Ja, wenn das im privaten Kreis stattfindet und der Film überhaupt kopiert werden durfte (weil er nicht kopiergeschützt war).* Darf ich das Original eines Computerspiels / eines Films weitergeben? *Ja.* **Filmabende** Darf ich meine besten Freunde einladen und einen Videofilm anschauen? *Ja.* Was muss ich beachten, wenn ich daraus eine öffentliche Veranstaltung (wie Kino) mache? *Die Erlaubnis einholen. Bei Filmen liegt das öffentliche Vorführungs- und Wiedergaberecht bei den Verleihfirmen (und bedarf ausdrücklicher schriftlicher Genehmigung).* Darf ich ein selbst zusammengeschnittenes Video aus meinen Lieblingsfilmen zu Hause zeigen? *Im privaten Rahmen schon. Bei einer Veröffentlichung, Urheberrechte beachten, s. Kapitel 2.1.4, Abschnitt „Beispiel Mashups, Videocollagen, Remixes".* Ich zeige an dem Abend ein selbst gedrehtes Video des letzten Urlaubs. Was gibt es zu beachten? *Das Persönlichkeitsrecht der im Video vorkommenden Personen ist zu achten.* **Öffentliche Partys veranstalten** Darf ich grundsätzlich eine öffentliche Party (ohne Musik) veranstalten? *Ja. (Dafür gibt es natürlich andere Auflagen, außerhalb des Urheberrechts.)* Muss ich die Veranstaltung bei der GEMA anmelden, wenn ich Musik spiele? *Ja.* Wie teuer wird das für mich? *Je nachdem, bei der GEMA gibt es eine Preisliste* (**https://online.gema.de/aidaos/index.faces**). Verstoße ich als Gast gegen das Urheberrecht, wenn der Veranstalter keine GEMA-Anmeldung gemacht hat? *Nein.*
Methode/n und Material	Internetrecherche, Stationenlernen
Organisationsformen	Gruppenarbeit
Zugang Internet / PC	Ja

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 8**
Thema	**Streaming – Was und wo du schauen darfst**
Inhalt	**Rechtliche Fragen zu Videostreams**
Ziele	Die Schüler sollen technische und rechtliche Aspekte des Streamings und Embeddings im Ansatz verstehen.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	2–3
Methodische Hinweise	Das Arbeitsblatt besteht im Prinzip aus einer anspruchsvollen Textarbeit, die durch den Lückentext etwas ansprechender gestaltet wurde. Nachdem der Text alleine ergänzt wurde, können die Schüler z. B. zur Vertiefung ein Partnerinterview dazu durchführen. Methode Partnerinterview Dazu fasst Partner A den Text in einer Minute kurz zusammen. Partner B wiederholt den Text mit den Worten: „Habe ich dich richtig verstanden, dass …?“. Als besondere Schwierigkeit (und um die Aufmerksamkeit zu stärken) darf Partner A einen Fehler einbauen, den Partner B finden muss. Danach wechseln die Rollen: Partner B fasst zusammen, Partner A wiederholt das Gesagte. Im Anschluss soll ein Informationsflyer gestaltet werden, durch den die Jugendlichen mit eigenen Worten das Gelernte formulieren, zusammenfassen und wiederholen können.
Lösungen	Film, Anbieter, Kopie, Browser, Zwischenspeicher, Vervielfältigungen, geschützten Werken, rechtswidrig, Mediathek, Domain, den Rest der Welt, öffentlich zugänglich, Zustimmung, einzubetten, Originalquelle
Methode/n und Material	Lückentext, Methode Partnerinterview, Infoflyer gestalten
Organisationsformen	Einzelarbeit, Partnerarbeit
Zugang Internet/PC	Nein

4_1 Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**Projekt** (Schwierigkeitsgrad: anspruchsvoll)
Thema	**Up- und Downloads – Was ist legal, was illegal?**
Inhalt	**Vergleich: „zum Download bereitstellen" und „selbst downloaden"**
Ziele	Die Schüler recherchieren über die beiden Nutzungsszenarien „zum Download bereitstellen" und „selbst downloaden". Sie können urheberrechtliche Probleme erkennen und denken über den legalen und illegalen Einsatz der unterschiedlichen Dienstleistungen sowie deren technisch-funktionale Unterschiede (Vergleich Tauschbörse – Filehoster) nach.
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	2–3
Methodische Hinweise	Mit dem ersten kurzen Austausch soll der Kenntnisstand (und vielleicht die Meinung) in der Lerngruppe ermittelt werden. Oft ist in diesem Bereich das Unrechtsbewusstsein bei Jugendlichen nicht sehr ausgeprägt, es existiert aber eine diffuse Vorstellung davon, dass es z. B. nicht rechtens ist, Musik weiterzugeben. Vielleicht greift an der Stelle schon die bisherige Arbeit zum Urheberrecht. Teilen Sie die Klasse in zwei Gruppen auf, z. B. nach dem Hausnummernprinzip, bei dem die Schüler durchgezählt werden und jeweils diejenigen mit den geraden und die mit den ungeraden Nummern eine Gruppe bilden. Es ist sicher ratsam, dass in jeder Gruppe Schüler sind, die sich bereits gut mit Tauschbörsen auskennen. Die Internetrecherche ist nicht ganz einfach. Sie sollten den Schülern ausreichend Zeit geben, die Fragen zu beantworten.
Lösungen	**Aufgabe 1:** Die Mando-Diao-Kopie – erlaubt oder nicht? Till hat die CD illegalerweise heruntergeladen und somit auch illegalerweise zum Download zur Verfügung gestellt. Er hätte wissen müssen, dass die aktuelle Platte der Band nicht kostenlos im Internet zur Verfügung steht. Im Auftrag der Universal Music GmbH sprechen Anwaltskanzleien auch bezüglich dieses Albums Abmahnungen wegen unerlaubter Verwertung aus. Till kann zu einem Schadensersatz verklagt werden. **Aufgabe 2:** Die Antworten befinden sich in den Sachinformationen in Kapitel 2.1 „Nutzungen im Internet", Abschnitte 2.1.1–2.1.3. **Aufgabe 3:** Textvorschlag Vorfahrtsschild Bleibt man bei Material, für das die Urheberrechte geklärt sind – sei es, weil es eigenes Material ist oder weil die Rechteinhaber eine Verbreitung erlaubt haben – oder nutzt Filehoster / Tauschbörsen zum rein privaten Gebrauch und nur passiv, ist man meist auf der sicheren Seite.
Methode/n und Material	Internetrecherche, Kurzreferat, Verkehrsschilder erstellen
Organisationsformen	Gruppenarbeit
Zugang Internet / PC	Ja

Lösungen Quiz Urheberrecht

Nr.	Beispiel	Darf ich!	Darf ich nicht!	Kommt drauf an! (Erkläre genauer, wann etwas erlaubt ist und wann nicht!)
	Nutzungen im Internet			
	Tauschbörsen			
1	Downloads aus Tauschbörsen: Spiele, Musik, Filme, Software			Die Antwort ist so kompliziert, wie in den Sachinformationen beschrieben. Es gibt keine allgemeinverbindliche Antwort. Man könnte sagen: Software, Games = immer verboten (nur eine Sicherungskopie vom eigenen Original ist erlaubt). Filme, Musik = nur dann erlaubt, wenn sie nicht offensichtlich rechtswidrig öffentlich zugänglich gemacht wurden (bei kommerziellen Produkten in der Regel verboten).
2	Spiele, Musik, Filme, Software öffentlich zugänglich machen			Das ist verboten, wenn man nicht selbst die Rechte hat (etwa bei eigenen Filmen, selbst komponierter Musik).
	YouTube und andere Videoportale (Vimeo, das ehemalige kino.to usw.)			
3	Videos anschauen: Was gilt bei eindeutig rechtswidrig angebotenen Videos?			Anschauen ist nach Auffassung von iRights.info legal, auch wenn das Video aus rechtswidriger Quelle stammt. Die Meinungen darüber gehen aber bei Juristen auseinander, eine endgültige Rechtsprechung gibt es nicht.
4	Videos oder Musik herunterladen			Gekaufte Musik aus dem Internet herunterzuladen, ist legal, Gleiches gilt für Musik, die lizenzfrei ist.
5	Videos hochladen: Was ist zu beachten, wenn es sich um kommerzielle Inhalte Dritter handelt (TV-Sendungen, Videos, die kommerzielle Musik enthalten, Karaoke usw.)?			Urheberrechtlich geschützte Inhalte hochzuladen, ist illegal! Vorsicht auch bei Karaoke und beim Nachsingen von Songtexten.
6	Videos embedden in der eigenen Webseite			Ist unter bestimmten Voraussetzungen erlaubt (siehe Abschnitt 2.1.4).
	Filehoster u. Ä. (Uploaded.net, MEGA usw.)			
7	Dateien freigeben: Bekanntgeben von Downloadlinks (im Internet, nur für Freunde)			In Foren / Blogs Downloadlinks zu veröffentlichen, ist verboten (Öffentlichmachung!), sie per Mail / im Chat an Freunde, also nur einer kleinen Gruppe bekannter Menschen weiterzugeben, ist erlaubt.

4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

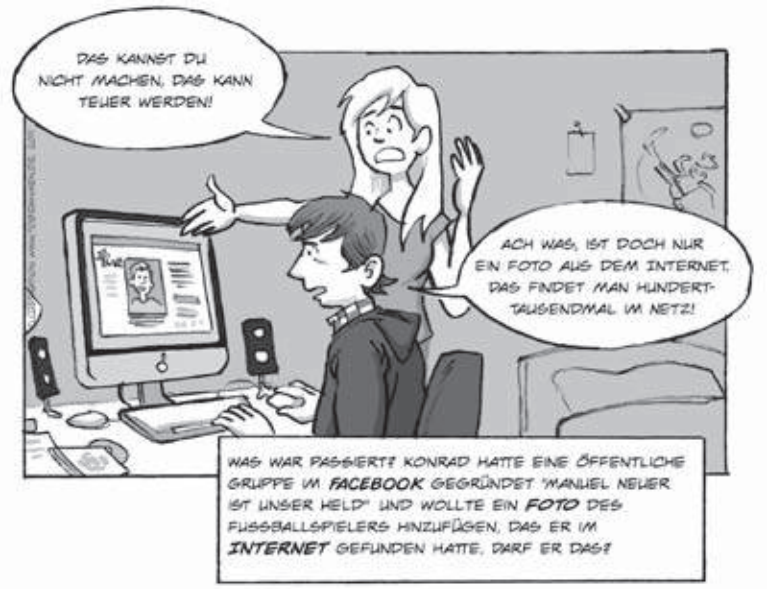
Nr.	Beispiel	Darf ich!	Darf ich nicht!	Kommt drauf an! (Erkläre genauer, wann etwas erlaubt ist und wann nicht!)
			Fanseiten	
8	Fremde Fotos einstellen		×	
9	Fremde Interviews einstellen		×	
10	Musik oder Filme (oder jeweils Ausschnitte davon) zum Download anbieten		×	
11	Verlinken von externen Quellen			Wenn diese legal sind, okay
12	Verkaufen deiner Lieblings-CD			Nach deutschem Recht ist es erlaubt, Produkte, die urheberrechtlich geschützte Inhalte enthalten, also z. B. eine CD der Lieblingsband, frei weiterzuverkaufen, wenn sie einmal rechtmäßig auf den Markt gelangt sind.
			E-Mail, Bluetooth	
13	Versand geschützter Dateien per E-Mail	×		Handeln sowohl derjenige, der die Mail mit der Datei verschickt als auch der Empfänger zu rein privaten Zwecken und wollen die Dateien ausschließlich im privaten Bereich nutzen, okay!
14	Versand geschützter Dateien per Messenger	×		s. Beispiel 13
			Offline-Nutzungen	
			CDs brennen	
15	Für sich	×		
16	Für Freunde und Verwandte	×		
17	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof		×	
18	Zum Verkaufen		×	
19	Was gilt bei kopiergeschützten CDs?		×	

4_1 Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Nr.	Beispiel	Darf ich!	Darf ich nicht!	Kommt drauf an! (Erkläre genauer, wann etwas erlaubt ist und wann nicht!)
	MP3s erstellen / tauschen			
20	Für sich	×		
21	Für Freunde und Verwandte	×		
22	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof		×	
23	Zum Verkaufen (z. B. über eBay)		×	
24	Was gilt bei kopiergeschützten Dateien?		×	
	Spiele kopieren (brennen) und tauschen			
25	Für sich (Sicherungskopie), soweit nicht kopiergeschützt	×		
26	Für Freunde und Verwandte		×	Spiele darf man nur für sich brennen (als Sicherungskopie), wenn man selbst ein Original hat, aber nicht für Freunde / Familie.
27	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof		×	
28	Zum Verkaufen (z. B. über eBay)		×	
29	Was gilt bei kopiergeschützten Dateien?		×	
	Partys und Filmabende			
30	Filme zeigen und Musik abspielen auf privaten Partys / Filmabenden / Sit-ins	×		
31	Filme zeigen und Musik abspielen, wenn jeder zur Party kommen kann		×	
32	Filme zeigen und Musik abspielen bei öffentlichen Partys (mit / ohne Eintritt)		×	
33	Musik spielen als DJ (in der Disko, wenn ich selbst als DJ die GEMA-Gebühren zahle)	×		

Urheberrecht – Was ist das?

Die Geschwister Konrad und Therese streiten sich …



Arbeitsauftrag:

1. Führt an dieser Stelle in der Klasse eine Blitzumfrage zu der Frage durch. Notiert das Ergebnis an der Tafel.



2 a. Überlege zunächst alleine, was dieser Satz bedeuten könnte!

Zum Glück hat Konrad eine schlaue Schwester (die nur ein wenig besserwisserisch ist): „Lies weiter", rät sie ihrem Bruder. „Paragraf 2 …"

§ (1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:

1. Sprachwerke, wie Schriftwerke, Reden und Computerprogramme;
2. Werke der Musik;
3. pantomimische Werke einschließlich der Werke der Tanzkunst;
4. Werke der bildenden Künste einschließlich der Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke;
5. Lichtbildwerke (…);
6. Filmwerke (…);
7. Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen.

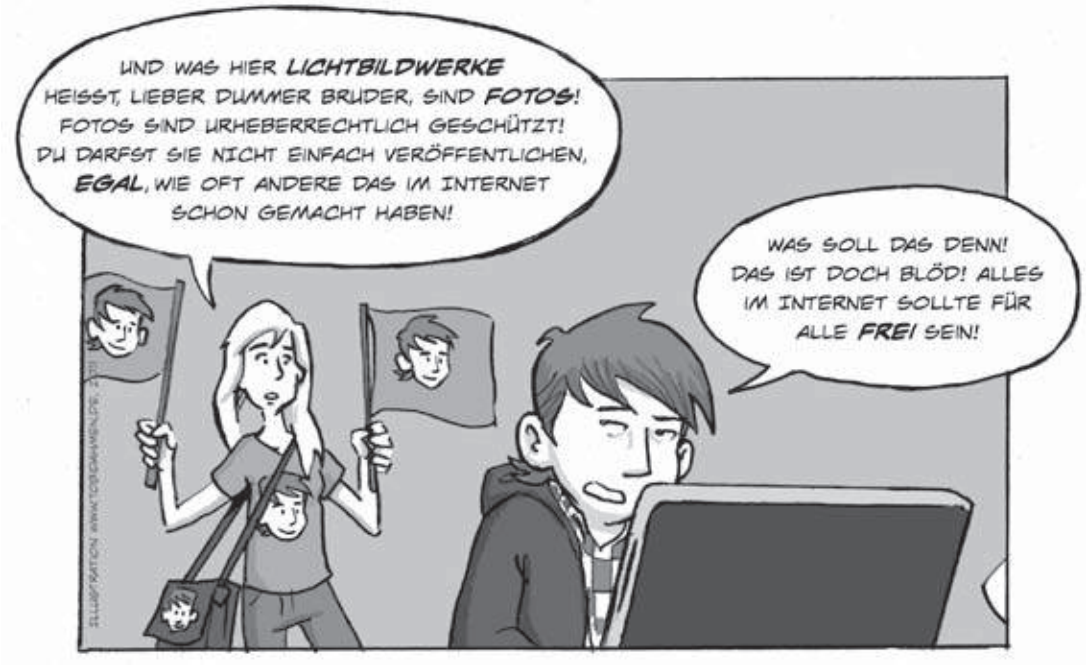
(Quelle: http://www.gesetze-im-internet.de/urhg/__2.html)

Arbeitsauftrag:

2b. Was ist das Urheberrecht? Bearbeitet die Frage in Kleingruppen mit der Methode Placemat.

3. Das Urheberrechtsgesetz ist wie alle Gesetze etwas kompliziert formuliert. Was sind Sprachwerke? Was sind Werke der bildenden Kunst? Klärt die Begriffe (1 bis 7 aus § 2) gemeinsam in der Klasse und findet Beispiele. Erstelle eine Tabelle in deinem Heft:

Begriff	Erklärung	Beispiel
Schriftwerk	Alle geschriebenen Texte	Das Buch „Bis(s) zum Morgengrauen – Twilight“ (Literatur)



4. Ihr seht, dass ganz viele Dinge urheberrechtlich geschützt sind und man sie nicht einfach verwenden darf. Ist das so blöd, wie Konrad meint? Sollten z.B. alle Fotos, Software, Filme und Bücher für alle frei sein?

Diskutiert die Frage anhand dieser vier Beispiele zunächst mit einem Partner und danach in der Klasse.

Fotos und das Urheberrecht



Jeder Mensch in Deutschland hat das Recht am eigenen Bild. Das bedeutet, dass jeder selbst bestimmen kann, ob ein Foto von ihm gemacht wird oder nicht. Eine kleine Einschränkung gibt es dabei: Wenn du auf dem Foto nur „Beiwerk" bist, dann hast du kein Recht, es zu verhindern. Wenn du also vor dem Eiffelturm stehst, dürfen andere Touristen ihn trotzdem fotografieren, auch wenn du auf dem Foto am Rand oder im Hintergrund zu sehen bist. Sie dürfen dieses Foto dann sogar veröffentlichen.
Jeder hat auch das Recht zu bestimmen, ob und welche Fotos von ihm veröffentlicht werden. Dies gehört zu den so genannten Persönlichkeitsrechten. Einige Menschen, Prominente wie Schauspieler, Politiker, Sportler, Musiker, haben ein eingeschränktes Persönlichkeitsrecht. Ihre Fotos darf man veröffentlichen, wenn sie in der Öffentlichkeit entstanden sind. Du darfst Fotos nur veröffentlichen, wenn du sie selbst gemacht hast. Denn man muss auch das Urheberrecht des Fotografen achten, der das Foto gemacht hat.

Arbeitsauftrag:

1. Zeichne einen Entscheidungsbaum mit dem Titel „Darf ich das Foto veröffentlichen?". Schreibe jeweils deutlich JA in grün und NEIN in rot unter die Äste des Baumes.
2. Baue darin folgende Beispiele ein. Du darfst die Kärtchen ausschneiden und aufkleben.

Du hast das Foto selbst gemacht.	Es sind keine Personen zu erkennen.	Die Personen auf dem Foto haben kein Einverständnis gegeben.	**Darf ich das Foto veröffentlichen?**	
Der Fotograf hat ohne Bedingungen (Honorar) zugestimmt.	Die Personen auf dem Foto haben ihr Einverständnis gegeben.	Der Fotograf stellt Bedingungen (z. B. Honorar).	Es handelt sich nicht um Prominente.	Der Fotograf hat keine Erlaubnis erteilt.
Du hast die Bedingungen des Fotografen erfüllt (Honorar bezahlt).	Es handelt sich um Prominente.	Es ist ein fremdes Foto eines Fotografen.	Der Fotograf hat die Erlaubnis erteilt.	Es sind Personen deutlich zu erkennen.

Open Content



Konrad hat Recht: Die Idee war so einfach wie genial. Zu Beginn des dritten Jahrtausends ärgerten sich viele Menschen über das strenge Urheberrecht, v. a. im Internet. Ein Professor namens Lawrence Lessig schuf deshalb ein Modell, wonach man als Urheber freiwillig bestimmte Nutzungen erlauben kann. Creative Commons (CC) heißt dieses Modell und dieses Zeichen zeigt dir an, dass das Werk unter dieser CC-Lizenz steht:

creative commons

Aber so ganz ohne Regeln geht es auch bei Creative Commons nicht:

Logo	Abkürzung	bedeutet
	by	(by = von) Der Name des Urhebers muss genannt werden.
	nc	(non-commercial = nicht kommerziell) Das Werk darf nicht für kommerzielle verwendet werden, also z. B. nicht verkauft werden.
	nd	(non-derivates = keine Abänderungen) Das Werk darf nicht verändert werden.
	sa	(share alike = genau so zu teilen) Geänderte Versionen des Werkes dürfen nur unter der gleichen Lizenz weitergegeben werden.

Arbeitsauftrag:

1. Die Regeln (by, nc, nd und sa) bei Creative Commons können alle frei miteinander kombiniert werden. Malt euch Symbolschilder und stellt euch im Klassenraum in unterschiedlichen CC-Kombinationen auf. Was bedeuten die Kombinationen im Einzelnen?
2. Wie funktioniert die Google-Suche nach lizenzfreien Werken? Finde es heraus und erkläre es kurz deinem Sitznachbarn (Tipp: Schaue mal unter „Erweiterte Suche").

4_1 Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter

Auf vielen Internetseiten werden Inhalte angeboten, die du kostenfrei nutzen darfst, ohne eine Erlaubnis einholen zu müssen. Bei **www.flickr.com** findest du Fotos. Bei der „Erweiterten Suche" kannst du anklicken, dass du nur Fotos sehen möchtest, die unter CC-Lizenz stehen. Probiere es einmal aus!

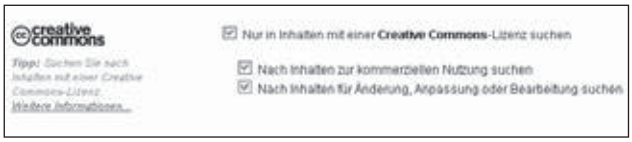


Foto	CC-Lizenz	Autor	Quelle
	by / sa	Thomas Claveirole	http://www.flickr.com/photos/thomasclaveirole/299623633/
	by / nc / sa	affnpack	http://www.flickr.com/photos/affenpack/4635278727/
	by / nd	vince42	http://www.flickr.com/photos/84609865@N00/4998370790/

Arbeitsauftrag:

3. Erkläre die Foto-Beispiele! Unter welcher Lizenz stehen die Fotos? Was darfst du damit machen? Was nicht? Was musst du bei einer Veröffentlichung beachten?

Zusatzaufgabe:

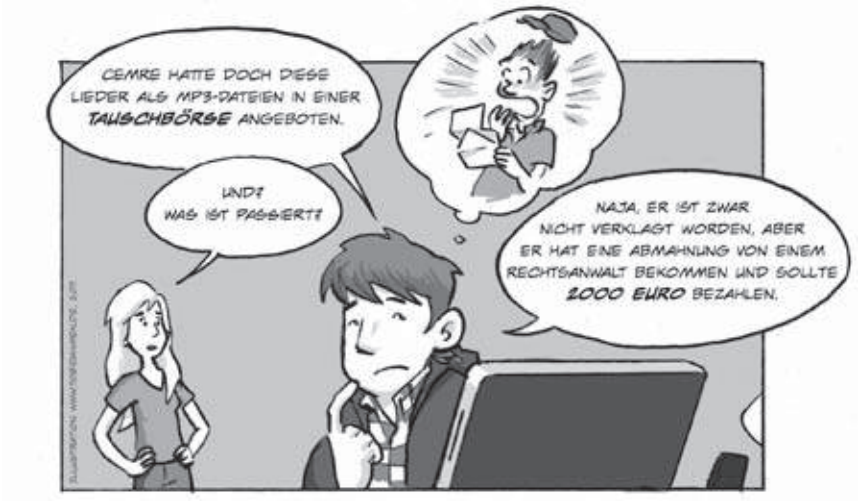
Es gibt noch weitere Beispiele für kostenlos nutzbare Werke, übrigens auch bei Musik. Recherchiere das Stichwort „Netlabels" und mache dir dazu einen Stichwortzettel, auf dem du alles sammelst, was du gefunden hast.

Erstellt ein Handyvideo, unterlegt es mit lizenzfreier Musik von einem Netlabel und ladet es auf ein Videoportal.

Recherchetipp:
http://bit.ly/2nW2wKp

Abmahnungen

Konrad erinnert sich daran, was seinem Freund vor Kurzem passiert ist …



Was sind Abmahnungen eigentlich?

R. TAPPT & Partner

Anwaltskanzlei Dr. R. Tappt & Partner | Postfach 28982 | 83637 Sauberstadt

Cemre Caioglu
Data Highway 13
00300 Surfburg

Dr. R. Tappt & Partner
Rechtsanwälte

Forderungs- und
Vollstreckungsabteilung

Telefon: 88854 / 62352 70
Telefax: 88854 / 62352 71
E-Mail: info@ertappt.de

Bürozeiten: Mo So: 0 24 Uhr

„Lady Gaga, Album The Fame"

Sauberstadt, 12.06.2016

Sehr geehrte Herr Caioglu,

in obiger Angelegenheit zeigen wir an, dass uns die Firma Milkyway Music GmbH mit der Wahrnehmung ihrer rechtlichen Interessen beauftragt hat. Ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Gegenstand unserer Beauftragung ist eine von Ihnen im Internet begangene Urheberrechtsverletzung. Unsere Mandantschaft ist Inhaberin ausschließlicher Rechte an Tonaufnahmen der Künstlerin Lady Gaga mit Bezug auf Filesharing in Peer-to-Peer-Netzwerken („Tauschbörsen").

1. Sie boten im Internet als Nutzer eines so genannten Peer-to-Peer-Netzwerks den oben genannten Tonträger anderen Nutzern durch Freigabe auf Ihrer Festplatte zum Download an.

1.1 Folgende Daten konnte unsere Mandantschaft anlässlich eines Testdownloads feststellen und beweislich dokumentieren lassen:

Datum und Uhrzeit: xx.xx.20xx; xxxUhr
Dateiname: The Fame
IP Adresse: 87.xxx.xx.xx

Der Ersatzanspruch unserer Mandantschaft sowie der Anspruch auf Erstattung von Anwalts- und sonstigen Kosten ist mit einer einmaligen Pauschalzahlung in Höhe von € xxx,00 (netto) zu erledigen.

Enthaltene anteilige Kosten:
- Anwalts- und Gerichtskosten
- die Kosten unserer Inanspruchnahme für dieses Abmahnschreiben sowie
- die Aufwendung, die unsere Mandantin Ihrem Provider für die Auskunftserteilung zu erstatten hatte.

Wir setzen Ihnen für die Zahlung eine Frist bis zum xx.xx.20xx

Mit freundlichen Grüßen

Anwaltskanzlei Dr. R. Tappt

Abmahnungen sind Schreiben, die meistens von Rechtsanwälten verschickt werden. Verletzt jemand das Urheberrecht, z. B. indem er Musikstücke in einer Tauschbörse zum Download anbietet, schaltet der Rechteinhaber (hier: die Plattenfirma) häufig einen Anwalt ein, der den Nutzer schriftlich auffordert, dies zukünftig zu unterlassen. Das nennt man Abmahnung. Dem Angeschriebenen wird in der Regel angedroht, verklagt zu werden, wenn er nicht eine verbindliche Erklärung abgibt, das nicht mehr zu tun. Außerdem muss er die Anwaltskosten und oftmals Schadensersatz bezahlen.

Nicht immer sind Abmahnungen berechtigt, manchmal sind die darin formulierten Geldforderungen zu hoch. Was also tun, wenn man eine Abmahnung erhält?

Arbeitsauftrag:

1. Informiere dich im Internet über Abmahnungen. Stelle auf einer Liste zusammen, wofür du eine Abmahnung erhalten könntest.
   Im Kasten findest du die Seiten, auf denen du recherchieren kannst.

- **http://www.klicksafe.de/nc/themen/rechtsfragen-im-netz/irights/abmahnungen**
- **https://de.wikipedia.org/wiki/Abmahnung**
- **https://www.abmahnwahn-dreipage.de**
- **http://tinyurl.com/zo9o6vb**

2. Suche ein (echtes) Fallbeispiel aus dem Internet heraus und stelle es in der Klasse vor.
   (Benutze die Suchbegriffe „Abmahnung Beispiel Urheberrecht Jugendliche". Oft gibt es solche Fallbeispiele auf den Webseiten von Zeitschriften und Zeitungen.)
   Einige Experten sprachen in den letzten Jahren von einer „Abmahnwelle".
   Recherchiere auch diesen Begriff und erkläre ihn!

3. Entscheide dich durch Ankreuzen für eine Handlungsfolge (Schritte 1 bis 3) und notiere auf der Rückseite des Blattes, wie man sich verhalten sollte, wenn man eine Abmahnung erhält.
   Erläutere außerdem kurz: Warum ist es wichtig, in jedem Fall einen Rechtsanwalt einzuschalten?!

1. Schritt	❍ Ich ignoriere die Post und vernagele den Briefkasten. ❍ Ich informiere sofort meine Eltern und erzähle ihnen alles. ❍ Ich wandere aus nach Tuvalu.
2. Schritt	❍ Ich prüfe sorgfältig, ob bei der Abmahnung wirklich alles stimmt. ❍ Ich bezahle sofort und ohne Verzug. ❍ Ich lasse die Abmahnung erst mal vier Wochen ungelesen liegen.
3. Schritt	❍ Ich wandere aus nach Tuvalu (wenn nicht schon vorher geschehen). ❍ Ich bitte meine Eltern, einen Rechtsanwalt einzuschalten. ❍ Ich frage meine Freunde, was sie tun würden.

Zusatzaufgabe:

Recherchiert zum Thema „Kulturflatrate" und diskutiert das Modell in der Klasse.
Überlegt euch in Teams ein eigenes Konzept und präsentiert es euren Klassenkameraden.

Urheberrecht im Unterricht

Therese bei der Referatsvorbereitung.



Nimm mal an, du sammelst für ein Referat Texte und Bilder (oder auch Videos) aus Zeitungen, Zeitschriften, Büchern oder aus dem Internet. Darfst du sie verwenden? Wie so oft bei Rechtsfragen ist die Antwort nicht ganz einfach:

- Für private Zwecke ist es erlaubt, Texte und Bilder abzulegen, auszudrucken oder zu speichern (das nennt man Privatkopie). Was du nur für dich alleine sammelst, interessiert niemanden. So dürftest du dir eine eigene Bildersammlung über Napoleon anlegen mit allen Bildern, die du zum Thema findest.
- Wie du inzwischen weißt, gilt bei jeder Veröffentlichung das Urheberrecht, und du darfst Werke nicht einfach veröffentlichen, es sei denn, der Urheber erlaubt es (z. B. über eine Creative-Commons-Lizenz).

Aber …

- du kannst ganz unbesorgt sein, wenn du das Referat nur zeigst (z. B. in Form einer PowerPoint-Präsentation). Der Unterricht ist nicht öffentlich und du darfst alle Bilder / Videos / Texte / Audios verwenden, die du magst. Wenn du Handouts verteilen willst, musst du aber beachten, dass von fremden Inhalten nur 15 % verwendet werden dürfen. „Werke geringen Umfangs" dürfen ganz enthalten sein. Du musst schauen, was hierunter fällt, die Regeln sind kompliziert.
- es gibt eine Ausnahme bei so genannten Zitaten. Zitate sind kleine Ausschnitte aus Texten oder Bildern, die eine „Belegfunktion" haben. So darfst du aus einem Buch etwas veröffentlichen (Quelle nennen nicht vergessen!), wenn du damit etwas zeigen möchtest, z. B. zwei Sätze aus einem Buch über Napoleon. Das darf also auch auf einem Ausdruck erscheinen.

> **!** Das Zitatrecht ist festgelegt in § 51 des Urheberrechtgesetzes. Juristen bezeichnen diese Nutzung im Unterricht (ohne Ausdrucke oder Weitergabe) übrigens als nicht öffentliche, unkörperliche Nutzung.

Wie sieht nun ein perfektes Referat aus?

Arbeitsauftrag:

1. Hier findest du Beispiele für Vorgehensweisen bei Referaten. Entscheide, ob sie erlaubt sind oder nicht. Die richtigen Antworten ergeben ein kurzes Lösungswort:

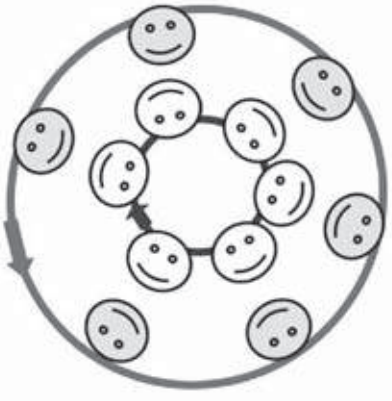
Beispiel	Ist das erlaubt?	Lösung
Zelda hält ein Referat über Robert Pattinson und baut viele Fotos ein, die sie in der Google-Bildersuche gefunden hat. Sie kopiert alle Folien der Präsentation für ihre Mitschüler.	JA = P NEIN = S	
Yan möchte über eine Rede von John F. Kennedy referieren. Er spielt die Audio-Datei der Rede im Unterricht ab.	JA = C NEIN = O	
Xavier findet ein spannendes Buch über Witze im Mittelalter und zitiert daraus einzelne Sätze, die sich auch auf dem kopierten Handout für die Mitschüler wiederfinden.	JA = A NEIN = N	
Wanda hat im Unterricht ein tolles Referat mit vielen Fotos gehalten. Nun stellt sie das Referat auf ihre Facebook-Seite zum Download.	JA = T NEIN = N	
Valentin ist Fan von Mesut Özil. Er speichert alle Fotos, die er finden kann, auf seinem heimischen Computer.	JA = N NEIN = C	
Ursula benutzt für ihr Referat über die Proteinbiosynthese ausschließlich Texte und Fotos mit einer CC-Lizenz. Sie stellt das Referat online.	JA = E NEIN = I	
Tina konnte die Bundeskanzlerin persönlich treffen und hat sie dabei fotografiert. Diese Fotos baut sie in ein Referat über das politische System der Bundesrepublik ein. Das Referat veröffentlicht sie auf der Schulhomepage.	JA = N NEIN = T	

Vergleicht eure Lösungen und diskutiert diese Beispiele in der Klasse.

2. Das perfekte Referat … wie sieht das aus?
Erstelle ein Merkblatt und notiere darauf, was du zum Thema Urheberrecht beachten musst.

3. Besprecht, wie das perfekte Referat auszusehen hat, mit der Methode Kugellager.

Setzt euch in der Klasse zu einem Kugellager zusammen (ein Außenkreis und ein Innenkreis, ihr sitzt euch gegenüber). Erkläre nun deinem Gegenüber, was für dich das perfekte Referat ist (der Außenkreis beginnt). Wechselt nach einer Minute die Rollen. Nach zwei Minuten rückt der Außenkreis im Uhrzeigersinn zwei Stühle weiter. Wiederholt dies insgesamt dreimal.



Videos anschauen und hochladen



Arbeitsauftrag:

1. Bitte beantworte die Fragen A bis J zunächst alleine. Benutze dafür die Rückseite des Blattes. Begründe deine Entscheidung. Tausche dich danach mit deinem Sitznachbarn aus.
2. Fasst an der Tafel zusammen, was ihr bei YouTube (oder anderen Videoportalen) beachten müsst, wenn es um das Urheberrecht geht.

Recherchetipp:
www.youtube.com/t/community_guidelines

Frage
A. Darf ich mir Videos bei YouTube anschauen?
B. Darf ich mir Videos anschauen, die offensichtlich rechtswidrig bei YouTube hochgeladen wurden?
C. Gibt es einen Unterschied zwischen Streaming und Download? Wenn ja, welchen?
D. Darf ich mir Videos auch herunterladen und dauerhaft auf meinem Rechner speichern?
E. Darf ich mir offensichtlich rechtswidrig hergestellte Videos auch herunterladen und dauerhaft auf meinem Rechner speichern?
F. Darf ich eigene (selbst gedrehte) Videos auf YouTube hochladen?
G. Darf ich fremde Videos (z. B. einen Mitschnitt aus dem Fernsehen oder ein Musikvideo) hochladen?
H. Darf ich ein Video in mein Profil bei Facebook einbinden?
I. Darf ich fremde Videos, die ich bearbeitet – z. B. mit fremder Musik unterlegt – habe, hochladen?
J. Darf ich fremde Videos, die ich bearbeitet – z. B. mit eigener Musik oder CC-Lizenz-Musik unterlegt – habe, hochladen?



Urheberrecht offline



Bitte helft dem armen Konrad, der verzweifelt scheint.

Arbeitsauftrag:

1. Teilt euch in folgende Gruppen A bis F auf.
2. Recherchiert auf **www.irights.info** und beantwortet die Fragen.
3. Bereitet ein Stationenlernen zum Thema vor. Jede Gruppe (A bis F) erstellt die Antworten (vielleicht auch in Bildern/Comics) für ihre Station.
4. Führt danach das Stationenlernen durch (s. Material auf der nächsten Seite) und besucht alle Stationen der anderen Gruppen.

Gruppe	A	B	C	D	E	F
Thema	**CDs brennen**	**MP3s erstellen**	**Musik tauschen**	**Spiele und Filme kopieren**	**Filmabende**	**Öffentliche Partys**
Fragen	Was ist eine Privatkopie?	Darf ich eine legal erworbene Original-Musik-CD rippen?	Darf ich eine legal erworbene Musik-CD kopieren und an meinen besten Freund weitergeben?	Gilt das Recht auf eine Privatkopie auch für eine Computerspiel-DVD? oder eine Video-DVD?	Darf ich meine besten Freunde einladen und einen Videofilm anschauen?	Darf ich grundsätzlich eine öffentliche Party (ohne Musik) veranstalten?
	Darf ich jede legal erworbene Musik-CD kopieren?	Darf ich die MP3-Dateien der gerippten CD weiterverkaufen?	Darf ich diese kopierte CD 100fach auf dem Schulhof verteilen?	Darf ich einen Kopierschutz umgehen?	Was muss ich beachten, wenn ich daraus eine öffentliche Veranstaltung (wie Kino) mache?	Muss ich die Veranstaltung bei der GEMA anmelden, wenn ich Musik spiele?
	Darf ich einen Kopierschutz umgehen?	Ich habe drei MP3-Player. Darf ich meine Musik auf alle drei aufspielen?	Verletze ich das Urheberrecht, wenn ich ein Lied per E-Mail-Anhang erhalte und speichere?	Darf ich ein kopiertes Computerspiel / einen kopierten Film weitergeben?	Darf ich ein selbst zusammengeschnittenes Video aus meinen Lieblingsfilmen zu Hause zeigen?	Wie teuer wird das für mich?
	Was ist mit einer Fernsehsendung, die ich vom Festplattenrekorder auf eine CD brenne?	Darf ich einen Kopierschutz umgehen?	Wenn wir uns als Geschwister nur eine CD kaufen, dürfen wir dann die Musik auf alle unsere MP3-Player übertragen?	Darf ich das Original eines Computerspiels / eines Films weitergeben?	Ich zeige an dem Abend ein selbst gedrehtes Video des letzten Urlaubs. Was gibt es zu beachten?	Verletze ich das Urheberrecht, wenn der Veranstalter keine GEMA-Anmeldung gemacht hat?

Stationenlernen

Habt ihr schon einmal ein Stationenlernen gemacht? Wenn nicht, beachtet bitte: Die Lösungen sollte man an einer Station auch selbst erarbeiten können. Eine Möglichkeit ist, die Fragen auf die Vorderseite und die entsprechenden Antworten auf die Rückseite von Karten zu schreiben.

Bitte bereitet Folgendes vor:

- ein Stationenschild mit eurem Thema und euren Namen
- mindestens vier Frage-Antwort-Karten: bitte schreibt die Fragen auf die Vorderseite, die Antworten auf die Rückseite – vielleicht wollt ihr die Karten noch hübsch gestalten?

Benutze folgenden Laufzettel, damit du weißt, welche Station du schon besucht hast:

Laufzettel		
Name:		
Gruppe	**okay**	**Fragen / Kommentare / Notizen**
A. CDs brennen		
B. MP3 erstellen		
C. Musik tauschen		
D. Spiele und Filme kopieren		
E. Filmabende		
F. Öffentliche Partys veranstalten		

Streaming – Was und wo du schauen darfst

Konrad steht mal wieder die Verzweiflung ins Gesicht geschrieben …



Kurze Zeit später erhält Therese eine E-Mail (s. unten), bei der aber leider einzelne Wörter herausgefallen sind:

Arbeitsauftrag:

1. Ergänze die folgenden Wörter im Text:



2. Erstellt aus den Antworten des Experten in eigenen Worten einen kurzen Infoflyer (für eure Parallelklasse/Geschwister/Freunde).

Tipp: Ihr könnt den Flyer auch mit urheberrechtsfreien Bildern und Grafiken verschönern!
Recherchetipps:
http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/
Schwerpunkte 22–24



4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter

Von:	therese@fragfix.de
An:	tillkreutzer@iRights.info
Betreff:	**Streaming-Anfrage**

Liebe Therese,
danke für deine E-Mail. Ich werde versuchen, deine Fragen zu beantworten:

Was ist der Unterschied zwischen Streaming-Seiten und Tauschbörsen?
Wer sich einen _____ bei einem Streaming-Dienst anschaut, stellt selbst keine Inhalte bereit. Bei Tauschbörsen sind z. B. – anders als beim inzwischen geschlossenen Streaming-Dienst kino.to – die Nutzer manchmal auch _____. Statt jedoch eine dauerhafte _____ des Films auf dem eigenen PC zu speichern, wird der jeweilige Film beim Streaming direkt im _____ angezeigt und nur live angeschaut.

Ist das Anschauen von Filmen über Streams im Gegensatz zum Herunterladen generell erlaubt?
Beim Streaming entstehen automatisch eine Reihe von Kopien. Manche dieser Kopien werden auch vom PC des Nutzers in einem _____ oder im Arbeitsspeicher erzeugt. Auch wenn diese spätestens bei einem Neustart des Rechners wieder gelöscht werden (man spricht hier von flüchtigen Kopien), handelt es sich aus urheberrechtlicher Sicht um _____. Und die sind nur mit einer gesetzlichen Gestattung erlaubt (s. Privatkopieschranke).

Was bedeutet Privatkopieschranke?
Die so genannte Privatkopieschranke gestattet, zu rein privaten Zwecken Kopien von _____ zu machen. Das Werk ist in diesem Fall das gestreamte Video, die Kopie ist die mittels Speicherprogramm oder Browser-Plug-In erstellte Datei auf dem eigenen Rechner. Generell gilt diese Nutzungsfreiheit also auch für das Abgreifen von Videostreams. Doch die Privatkopieschranke wurde durch Gesetzesreformen zuletzt insofern eingeschränkt, als Privatkopien nicht mehr erlaubt sind, wenn das Video „offensichtlich _____" ins Netz gestellt wurde. Wenn dies für mich also eindeutig erkennbar ist, darf ich keine Kopie für meine private Sammlung machen.

Darf ich überhaupt keine Streaming-Angebote anschauen?
Klar ist also nur, dass rechtmäßig ins Internet gestellte Inhalte per Streaming auf dem eigenen Rechner angeschaut werden dürfen. Sich die Tagesschau in der ARD- _____ anzusehen, ist also in Ordnung. Bei Streams, die über Portale wie z. B. das geschlossene kinox.to abgerufen werden können, ist das schwieriger zu beurteilen und rechtlich noch nicht endgültig entschieden. Es ist wohl kein Zufall, dass eine _____, die die neuesten Kinofilme „für lau" anbietet, im Südseeinselstaat Tonga registriert ist. Es ist davon auszugehen, dass der Betreiber des Portals nicht die für ein solches Online-Angebot erforderlichen Rechte hat, es sich also wahrscheinlich um eine rechtswidrige Quelle handelt. Vorsicht auch vor unsichtbaren Dialern, Betrugsabos und Viren, Keyloggern oder Trojanern, die man sich auf diesem Weg leicht einfangen kann.

Darf ich von mir heruntergeladene Videostreams selbst online stellen?
Keinesfalls ist es erlaubt, den heruntergeladenen Videostream anschließend für _____ in einer Tauschbörse oder auf der eigenen Webseite zum Download anzubieten. Es ist rechtlich ein großer Unterschied, ob man einen Film aus dem Netz abruft oder ob man einen Film anderen online zur Verfügung stellt. Geschützte Inhalte online zu stellen und damit _____ zu machen, ist nach dem Urheberrechtsgesetz keine private Nutzung und damit verboten, wenn man nicht die _____ des Rechteinhabers hierfür hat. Das gilt unabhängig davon, ob der Anbieter kommerzielle Ziele verfolgt oder nicht.

Darf ich Videos auf meiner Seite einbetten?
Videos im eigenen Blog oder auf der eigenen Homepage _____, ist sehr beliebt und einfach. Nach dem Einbetten wird das Video angezeigt, als sei es dort gespeichert. Tatsächlich bleibt das Video aber an der _____ (dem Videoportal) und wird von dort gestreamt. Auch diesbezüglich stellt sich die Frage, ob das rechtlich ohne Weiteres erlaubt ist. Dafür spricht generell, dass bei allen Videoportalen die Möglichkeit besteht, die gezeigten Videos mit wenigen Klicks auf andere Seiten einzubetten. Das Einbinden auf einer anderen Webseite ist von Seiten der Plattformbetreiber somit ausdrücklich gewollt. Entsprechend wissen auch die Nutzer, die ihre Videos hochladen, in aller Regel davon und sind damit einverstanden. Aber auch hier gilt: Wenn man das Gefühl hat, dass ein Video illegal ins Netz gestellt wurde, sollte man vom Einbetten die Finger lassen.

Ich hoffe, ich konnte dir helfen!
Till Kreutzer, iRights.info

Up- und Downloads – Was ist legal, was illegal?

Konrad und sein Freund Till hören auf dem Heimweg von der Schule das neue David Guetta Album …



Super Sache, aber kann das wirklich so einfach sein? Und ist das überhaupt legal? Darf man Dateien über solche Angebote herunterladen? Was denkt ihr? Macht eine kurze Umfrage in der Klasse.

Arbeitsauftrag:

1. Teilt euch in zwei Gruppen auf und recherchiert im Internet zu beiden Fragen.
2. Bereitet ein Kurzreferat (maximal zehn Minuten) zum Thema vor und stellt es den anderen vor.

Gruppe	**A** **Zum Download öffentlich bereitstellen**	**B** **Dateien selbst downloaden**
Thema	Darf ich der Öffentlichkeit Dateien zum Download anbieten?	Darf ich Dateien herunterladen?
Fragen	Was ist verboten? Was ist erlaubt? Welche technischen Unterschiede gibt es zwischen Tauschbörsen und Filehostern?	
Stichwörter für die Suche in Suchmaschinen	Privatkopieschranke, Vervielfältigung, öffentlich zugänglich machen, Filehoster, Filesharing, Tauschbörse	
Internetadressen	http://irights.info/kategorie/themen/filesharing-streaming http://www.klicksafe.de/themen/downloaden/tauschboersen/ http://www.klicksafe.de/themen/downloaden/urheberrecht/ Artikel: Filehoster - Hehler oder Helfer auf www.spiegel.de („Hehler oder Helfer" in die Suchmaske eingeben)	

3. Erstellt nun Verkehrsschilder für das Bereitstellen und das Herunterladen von Dateien (in Tauschbörsen und über Filehoster) mit folgenden Überschriften:

   Stoppschild: Das ist verboten! Vorfahrtsschild: Das ist erlaubt!

Quiz Urheberrecht

Nr.	Beispiel	Darf ich!	Darf ich nicht!	Kommt drauf an! (Erkläre genauer, wann etwas erlaubt ist und wann nicht!)
	Nutzungen im Internet			
	Tauschbörsen			
1	Downloads aus Tauschbörsen: Spiele, Musik, Filme, Software			
2	Spiele, Musik, Filme, Software öffentlich zugänglich machen			
	YouTube und andere Videoportale (Vimeo, die Plattform kinox.to usw.)			
3	Videos anschauen: Was gilt bei eindeutig rechtswidrig angebotenen Videos?			
4	Videos oder Musik herunterladen			
5	Videos hochladen: Was ist zu beachten, wenn es sich um kommerzielle Inhalte Dritter handelt (TV-Sendungen, Videos, die kommerzielle Musik beinhalten, Karaoke usw.)?			
6	Videos embedden in der eigenen Webseite			
	Filehoster u. Ä. (RapidShare, Megaupload usw.)			
7	Dateien freigeben: Bekanntgeben von Downloadlinks (im Internet, nur für Freunde)			
	Fanseiten			
8	Fremde Fotos einstellen			
9	Fremde Interviews einstellen			
10	Musik oder Filme (oder jeweils Ausschnitte davon) zum Download anbieten			
11	Verlinken von externen Quellen			
12	Verkaufen deiner Lieblings-CD			
	E-Mail, Bluetooth			
13	Versand geschützter Dateien per E-Mail			
14	Versand geschützter Dateien per Bluetooth (Handy)			

Nr.	Beispiel	Darf ich!	Darf ich nicht!	Kommt drauf an! (Erkläre genauer, wann etwas erlaubt ist und wann nicht!)
	Offline-Nutzungen			
	CDs brennen			
15	Für sich			
16	Für Freunde und Verwandte			
17	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof			
18	Zum Verkaufen			
19	Was gilt bei kopiergeschützten CDs?			
	MP3s erstellen / tauschen			
20	Für sich			
21	Für Freunde und Verwandte			
22	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof			
23	Zum Verkaufen (z. B. über eBay)			
24	Was gilt bei kopiergeschützten Dateien?			
	Spiele kopieren (brennen) und tauschen			
25	Für sich (Sicherungskopie), soweit nicht kopiergeschützt			
26	Für Freunde und Verwandte			
27	Für andere (die man nicht kennt) – Beispiel: Tausch auf dem Schulhof			
28	Zum Verkaufen (z. B. über eBay)			
29	Was gilt bei kopiergeschützten Dateien?			
	Partys und Filmabende			
30	Filme zeigen und Musik abspielen auf privaten Partys / Filmabenden / Sit-ins			
31	Filme zeigen und Musik abspielen, wenn jeder zur Party kommen kann			
32	Filme zeigen und Musik abspielen bei öffentlichen Partys (mit / ohne Eintritt)			
33	Musik spielen als DJ (in der Disko, wenn ich selbst als DJ die GEMA-Gebühren zahle)			



4_1 Urheberrecht, Youtube/Video/MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Musik aus dem Internet?**	**Up- und Downloads – Was ist legal, was illegal?**
Kompetenzen	Die Schülerinnen und Schüler leiten Möglichkeiten für den legalen und gleichzeitig kostenlosen Musik-Download ab.	Die Schülerinnen und Schüler erkennen den Unterschied verschiedener Nutzungsformen von Up- und Downloads urheberrechtlich geschützter Materialien.
Methoden	Internet-Recherche, Tabelle, Unterrichtsgespräch, Einzelarbeit, Partnerarbeit	Internetrecherche, Gruppenarbeit, Kurzreferat, Präsentation als „Verkehrsschild"
Material	Arbeitsblatt	Arbeitsblatt, großes Papier, dicke Stifte.
Zeit (in Minuten)	90	135
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Musik aus dem Internet?

Verständlicherweise ist es die Regel, dass Musikrechteinhaber Geld verdienen wollen, und die allermeisten kostenlosen Angebote sind illegal. Aber es gibt eben auch Ausnahmen wie die Lizenz „Creative Commons" oder vereinzelte Angebote. Die „Kindermusikbox" ist so ein Angebot und soll hier als Beispiel dienen. Die Schülerinnen und Schüler sollen über das Problem reden, das bei kostenloser Musik aus dem Internet entstehen kann. Danach sollen sie in die Rolle des Künstlers/der Künstlerin schlüpfen und ihre Sicht der Dinge (Vor- und Nachteile) mit der eigenen Einstellung vergleichen (ebenfalls Vor- und Nachteile). Zum Schluss sollen sie lernen, genau auf eine Webseite zu schauen und das „Kleingedruckte" zu lesen. Auf der Seite ⓘ **www.kindermusikbox.de** unter ⓘ **www.kindermusikbox.de/Lizenzbedingungen/** zu finden

Die Tabelle könnte so aussehen:

Für den Künstler/die Künstlerin		**Für dich**	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**
Viele hören die Musik	Sie verdienen kein Geld	Die Musik ist kostenlos	Die Qualität ist vielleicht nicht gut
Es ist billig herzustellen	Sie haben keine Kontrolle, wo die Musik auftaucht	Ich komme schnell an die Musik	Es ist vielleicht verboten
Sie brauchen keinen Plattenvertrag	Sie werden nicht berühmt	Ich kann sie vorher anhören	Ich bekomme keine CD

Außerdem sollen die Schülerinnen und Schüler verschiedene kostenlose (genauer gesagt für Deutschland GEMA-freie) Angebote zum Musik-Download kennenlernen.
Im vierten Arbeitsauftrag sollen die Schülerinnen und Schüler sich darüber informieren, welche legalen Möglichkeiten es gibt, an Musik zu gelangen. Dies sind:
- über Musikportale gegen Bezahlung
- als Download aus freien Quellen, so unter bestimmten Lizenzen und
- als Aufnahmen aus dem Radio (auch dem Internetradio)

Das Problem ist – wie oben beschrieben – dass es nicht immer einfach ist, zu sehen, ob die Quelle legal ist oder nicht. Deshalb ist es sicher von Vorteil, auf bekannten, seriösen Webseiten zu bleiben.

Aus diesem Grunde auch nochmals der ausdrückliche Hinweis auf den Mitschnitt von Musik aus dem Radio, wobei es keine Rolle spielt, ob die Technik zur Übertragung UKW, DAB oder Internet-Streaming heißt.

4_1 Urheberrecht, Youtube / Video / MP3 (Downloads), Recht am eigenen Bild – Arbeitsblätter methodisch-didaktische Hinweise

Hinweise für die Durchführung

AB 2: Up- und Downloads – Was ist legal, was illegal?

Die Schüler recherchieren über die beiden Nutzungsszenarien „zum Download bereitstellen" und „selbst downloaden". Sie können urheberrechtliche Probleme erkennen und denken über den legalen und illegalen Einsatz der unterschiedlichen Dienstleistungen sowie deren technisch-funktionale Unterschiede (Vergleich Tauschbörse – Filehoster) nach.
Mit dem ersten kurzen Austausch soll der Kenntnisstand (und vielleicht die Meinung) in der Lerngruppe ermittelt werden. Oft ist in diesem Bereich das Unrechtsbewusstsein bei Jugendlichen nicht sehr ausgeprägt, es existiert aber eine diffuse Vorstellung davon, dass es z. B. nicht rechtens ist, Musik weiterzugeben. Vielleicht greift an der Stelle schon die bisherige Arbeit zum Urheberrecht. Teilen Sie die Klasse in zwei Gruppen auf, z. B. nach dem Hausnummernprinzip, bei dem die Schüler durchgezählt werden und jeweils diejenigen mit den geraden und die mit den ungeraden Nummern eine Gruppe bilden. Es ist sicher ratsam, dass in jeder Gruppe Schüler sind, die sich bereits gut mit Tauschbörsen auskennen.

Die Internetrecherche ist nicht ganz einfach. Sie sollten den Schülern und Schülerinnen ausreichend Zeit geben, die Fragen zu beantworten.

Lösungen:

Aufgabe 1: Die David Guetta-Kopie – erlaubt oder nicht?
Till hat die CD illegalerweise heruntergeladen und somit auch illegalerweise zum Download zur Verfügung gestellt. Er hätte wissen müssen, dass die aktuelle Platte der Band nicht kostenlos im Internet zur Verfügung steht. Im Auftrag des Musiklabels sprechen Anwaltskanzleien Abmahnungen wegen unerlaubter Verwertung aus. Till kann also auch zu einem Schadensersatz verklagt werden.

Aufgabe 2: Die Antworten befinden sich in den Sachinformationen.

Aufgabe 3: Textvorschlag Vorfahrtsschild
Bleibt man bei Material, für das die Urheberrechte geklärt sind – sei es, weil es eigenes Material ist oder weil die Rechteinhaber eine Verbreitung erlaubt haben – oder nutzt Filehoster / Tauschbörsen zum rein privaten Gebrauch und nur passiv, ist man meist auf der sicheren Seite.

Lust auf mehr?
- Lebensweltbezug: Ist der Mitschnitt von Musik bei Videos auf YouTube legal? Diese Frage können Sie als Zusatz- oder Hausaufgabe geben.
- Ähnlich wie bei Musik verhält es sich mit Filmen, hier könnten Sie die Schülerinnen und Schüler ebenfalls recherchieren lassen.

Musik aus dem Internet?

Deine Freundin Anna hat dir vor kurzem erzählt,
dass sie sich Lieder aus dem Internet heruntergeladen hat.
Bisher hast du immer gedacht, dies sei verboten.
Auch dein Vater hat dir so etwas erzählt und
in den Nachrichten hört man das doch auch immer.

Arbeitsaufträge:

1. Stelle dir vor, du bist ein bekannter Musiker, der auch schon einige CDs gemacht hat. Würdest du wollen, dass man deine Lieder auch umsonst aus dem Internet bekommen kann? Diskutiert dies in der Klasse!

2. Setze dich mit einer Partnerin/einem Partner zusammen und überlege, welche Vorteile und Nachteile es hat, wenn man Musik kostenlos aus dem Internet herunterladen kann. Füllt die Tabelle alleine aus und vergleicht dann:

Für den Künstler/die Künstlerin		**Für dich**	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**

Selbstverständlich ist es verboten, Musik kostenlos aus dem Internet herunterzuladen, wenn der Künstler dies nicht erlaubt. Im Laden musst du ja auch für eine CD bezahlen. Auf **www.kindermusikbox.de** *ist das anders, der Künstler hat dort seine Musik „freigegeben" und jeder darf sie sich kostenlos anhören. Aber das ist eigentlich eine Ausnahme, denn normalerweise muss man für die Lieder bezahlen.*

www.kindermusikbox.de
www.jamendo.de
https://archive.org/details/audio

3. Schaue dir die Seiten aus dem Kasten genau an. Wo steht, dass du die Musik kostenlos benutzen darfst? Arbeitet zu zweit und zeige es deiner Partnerin/deinem Partner.

4. Dein Wunschlied läuft den ganzen Tag im Radio rauf und runter. Informiere dich, ob du Lieder aus dem Internetradio aufnehmen darfst oder nicht. Falls ja, wie darfst du das Lied nutzen? Ist die Weitergabe erlaubt? Das Anfertigen einer Kopie? Oder das Kopieren auf einen mp3-Player?

Informiere dich hier, wie du Musik aus dem Internet legal nutzen darfst:

www.irights.info und
www.respectcopyrights.de

5

5|1 Internet

5|2 PC-Sicherheit

5|3 Passwörter

Internet, PC-Sicherheit und Passwörter



Übersicht der Bausteine:

- **Internet** | **Arbeitsblätter**
- **PC-Sicherheit** | **Arbeitsblätter**
- **Passwörter** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Wie finde ich, was ich suche? Suchmaschinen kompetent nutzen
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmaschine/LH_Zusatzmodul_Suchmaschinen_klicksafe.pdf



Safer Smartphone – Sicherheit und Schutz für das Handy
Arbeitsmaterial für den Unterricht – Heft 2
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/SaferSmartphone_Heft2.pdf



Passwortübung Grundschule
http://www.surfen-ohne-risiko.net/fileadmin/media/documents/Passwort-Schluessel-Automat/Passwort-Schluessel_Uebung-Beispiel.pdf



klicksafe to go
Datensatz – Datenschatz
Warum Datenschutz und Sicherheit wichtig sind
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf

Internet, PC-Sicherheit und Passwörter



5_1 Internet – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Wo ist Klaus?**	**Vor- und Nachteile der Internet-Nutzung für Kinder**
Kompetenzen	Die Schülerinnen und Schüler listen die Handlung des Klicksafe-Spots auf, erkennen die Zusammenhänge zur Internet-Sicherheit und gestalten eine Lernhilfe in Form eines Plakats.	Die Schülerinnen und Schüler veranschaulichen die Ergebnisse der KIM-Studie in Form einer Zeitungsmeldung und beurteilen sie gemeinsam. Sie benutzen die Klassifizierung von Livingstone und leiten daraus eigene Beispiele ab, mit denen sie ein Plakat für jüngere Schülerinnen/Schüler kreieren.
Methoden	Tabelle, Plakat	Statistik-Analyse, Tabelle, Plakat
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	nein

Hinweise für die Durchführung

AB 1: Wo ist Klaus?

Grundlage des Arbeitsblattes ist der Werbe-Spot „Wo ist Klaus?" der EU-Initiative klicksafe. Er ist kostenlos im Internet zu sehen auf der Internetseite ⓘ **www.klicksafe.de**
Daran sollen die Schülerinnen und Schüler sich die dargestellten Probleme (gewalthaltige Seiten, pornografische Inhalte, gewalthaltige Spiele und pädophile Kontakte) erarbeiten.
Als Produkt soll ein Plakat mit Tipps zur sichereren Nutzung entstehen.

AB 2: Vor- und Nachteile der Internet-Nutzung für Kinder

Die Schülerinnen und Schüler erkennen durch die Auswertung der KIM-Studie Probleme, die im Internet auftauchen können und beschäftigen sich intensiv mit diesen, indem sie Regeln für sicheres Chatten formulieren.
Wie oben, ergänzt durch eine Statistik der KIM-Studie die die Schülerinnen und Schüler in Textform zusammenfassen sollen. Die Vorgabe der Kategorien von Sonia Livingstone ist sicherlich anspruchsvoll und sie bedürfen der Erläuterung und vielleicht auch der konkreten Beispiele, wobei die Unterscheidung nach „Empfänger/Rezipient", „Teilnehmer" und „Handelnde/Akteur" sicherlich anschaulich ist, aber auch manchmal schwierig zu unterscheiden.

		Content Kind als Rezipient	**Contact** Kind als Teilnehmer	**Conduct** Kind als Akteur
Chancen	Bildung, Lernen und digitale Kompetenz	Bildungsressourcen	Kontakt mit Gleichgesinnten	Eigeninitiative oder gemeinsames Lernen
	Teilnahme und soziales Engagement	Allgemeine Informationen	Austausch in Interessengruppen	Konkrete Formen sozialen Engagements
	Kreativität und Selbstdarstellung	Ressourcenvielfalt	Eingeladen/inspiriert werden, kreativ zu sein oder mitzumachen	Erstellung von benutzergenerierten Inhalten
	Identität und soziale Beziehungen	Beratung (Persönliches/Gesundheit/Sexualleben usw.)	Soziale Netzwerke, Erfahrungen mit anderen teilen	Ausdruck eigener Identität
Risiken	Kommerzielle Interessen	Werbung, Spam, Sponsoring	Verfolgung/Sammlung von persönlichen Informationen	Glücksspiel, illegale Downloads, Hacken
	Aggression/Gewalt	Gewaltverherrlichende/grausame/volksverhetzende Inhalte	Mobbing, Belästigung oder Stalking	Andere mobben oder belästigen
	Sexualität	Pornographische/schädliche Inhalte	Treffen mit Fremden, missbräuchliche Annäherungsversuche	Erstellen/Hochladen von pornographischem Material
	Werte	Rassistische/verzerrte Informationen/Ratschläge (z. B. Drogen)	Selbstverletzung, ungewolltes Zureden/Überredung	Ratschläge z. B. zu Selbstmord/Magersucht geben

Lust auf mehr? Die KIM-Studie wird alle zwei Jahre erhoben und unter ⓘ **www.mpfs.de** veröffentlicht. Dort finden sich zahlreiche andere statistische Daten zur Mediennutzung von Kindern.

Wo ist Klaus?



Es klingelt … und die komischsten Typen stehen vor der Türe und fragen nach Klaus. Was macht die Mutter? Sie öffnet bereitwillig die Türe und lässt alle hinein.

Wie im wahren Leben?
Nein, sicherlich nicht. Aber im Internet? Der Video-Spot der EU-Initiative klicksafe.de macht es in Form eines Werbe-Clips deutlich: Es gibt Gefahren im Internet und Kinder sollten davor geschützt werden.

Schaue dir den Werbe-Spot auf der Webseite der EU-Initiative klicksafe.de an: **www.klicksafe.de**

1. Arbeitsauftrag:
Fülle folgende Tabelle aus:

Szene	Wer kommt?	Welches Problem wird dargestellt?	Wie könnte das Problem im Internet auftreten?
Szene 1			
Szene 2			
Szene 3			
Szene 4			

Bildet mehrere Gruppen (4 – 5 Schüler pro Gruppe).

2. Arbeitsauftrag:
Sammelt Tipps, wie das Surfen im Internet für Kinder sicherer sein kann. Formuliert (oder zeichnet) diese gemeinsam auf einem Plakat.

Ruft folgende Internetseite auf:
www.klicksafe.de/fuer-kinder/internet-abc/sicher-surfen/wissen-wies-geht
Dort findet ihr Tipps zum sicheren Surfen im Internet!

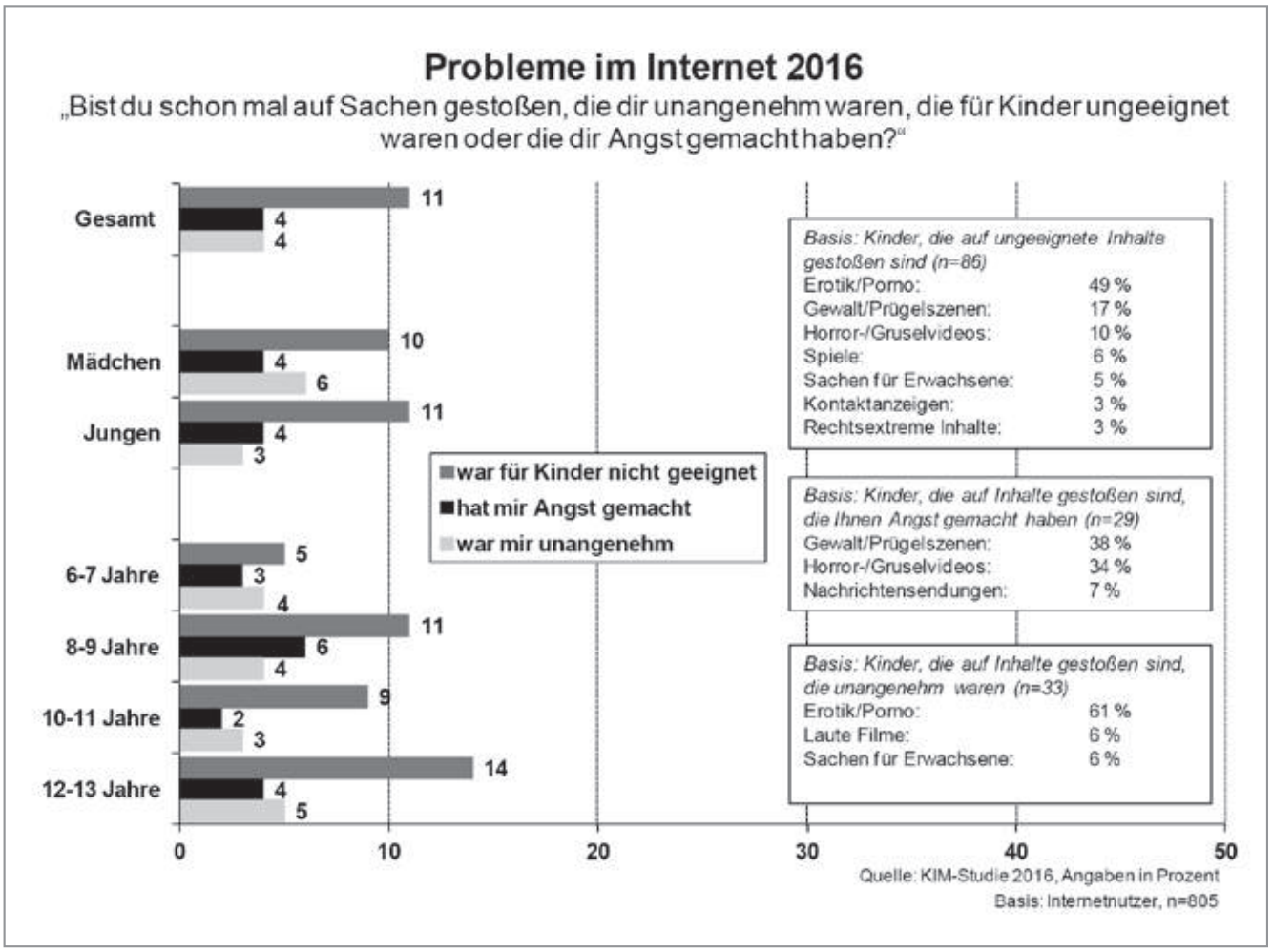
3. Arbeitsauftrag:
Vergleicht eure Tipps mit denen von klicksafe.de und ergänzt sie evtl. auf eurem Plakat.

Vor- und Nachteile der Internet-Nutzung für Kinder (1/2)

Das Internet ist aus eurem Alltag nicht mehr wegzudenken und auch viele jüngere Kinder nutzen das Internet bereits, häufig über Smartphones und mit einem ständigen Online-Zugang.

Wie sich diese Entwicklung in den letzten Jahren vollzog, zeigt die Grafik aus der Studie „Kinder + Medien, Computer + Internet", kurz „KIM-Studie", die alle zwei Jahre repräsentativ in Deutschland erhoben wird:

Entwicklung Internet-Nutzer 2006 – 2012
– Nutzung zumindest selten –



Vor- und Nachteile der Internet-Nutzung für Kinder (2/2)

Neben den zahlreichen Vorteilen, die sich für Kinder bei der Nutzung des Internets ergeben, gibt es leider auch viele Nachteile. Die englische Psychologin Sonia Livingstone entwickelte in der Studie „EU Kids Online" folgendes Raster von Chancen und Risiken:

	Bereich	Kind als Rezipient	Kind als Teilnehmer	Kind als Akteur
Chancen	Lernen			
	Soziales Engagement			
	Kreativität			
	Soziale Beziehungen			
Risiken	Kommerzielle Interessen			
	Aggression/ Gewalt			
	Sexualität			
	Werte			

Arbeitsaufträge:

1. Bitte wertet das Diagramm der KIM-Studie aus. Fasst das Ergebnis in Form einer kurzen Zeitungsmeldung (Überschrift und kurzer Text) zusammen.

2. Hättet ihr diese Zahlen erwartet? Bitte diskutiert – zunächst in kleinen Gruppen, danach mit der ganzen Klasse – was diese Entwicklung bedeutet. Welche Veränderungen ergeben sich daraus?!

3. Bitte setzt euch zu zweit zusammen und füllt das Raster von Sonia Livingstone mit Beispielen. Klärt zuvor in der Klasse, was unter Rezipient, Teilnehmer und Akteur zu verstehen ist. Findet euch danach in 6er-Gruppen zusammen und stellte eure Ergebnisse gegenseitig vor und ergänzt das eigene Raster. Fasst danach die Ergebnisse der Klasse an der Tafel zusammen.

4. Setzt euch danach wieder in die 6er-Gruppe und erstellt ein Plakat mit dem Titel „Sicheres Surfen im Internet", das man in einer Grundschulklasse aufhängen könnte.

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Digitale Datenspuren im Alltag**	**Hat das Internet ein Gedächtnis?**
Kompetenzen	Die Schülerinnen und Schüler übertragen ein fiktives Beispiel eines Tages ohne Datenspuren in Form einer Reportage auf die Realität und erfassen, an welchen Stellen der Autor Datenspuren hinterlassen hätte.	Die Schülerinnen und Schüler führen eine Internet-Recherche über das digitale Archiv www.archive.org durch und reflektieren über das Für und Wider der dauerhaften Speicherung digitaler Daten.
Methoden	Textanalyse, Vorlesen, Partnerarbeit	Pro- und Contra-Tabelle, Einzelarbeit, Unterrichtsgespräch, Textanalyse
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	45	90
Zugang Internet/PC	Nein (Ja, bei Recherche zur Qualität der Daten)	ja

Hinweise für die Durchführung

AB 1: Digitale Datenspuren im Alltag	An einem Text, der einen Selbstversuch schildert, einen Tag ohne Datenspuren zu verleben, sollen die Schülerinnen und Schüler erfahren, wie wir alltäglich (digitale) Datenspuren hinterlassen. Danach sollen sie dies auf ihre eigene Situation übertragen. Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler für die (digitalen) Datenspuren im Alltag sensibilisiert werden. Ein Einstieg könnte über die Frage erfolgen, wer alles weiß, dass die Schülerin / der Schüler jetzt und hier ist. Etwa: Wer weiß, dass du jetzt hier bist? Neben – hoffentlich – den Eltern könnten dies ihre Mobilfunkanbieter, über die Ortungsfunktionen WhatsApp und Facebook oder ähnliche Anwendungen sein oder sogar die Polizei, wenn auf dem Schulweg eine Kamera zur Überwachung des öffentlichen Raumes installiert ist. Lassen Sie den Text von einem guten Leser / einer guten Leserin vorlesen oder tun sie es selbst, vielleicht mit etwas Dramatik und Spannung in der Stimme. Die anschließende Phase der ersten Eindrücke könnten Sie wie die Methode „Blitzlicht" durchführen, also Meldungen ohne Kommentare der anderen oder auch die Meldungen direkt zur Diskussion stellen. Das Beispiel aus der Berufswelt eines Erwachsenen enthält einige Merkmale, die für Kinder und Jugendliche (noch) nicht relevant sind, so Zeiterfassungssysteme, Mautbrücken oder Kreditkarten. Nichtsdestotrotz ist es ein alltägliches Beispiel, das in dieser Form vielleicht den Eltern passieren kann. Die Auflistung der Datenspuren fällt sicherlich leicht, eine genaue Auflistung der erhobenen Daten finden Sie in den Sachinformationen (so werden beim Handy die Verbindungsdaten, aber nicht die Inhalte gespeichert, ebenso beim E-Mailing oder SMS). Sie könnten den Einstieg wieder aufgreifen und das Beispiel auf die eigene Alltagssituation übertragen lassen und deutlich machen, inwieweit auch Kinder und Jugendliche Datenspuren im Alltag hinterlassen. Die Idee für eine Vertiefung ist als Vorschlag für interessierte Schülerinnen / Schüler zu verstehen und mit einem positiven Ergebnis nur sehr schwierig zu realisieren (es ist fast unmöglich, keine Datenspuren zu hinterlassen!).
AB 2: Hat das Internet ein Gedächtnis?	Das digitale Archiv ist Thema dieses Arbeitsblattes. Darin werden frühere Versionen von Internetseiten gespeichert. Im zweiten Arbeitsauftrag werden die Schülerinnen und Schüler mit der These konfrontiert, dass auch für digitale Daten ein Verfallsdatum eingeführt werden sollte. Dies sollen die Jugendlichen als Pro und Contra gegenüberstellen. Zum Schluss schließlich wird auf die Tatsache eingegangen, dass viele Jugendliche heute sehr freizügig mit ihren Daten im Internet umgehen. Sie sollen sich vorstellen, wie es wäre, wenn diese Daten (Beschreibungen, Fotos, Videos, Forenbeiträge) in zehn Jahren in die Hände anderer Menschen (angegeben sind Beispiele) fallen. Dies kann sehr peinlich sein.

Lust auf mehr?

- Seit 2014 gibt es auch gegenüber Google ein „Recht auf Vergessen". Der Europäische Gerichtshof entschied, dass Google auf Antrag Suchergebnisse löschen muss (Das Original-Urteil ist hier zu finden: ⓘ **http://bit.ly/U6yFxH**). Eine Rechtsgrundlage findet sich jetzt auch in Art. 17 DSGVO. Vielleicht gibt dieses Thema Anregung für ein interessantes Referat eines Schülers / einer Schülerin.
- Schon 2008 hat der Journalist Christoph Drösser in der Zeitung „DIE ZEIT" einen Artikel mit dem Titel „Das digitale Alexandria" geschrieben. Die Schüler lesen den Artikel und fassen ihn in eigenen Worten zusammen: ⓘ **www.zeit.de/2008/04/OdE13-Wissen**

Hat das Internet ein Gedächtnis?

Der Amerikaner Brewster Kahle hatte schon zu Beginn des Internets in seiner heutigen Form einen Traum: Er wollte ein digitales Archiv schaffen und das Internet archivieren. Unmöglich? Seit 1996 sammelt sein „Internet-Archiv" (**www.archive.org**), und hatte bis 2014 über 18 Petabyte (das sind 18.000.000.000.000.000 Byte) archiviert, das in vier Rechenzentren auf 20.000 Festplatten gespeichert ist. Sein Internet-Archiv steht (allerdings mit Spiegelservern zum Beispiel in Kairo) in San Francisco und ist mittlerweile offiziell als Bibliothek von Kalifornien anerkannt. Mit einer speziellen Soft-ware werden Momentaufnahmen von Webseiten gespeichert. Auf diese Weise sind über 400 Milliarden Seiten (für immer?) zugänglich.

Mit der „Wayback-Machine" kann man sich z. B. die Seiten von **www.klicksafe.de** *anschauen. Über eine Datumsliste kann auf die gespeicherten Seiten zugegriffen werden.*

Hier findest du eine Video-Dokumentation über das Archiv: **https://vimeo.com/59207751** *(auf Englisch).*

Arbeitsaufträge:

1. Begib dich auf eine digitale Zeitreise und rufe frühere Versionen von Webseiten auf. Du darfst private, bekannte oder auch die Schulhomepage nehmen. Vergleiche die alte und die aktuelle Version. Was fällt dir auf?

2. Es gibt immer wieder die Forderung nach einem „Recht auf Vergessen", also der Möglichkeit, digitale Daten auch wieder (endgültig) löschen zu dürfen.
   Lies nun folgende Artikel in der Zeitschrift „Heise" mit einer Pro- und Contra-Diskussion zu diesem Thema und aus der Zeitung „Die Zeit" mit der Idee des „digitalen Radiergummis":

   http://www.heise.de/newsticker/meldung/Pro-Contra-Das-Recht-auf-Vergessen-im-Internet-2189293.html

   http://www.zeit.de/digital/datenschutz/2011-01/radiergummi-vergessen-schoenberger

   https://www.heise.de/newsticker/meldung/Recht-auf-Vergessenwerden-Google-erhielt-bislang-2-4-Millionen-URL-Loeschanfragen-3981437.html

   Erstelle eine Liste mit den Vor- und Nachteilen eines „Rechts auf Vergessen". Diskutiert diese Forderung anschließend in der Klasse. Bewertet die Argumente und ergänzt eure eigene Liste. Zu welchem Ergebnis kommst du persönlich? Begründe!

3. Stelle dir vor, in zehn oder zwanzig Jahren stoßen folgende Menschen auf die Dinge (z. B. Fotos, Foren-Einträge, Texte, Bilder, Videos), die du heute im Internet hinterlassen hast:

   Welche Folgen könnte das für dich haben! Schreibe sie in einer Tabelle auf!

a. deine Mutter / dein Vater	
b. deine Ehefrau / Partnerin	
c. deine Kinder	
d. dein Arbeitgeber	
e. deine (wichtigen) Kunden	
f. deine Arbeitskollegen	



5_1 Internet – Arbeitsblätter
5_2 PC-Sicherheit – Arbeitsblätter
5_3 Passwörter – Arbeitsblätter

Übersicht über die Arbeitsblätter

A Informations– und Bewertungskompetenz

AB	Titel	Methoden	Lernziel	Anspruch	Zeit in Std. à 45 Min.	Zugang Internet/PC
AB 1	Richtig Fragen stellen	Frage-Antwort-Spiel, Onlinerecherche, Online-Jeopardy	Effektives und zielgerichtetes Fragen lernen durch Zerlegen und Umformulieren von Fragestellungen	▶●● (auch in Kl. 4 mögl.) Kombinierbar mit AB 2	1	nein (nur für Aufg. 4 notwendig)
AB 2	Kindersuchmaschine <–> Erwachsenen-suchmaschine	Onlinerecherche, Vergleich, Podcast	Vergleich von Kindersuch-maschinen mit Erwachsenen-suchmaschinen	▶●● (auch in Kl. 4 mögl.) Kombinierbar mit AB 1	1 2*	ja
AB 3	Suchtipps	Tafelbild Venn-Diagramme, Onlinerecherche, PowerPoint-Karaoke	Effektives und zielgerichtetes Suchen durch Erlernen von Suchtechniken	▶▶●	1	ja
AB 4	Suchergebnisse beurteilen: Orientierung auf der Ergebnisseite	Screenshot einer Suchseite, Zuordnen von Begriffen	Erlangen eines ersten Überblicks auf der Suchseite	▶●● Kombinierbar mit AB 5 u. 6	1	ja
AB 5	Suchergebnisse beurteilen: Quellen einschätzen	Screenshot einer Ergebnisseite, Zuordnen und Bewerten von Quellen	Schnelle Einordnung und Beurteilung von Ergebnissen im Bezug auf Urheber und Glaubwürdigkeit einer Quelle	▶●● Kombinierbar mit AB 4 u. 6	1	nein
AB 6	Suchergebnisse beurteilen: Der Checkbogen	Checkbogen, Webseitencheck	Tiefergehende Beschäftigung mit einer Internetquelle durch Beurteilung des Urhebers anhand eines Checkbogens	▶▶● Kombinierbar mit AB 4 u. 5	1	ja

Auf ⓘ **www.klicksafe.de** im Bereich Suchmaschinen finden Sie zwei weitere Projekte aus diesem Bereich zum Download: „Google, dmoz.de und Metager im Test“ und „Unangenehme Inhalte“

* mit Podcast

Schwierigkeitsgrade

▶●● **einfach:** geeignet ab Klasse 5
▶▶● **mittleres Niveau:** geeignet ab Klasse 8
▶▶▶ **anspruchsvoll:** geeignet ab Klasse 10

B Einsatz von Suchmaschinen im Unterricht

AB	Titel	Methoden	Lernziel	Schwierigkeitsgrade und Kombinationsvorschläge	Zeit in Std. à 45 Min.	Zugang Internet/PC
AB 7	Methodentraining: Die 4-Schritte-Methode – Suchergebnisse richtig verwenden und ordentlich verwalten	4-Schritte-Methode	Kennenlernen einer Methode zur Quellenkritik und zur Abspeicherung von Recherchematerial	▶▶● Kombinierbar mit AB 5 u. 6	2	ja

Auf ⓘ **www.klicksafe.de** im Bereich Suchmaschinen finden Sie zwei weitere Projekte aus diesem Bereich zum Download: „Broadcast Yourself – YouTube als Suchmaschine nutzen" und „Einen Klassenausflug mit einer Suchmaschine planen"

C Sachwissen zum Thema Suchmaschinen und Medienkritik

AB	Titel	Methoden	Lernziel	Schwierigkeitsgrade und Kombinationsvorschläge	Zeit in Std. à 45 Min.	Zugang Internet/PC
AB 8	So funktionieren Suchmaschinen	Textarbeit, Funktionszeichnung	Verstehen der Funktionsweise von Suchmaschinen durch exemplarisches Betrachten der Suchmaschine Google	▶▶▶	1 2*	ja
AB 9	Einfluss von Suchmaschinen	Textarbeit, Think – Pair – Share	Reflexion über den Einfluss von Suchmaschinen	▶▶▶	2	nein
AB 10	Datenschutz und Nutzerinformationen in Suchmaschinen	Gruppen	Kennenlernen von Datenschutzaspekten und Anstoß zu einem kritischen Nutzungsverhalten	▶▶▶	3	ja

* mit Funktionszeichnung

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**
Titel	**Richtig Fragen stellen**
Ziele	Effektives und zielgerichtetes Fragen lernen durch Zerlegen und Umformulieren von Fragestellungen
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1** (auch in Kl. 4 möglich) Kombinierbar mit AB 2
Methodische Hinweise und Lösungen	**Aufgaben 1 und 2:** In einer Frage-Antwort-Übung lernen die Schüler, Fragen zu stellen. Der nächste Schritt besteht darin, Fragen so zu formulieren, dass sie von einer Suchmaschine verstanden werden (siehe Infokasten „Fragetricks" auf AB). **Lösung:** ■ Wie lautet der **Fachbegriff** für ein **Tuwort**? ■ **Wie viele Sinnesorgane** gibt es? *Trick Umformulierung: [Anzahl Sinnesorgane]* ■ Welches ist der **größte(r)** der 3 **Stadtstaaten** in **Deutschland**? ■ Wie heißt die **deutsche Regierungschefin**? *Trick Synonyme: [Bundeskanzlerin]* ■ **Woher kommt** der **Tiger** ursprünglich? *Trick Umformulierung: [Herkunft Tiger]* ■ Wie heißt die **Hauptstadt** von **Neuseeland**? **Aufgabe 3:** Im Plenum Auflösung der Aufgabe 1 und Sammeln der Tricks aus dem Infokasten. Bei ausreichend Zeit können die einzelnen Suchanfragen auch durchgeführt werden. *Mögliches Tafelbild: „Tricks für eine gute Suchanfrage"* ■ Herausfiltern von Schlüsselbegriffen, z. B. durch Unterstreichen ■ Finden von anderen Begriffen mit gleicher (Synonym) oder ähnlicher Bedeutung ■ Umformulierung, z. B. durch Substantivierung ■ Auf richtige Rechtschreibung achten (Hinweis: Die bekanntesten Suchmaschinen wie Google, Yahoo oder Bing besitzen eine Rechtschreibkorrektur. In Kindersuchmaschinen muss die richtige Schreibweise beachtet werden.) **Aufgabe 4 (falls Internet und PCs vorhanden):** Die Schüler können nun in Partnerarbeit eine Suchanfrage online in der Suchmaschine **www.fragfinn.de** ausprobieren. In einem Klassengespräch kann ausgewertet werden, welche Suchtricks sie bei ihrer Suche angewendet haben. **Variation:** Gemeinsame Suche nach einem aktuellen Unterrichtsthema und Effektivitätsanalyse. Wer hat am schnellsten mit welcher Methode das richtige Ergebnis/einen geeigneten Inhalt gefunden? **Tipp:** Online-Jeopardy erstellen, d. h. Antworten vorgeben, Fragen finden **http://jeopardylabs.com/** (englische Version, aber deutsche Fragestellungen möglich) **Lösung Zusatzaufgabe/Hausaufgabe:** ■ Suchanfragen, einfach, eindeutig ■ anderen Begriffen, ähnlicher oder gleicher Bedeutung ■ Umformulierung ■ richtige Rechtschreibung
Methoden und Organisationsformen	Frage-Antwort-Spiel, Onlinerecherche, Online-Jeopardy; Einzelarbeit, Partnerarbeit, Klassengespräch
Zugang Internet / PC	nein (nur für Aufgabe 4 notwendig)
Kapitel 1	Tipps & Tricks beim Suchen

„Der, die, das, wer, wie, was – wieso, weshalb, warum – wer nicht fragt, bleibt dumm!" So hieß es in der berühmten Fernsehsendung „Sesamstraße". Richtig Fragen zu stellen, ist manchmal gar nicht so einfach.



Arbeitsaufträge:

1. Kannst du gute Fragen stellen? Schreibe die richtigen Fragen zu folgenden Antworten in die Spalte „Frage":

Antwort	**Frage**	**Fragetrick** (siehe Aufg. 3)
Der Fachbegriff für ein Tuwort lautet Verb.		
Es gibt fünf Sinnesorgane.		
Berlin ist der größte der drei Stadtstaaten in Deutschland.		
Die deutsche Regierungschefin heißt Angela Merkel.		
Der Tiger kommt ursprünglich aus Asien.		
Die Hauptstadt von Neuseeland heißt Wellington.		

2. **Wusstest du schon:** Wenn du in einer Suchmaschine nach etwas suchst, dann musst du nicht die ganze Frage eingeben! Warum? Lies dir zunächst den Infokasten durch.

3. Unterstreiche in deinen Fragen aus dem ersten Arbeitsauftrag einzelne Wörter, die sich als Suchbegriffe eignen. Welche Fragetricks aus dem Infokasten könnte man hier außerdem anwenden? Schreibe sie in die Spalte „Fragetrick".

4. **Partnerarbeit:** Stellt euch nun gegenseitig eine weitere Frage (z. B. aus euren Schulfächern), zu der ihr in der Suchmaschine ⓕ **www.fragfinn.de** die Antworten finden dürft. Wendet dabei die Fragetricks aus dem Infokasten an.

Fragetricks:

- Internet-Suchmaschinen verstehen einzelne Wörter besser als ganze Sätze. Daran solltest du bei deiner Suche im Netz denken und deine Suchanfragen möglichst einfach und eindeutig halten.
- Du kannst auch nach anderen Begriffen mit ähnlicher oder gleicher Bedeutung suchen, z. B. [Bundeskanzlerin] oder [Regierungschefin].
- Manchmal ist es auch sinnvoll, eine Umformulierung zu versuchen, z. B. [woher kommt] = Frage nach der [Herkunft].
- Achte auf die richtige Rechtschreibung der Suchbegriffe. Eine Suchmaschine sucht alle Seiten nach genau deiner Abfolge von Buchstaben. Bei falscher Schreibweise können auch falsche Suchergebnisse kommen.

Frage	**Suchbegriffe/Suchtricks**	**Antwort**	**Adresse, wo ich die Antwort gefunden habe**
…	…	…	…

Zusatzaufgabe/Hausaufgabe:
Was solltest du bei einer guten Suchanfrage beachten? Unterstreiche die wichtigsten Begriffe im Kasten Fragetricks!

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 2**
Titel	**Kindersuchmaschine vs. Erwachsenensuchmaschine**
Ziele	Vergleich von Kindersuchmaschinen mit Erwachsenensuchmaschinen
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1 / mit Podcast: 2** (auch in Kl. 4 möglich) Kombinierbar mit AB 1

Methodische Hinweise und Lösungen

Studien haben gezeigt, dass bereits sehr junge Kinder (GS-Alter) in Suchmaschinen für Erwachsene suchen, auch wenn Kindersuchmaschinen für ihr Alter besser geeignet wären bzgl. Übersichtlichkeit, Anspruch der Texte, thematischer Ausrichtung (Recherche für Schulaufgaben), Interessen von Kindern (z. B. ausgewählte Spiele-Seiten) und kindgerechter Inhalte. Hier soll deshalb herausgearbeitet werden, dass Kindersuchmaschinen für jüngere Kinder (bis 12) einen Mehrwert haben.

Möglicher Einstieg:

- Wenn ihr etwas sucht, wo und wie sucht ihr?
- Welche Suchmaschinen kennt ihr/nutzt ihr?
- Sammlung (Strichliste) an der Tafel, evtl. prozentuale Berechnung, welcher Klassenanteil welche Suchmaschinen nutzt
- Möglicher Vergleich mit Nutzungsverteilung und Nutzungszahlen von Suchmaschinen in Deutschland (Grafik „Nutzung von Suchmaschinen", Kapitel „Vom Suchen und Finden")
- Wie funktioniert überhaupt eine Suchmaschine?
  Je nach Wissensstand der Schüler bietet sich als Einstieg ein Erklärvideo zu Suchmaschinen an: **http://vimeo.com/28807307**
  Oder AB „So funktionieren Suchmaschinen", erhöhter Schwierigkeitsgrad

Podcast „fragFINN zu Gast bei klicksafe"
http://www.klicksafe.de/suchmaschinen/

Podcast entweder der ganzen Klasse vorspielen (auch in Stücken, z. B. durch die Fragen strukturiert) oder die Schüler mit Kopfhörern am eigenen PC oder im Tandem hören lassen. Vorteil: Jeder kann sein eigenes Tempo bestimmen, mehrmals hören und bei Bedarf an entsprechende Stellen spulen. Im Podcast kommen zwei Begriffe vor, die nicht erklärt werden; mit den Schülern vorher klären: Whitelist = Datenbank oder Katalog mit positiv bewerteten Seiten; Alarmbutton = bei fragFINN können Inhalte, die Kinder anstößig finden, dem Team direkt über den Alarmbutton gemeldet werden. Mögliche Fragen (z. B. Tafelanschrieb) und Antworten:

Was ist eine Suchmaschine, was ist eine Kindersuchmaschine?	**Suchmaschine** = Programm, das das Internet nach Suchbegriffen durchsucht. **Kindersuchmaschine** = Ein Team von Redakteuren durchsucht das Internet und gibt per Hand die für Kinder geeigneten Seiten in eine Whitelist ein.
Warum gibt es Kindersuchmaschinen?	Das Internet ist zu großen Teilen ein Erwachsenennetz. Viele Seiten sind für Kinder nicht verständlich oder nicht geeignet. Kindersuchmaschinen stellen einen sicheren Surfraum zur Verfügung und bieten Inhalte an, die Kinder interessieren.
Warum kann man Seiten wie YouTube nicht bei fragFINN finden?	Auf Videoplattformen kann es Videos geben, die für Kinder nicht geeignet sind. Deshalb lassen fragFINN und die anderen Kindersuchmaschinenbetreiber solche Plattformen nicht zu.
Wann nimmt die Redaktion eine Seite aus der Datenbank der Suchmaschine heraus?	Wenn falsche Informationen oder nicht kindgeeignete Inhalte auf einer Webseite stehen.
Welche Suchtipps gibt Friederike Siller von fragFINN?	Sich genau überlegen, was man suchen will. Einfach formulieren. Auf Rechtschreibung achten. Nicht nur die ersten Treffer anschauen, auch die Treffer weiter hinten in der Trefferliste anschauen.

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Methodische Hinweise und Lösungen	Suchmaschinen und Suchvorgänge werden hier für Kinder zwischen 6 und 12 Jahren ausführlich erklärt: **http://www.internet-abc.de/kinder/suchen-finden-suchmaschinen.php?rev_eltern=1** **Aufgabe 1:** In Einzel- oder Partnerarbeit wird eine Kinder- mit einer Erwachsenensuchmaschine (Auswahl aus der Tabelle) anhand der vorgegebenen Rechercheaufgaben verglichen. Beurteilungskriterien mit der Klasse durchgehen und bei Bedarf ein zusätzliches Kriterium hinzufügen. **Lösungen Fragen 1 und 2:** „Wal Säugetier" und „Milch weiß" genügt für die Eingabe in die jeweilige Suchleiste. ■ Der Wal ist ein Säugetier (Begründung: Lungen- und nicht Kiemenatmung, gebären Junge im Vergleich zum Laichen), z. B. auf **www.wasistwas.de** ■ Die Milch bekommt die weiße Färbung durch Fett und Eiweiß. Je fetter die Milch, desto weißer ist sie z. B. auf der Seite **www.tagesspiegelkinder.de/wewetzer/fragen/m/art66,157** *Alternative Fragen, die Kinder auch gut beantworten können:* Wieso stehen Flamingos auf einem Bein? Was macht die Eule nachts? Wieso jaulen Wölfe? Warum sind die Blätter grün? Oder: Warum werden die Blätter im Herbst bunt? *Auswertung:* Bestimmen der Siegermaschine der ganzen Klasse und Herausarbeiten der Besonderheiten und Vorteile für die Schüler bei der Nutzung von Kindersuchmaschinen im Vergleich zu Erwachsenensuchmaschinen. **Aufgabe 2:** Wichtige Aspekte von Kindersuchmaschinen werden hier noch einmal zusammengefasst abgefragt: ■ Das Suchfeld ist leicht zu finden. ■ Die Schrift ist ausreichend groß. ■ Durch eine übersichtliche Gestaltung der Seite findest du dich schnell zurecht. ■ Die Texte sind leicht verständlich.
Methoden und Organisationsformen	Onlinerecherche, Vergleich, Podcast; Einzelarbeit, Partnerarbeit, Plenum
Zugang Internet / PC	Ja
Kapitel 2	Kindersuchmaschinen – Der sichere Einstieg ins Netz

Welche dieser Suchmaschinen hast du schon einmal benutzt?

www.fragfinn.de	www.google.de
www.helles-koepfchen.de	www.bing.com
www.blindekuh.de	www.yahoo.de
	www.ask.com

Arbeitsauftrag:

1. **Der Suchmaschinenvergleich:** Kindersuchmaschine <-> Erwachsenensuchmaschine. Für den Vergleich sollst du folgende Fragen in einer Kindersuchmaschine und einer Erwachsenensuchmaschine recherchieren. Wähle jeweils eine Suchmaschine aus.
   Tipp: Schreibe vorher die Suchbegriffe dazu auf, die du in die Suchmaschine eingeben willst.

Frage 1: **Ist der Wal ein Säugetier?**	Antwort:	
Suchbegriffe		
Suchmaschine	Kindersuchmaschine	Erwachsenensuchmaschine
Anzahl der Klicks bis zum Ergebnis		

Frage 2: **Wieso ist Milch weiß?**	Antwort:	
Suchbegriffe		
Suchmaschine	Kindersuchmaschine	Erwachsenensuchmaschine
Anzahl der Klicks bis zum Ergebnis		

Überlege dir eine Frage, die du deinem Sitznachbarn stellst und die er beantworten soll.
Danach beantworte seine Frage an dich!

Frage des Partners:	Antwort:	
Suchbegriffe		
Suchmaschine	Kindersuchmaschine	Erwachsenensuchmaschine
Anzahl der Klicks bis zum Ergebnis		

Welche Suchmaschine ist dein Sieger? Beurteile die Suchmaschinen, die du getestet hast.

Hier gefällt mir der Aufbau der Seite am besten:	
Hier habe ich die meisten nützlichen Informationen gefunden:	
Hier habe ich die Texte leicht verstehen können:	
Hier habe ich am schnellsten meine Antworten gefunden:	
Eigenes Kriterium:	
Mein Testsieger:	

2. Kindersuchmaschinen unterscheiden sich von Erwachsenensuchmaschinen in einigen Punkten.
Kreuze an, was auf eine Kindersuchmaschine zutrifft!

- ☐ Das Kästchen zum Eintragen der Suchbegriffe (Suchfeld) ist leicht zu finden.
- ☐ Die Schrift ist ausreichend groß.
- ☐ Auf der Suchergebnisliste erscheint auch Werbung.
- ☐ Sie zeigen tausende von Ergebnissen.
- ☐ Durch eine übersichtliche Gestaltung der Seite findest du dich schnell zurecht.
- ☐ Sie zeigen auch Seiten an, die nur für Erwachsene gedacht sind.
- ☐ Die Texte sind leicht verständlich.

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

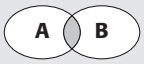
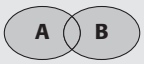
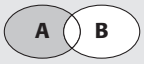
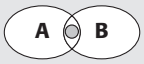
Arbeitsblatt	**AB 3**
Titel	**Suchtipps**
Ziele	Effektives und zielgerichtetes Suchen durch Erlernen von Suchtechniken
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1**

Methodische Hinweise und Lösungen

Die Suche mit Operatoren durch Eingabe in die Suchleiste ist bei der Nutzung der meistgenutzten Suchmaschinen wie Google, Bing oder Yahoo nicht zwingend erforderlich, da die Suchmaschinen immer „intelligenter" werden, d. h. Suchanfragen intuitiver verstehen. Für die Suche in Katalogen und das Wissen um die Funktionsweise von Suchmaschinen sind die klassischen Suchtechniken jedoch von Relevanz.

Aufgabe 1:
Zur Veranschaulichung der Beispiele mit der Operatorensuche können die Grafiken (Venn-Diagramme) von den Schülern entwickelt und in der Klasse z. B. durch Tafelanzeichnung verglichen werden.
Variation: Diagramme vorgeben und den jeweiligen Operatoren zuordnen lassen.

Tafelbild:

Modale Operatoren	Boolesche Operatoren	Auswahlfelder	Grafik
Leerzeichen	AND	mit allen Wörtern	
Klammern	OR	mit irgendeinem der Wörter	
Minuszeichen	NOT	ohne die Wörter	
Anführungszeichen	Anführungszeichen	mit der genauen Wortgruppe	

Quelle: http://www.ub.uni-bielefeld.de/biblio/search/help/

Mögliche Lehrererklärung für Situation 1:
Die Kreise stehen für die Treffermenge der Begriffe Jaguar (=A) und Tier (=B).
Die Schnittmenge ist der Trefferanteil, in dem beide Begriffe vorkommen, wenn sie durch den Operator AND verbunden werden, nämlich Informationen über das Tier Jaguar.
Bei Beispiel 3, der Minussuche, geht es in erster Linie darum, qualitativ zu suchen, indem man Wörter oder Wortgruppen ausschließt. Es kann sein, dass die Anzahl der Treffer nicht weniger wird (sogar eine erhöhte Trefferzahl ist möglich).

Aufgabe 2:
Die meisten Funktionen der Suchmaschine in der Erweiterten Suche sind identisch mit der klassischen Operatorensuche. Für die schnelle Suche können die Schüler die Operatoren durch Direkteingabe ins Suchfeld nutzen.
Schauen Sie sich mit den Schülern die Erweiterte Suche in den Suchmaschinen Google und der Metasuchmaschine Ixquick an. Welche der Suchoperatoren erkennen die Schüler wieder?
Erweiterte Suche bei Google (am linken unteren Rand der Webseite):
Suche mit AND, „ " , OR, NOT (Minussuche)
Erweiterte Suche bei Ixquick:
mit allen Wörtern (AND), mit dem exakten Ausdruck („"), mit mindestens einem der Wörter (OR), ohne die Wörter (NOT)

Methodische Hinweise und Lösungen	**Lösung Aufgabe 2:** Weitere nützliche Suchfunktionen: *Google:* Suche nach Sprache (Übung beim Fremdsprachenerwerb), Suche nach letzter Aktualisierung der Seite (Aktualität der Seite), Suche nach Dateityp (.ppt, .pdf, .doc), Suche nach Nutzungsrechten (Bildrechte etc.) *Ixquick:* Suche in bestimmter Domain (z. B. edu, gov) oder Suche mit Hyperlinks (mit Links zu diesem Dateinamen) **Zusatzaufgabe/Hausaufgabe:** Für die Schüler ist „PowerPoint-Karaoke" eine sehr gute Möglichkeit, spontanes und kreatives Präsentieren zu üben. Sie lernen außerdem auf spielerische Weise die Suche nach bestimmten Dateiformaten. **Zusatzaufgabe/Hausaufgabe:** Kennst du PowerPoint-Karaoke? Dazu lädst du eine dir völlig unbekannte PowerPoint-Präsentation mit einem unbekannten Thema herunter und präsentierst sie deinen Freunden oder deiner Klasse. Du darfst sie nur kurz anschauen (Verschärfte Regel: Vortragen, ohne vorher die PPT gesehen zu haben)! Woher bekommst du die Präsentationen? Nutze die Suchfunktion von Google, indem du bei der Suche nach dem Dateiformat das Format „Windows PowerPoint (.ppt)" wählst! *Quellen:* Als Lerncheck und für das Erlernen weiterer Suchhilfen können folgende Tutorials eingesetzt werden: **http://www.suche-im-internet.de/suche_video.html** Suchhilfen bei Google, Yahoo, Bing und Ixquick in der Erweiterten Suche.
Methoden und Organisationsformen	Tafelbild Venn-Diagramme, Onlinerecherche, PowerPoint-Karaoke; Plenum, Einzelarbeit, Partnerarbeit
Zugang Internet / PC	ja
Kapitel 1 und 2	Tipps & Tricks beim Suchen, Glaubwürdigkeits-Check

Eva schreibt für Biologie an einer Facharbeit zum Thema „Jaguar“. Als sie bei der Recherche den Suchbegriff „Jaguar“ in eine Suchmaschine eingibt, erhält sie 325 000 000 Treffer.

Oft bekommt man zu viele Treffer angezeigt, dann muss man aussortieren und auswählen. Daher sollte Eva einige Tricks für ihre Suchanfrage kennen. Denn eine gezielte Suche spart Zeit und bringt genauere Ergebnisse.



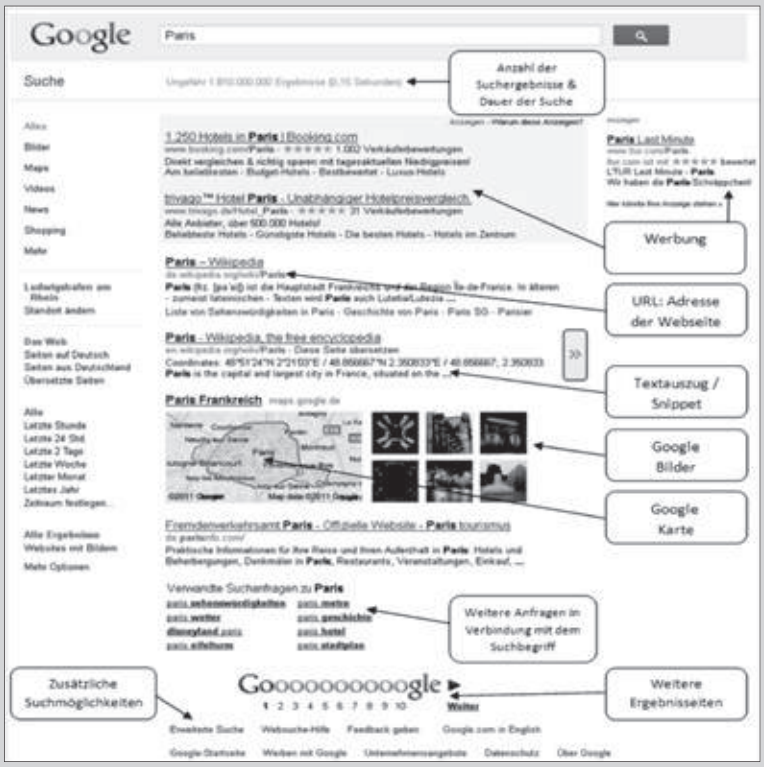
Wenn du in einem Textdokument oder auf einer Internetseite nach bestimmten Wörtern suchen willst, dann nutze dazu die Tastenkombination Strg + F und gib deinen Suchbegriff in die Suchleiste am unteren Bildschirmrand ein.

Arbeitsauftrag:

1. Lest in der Klasse die Beispiele durch.

Situation	Problem	Suchhilfe, auch Operator genannt
1. Eva tippt *[Jaguar]* in den Eingabezeile ein. Anzahl der Treffer: _____	Es werden auf den ersten Seiten hauptsächlich Treffer für das Luxusauto Jaguar angezeigt.	**Die Suche mit dem Operator AND** In die Suchmaske *[Jaguar]* AND *[Tier]* eingeben, denn dann wird die Suche Jaguar (A) mit Tier (B) verknüpft. Das AND kann weggelassen werden, wenn Leerzeichen zwischen den Begriffen sind, weil die Suchmaschine das automatisch verknüpft.
2. Ein Beutetier des Jaguars ist das Nabelschwein. Eva möchte ein Bild davon in ihre Facharbeit nehmen. Anzahl der Treffer: _____	Eva hätte gerne mehr Bilder zur Auswahl.	**Die Suche mit dem Operator OR** Das Nabelschwein wird auch Pekari genannt. Wenn Eva *[Nabelschwein]* OR *[Pekari]* bei der Suche eingegeben hätte, hätte sie mehr Treffer angezeigt bekommen, nämlich alle, in denen entweder Pekari (A), Nabelschwein (B) oder beide Begriffe vorkommen. *Tipp:* Man kann die Trefferquote erhöhen, wenn man Wörter, die das Gleiche bedeuten, mit OR verknüpft.
3. Jaguare leben im Dschungel. Eva möchte auch hierzu Infos aus dem Internet.	Bei Eingabe des Begriffs „Dschungel“ tauchen vor allem Infos zu der Fernsehsendung „Dschungelcamp“ auf.	**Die Suche mit dem Operator – *(gesprochen: Minus)*** Eva sollte nach *[Dschungel – Dschungelcamp] (gesprochen Dschungel minus Dschungelcamp)* suchen. Durch das Minus vor dem Begriff werden Seiten angezeigt, auf denen zwar der Begriff *Dschungel* vorkommt, aber eben nicht *Dschungelcamp*. *Tipp:* Das Minus muss ohne Leerzeichen vor dem Wort stehen, das man ausschließen möchte.
4. Lehrerin Frau Müller-Schmidt ist skeptisch, weil in Evas Facharbeit Fremdwörter vorkommen, die sie selbst noch nicht einmal kennt. Sie hat die Vermutung, dass Eva Texte aus dem Internet genommen hat, kann jedoch in den Quellenangaben nichts dazu finden. Sie gibt folgenden Satz in ihre Lieblingssuchmaschine, die Metasuchmaschine **www.ixquick.com** ein: *Hier entwickelten sie sich vermutlich über den pleistozänen Amerikanischen Jaguar (Panthera onca augusta) zur heute lebenden Form.*	Frau Müller-Schmidt bekommt in der Suchmaschine Ixquick keine Ergebnisse, die ihre Vermutung untermauern.	**Die Phrasensuche in „“** Frau Müller-Schmidt muss den Text oder einen besonders auffälligen Teil davon in Anführungszeichen setzen: „pleistozänen Amerikanischen Jaguar“. *Denn:* Hierbei kann nach ganzen Sätzen bzw. Wortfolgen gesucht werden. Wenn eine Webseite genau diese Wortfolgen enthält, wird sie unter den Ergebnissen gelistet. *Übrigens:* Der Text stammt aus Wikipedia und die Quelle hätte angegeben werden müssen.

2. Welche weiteren Suchfunktionen gibt es in den Suchmaschinen **www.google.de** *und* **www.ixquick.de***? Nenne zwei und finde Beispiele, wofür du sie nutzen würdest.*

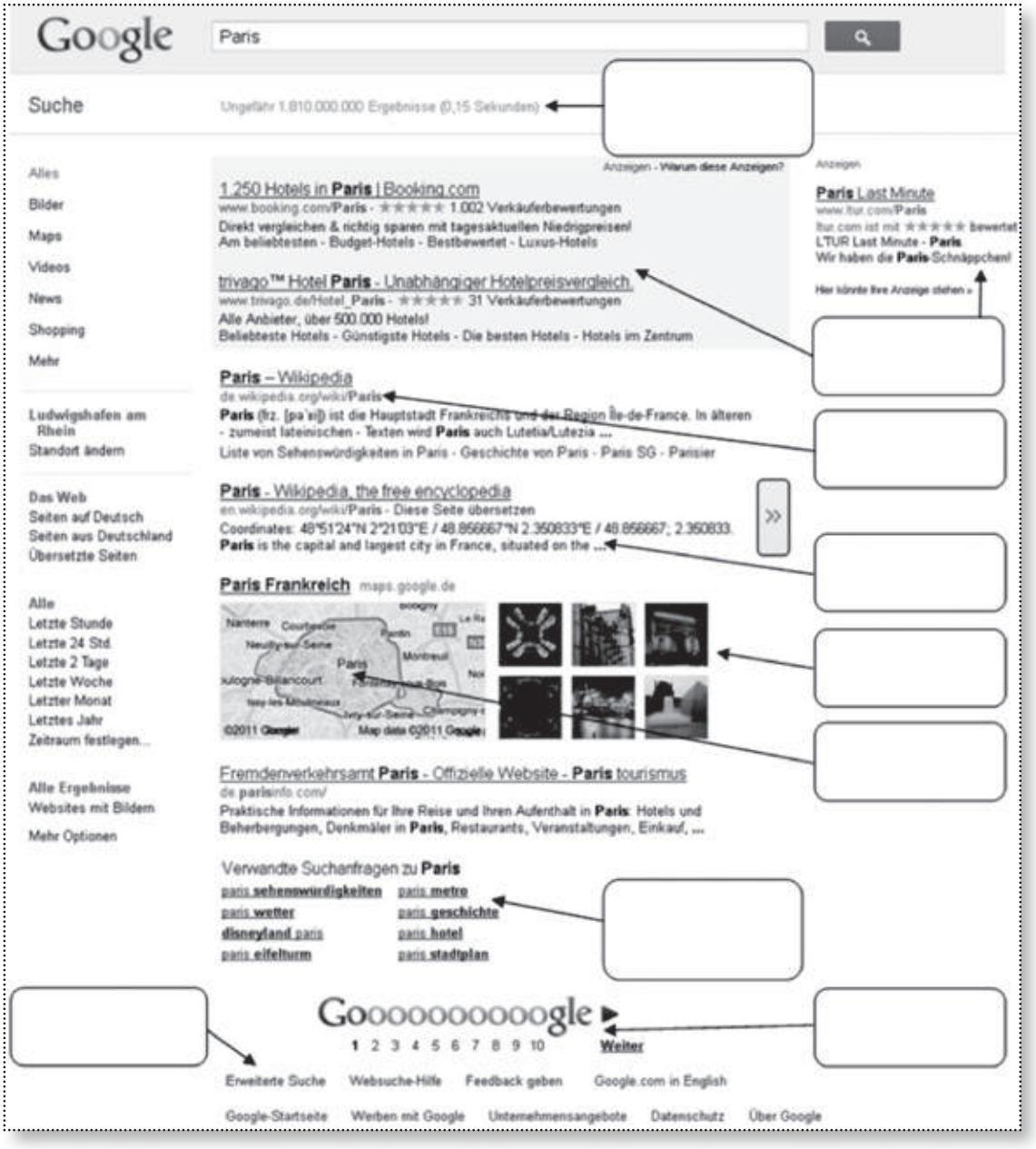
Arbeitsblatt	**AB 4**
Titel	**Suchergebnisse beurteilen: Orientierung auf der Ergebnisseite**
Ziele	Erlangen eines ersten Überblicks auf der Suchseite
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1** Kombinierbar mit AB 5 u. 6
Methodische Hinweise und Lösungen	In den aufeinander aufbauenden ABs 4, 5, 6 zum Thema „Suchergebnisse beurteilen" werden drei Grundsätze zur Beurteilung von Ergebnissen aufgegriffen: 1: Augen auf! Orientierung auf der Ergebnisseite. Vorschau genau ansehen! 2: Gehirn an! Wahrheitsgehalt von Informationen einordnen. Bekannte Quellen nutzen! 3: Suchergebnisse beurteilen! Beurteilung des Urhebers einer Quelle anhand eines Checkbogens. **Aufgabe 1:** Zeigen Sie die Trefferseite zur Suchanfrage „Paris" auf ⓘ **www.google.de**, falls Internetzugang vorhanden (PDF des Screenshots auch auf ⓘ **http://www.klicksafe.de/suchmaschinen/**). Aufbau der Seite bzw. für die Suche relevante Bereiche sowie einzelne Funktionen besprechen. Hier können Sie sich selbst informieren: Tipp: ⓘ **http://www.suche-im-internet.de/treffervideo.html** Schüler füllen selbstständig die Kästchen aus. **Variation:** Lösungen vorgeben und von den Schülern zuordnen lassen.  Quelle Screenshot Google-Suche: http://tinyurl.com/6zm7mmu, 28.7.2011; 13.22 Uhr **Lösung Aufgabe 2:** Durch Klicken auf das Pfeilsymbol neben dem Titel des Suchergebnisses öffnet sich eine Miniaturansicht der Webseite (erster Eindruck von einer Webseite möglich, ohne auf die Seite direkt zu gehen). Bei ⓘ **www.bing.de** gibt es auch eine entsprechende Voransichtsfunktion (Pfeil rechts neben dem Ergebnis); keine Miniaturansicht, aber Textauszug und Anzeige von Referenzseiten/verlinkten Seiten.
Methoden und Organisationsformen	Screenshot einer Suchseite, Zuordnen von Begriffen; Lehrerdemonstration, Einzelarbeit
Zugang Internet / PC	nein (nur für Aufg. 2 notwendig)
Kapitel 1	Aufbau der Seite mit den Suchergebnissen

Wusstest du schon: Die überwiegende Anzahl der Nutzer von Suchmaschinen klicken auf die ersten fünf Treffer. Nach der KIM-Studie 2010 arbeiten Mädchen häufiger die Ergebnisse durch. Je älter die Nutzer, desto eher schauen sie sich auch weitere Treffer an.

ORIENTIERUNG IST WICHTIG!

Arbeitsauftrag:

1. Hier siehst du einen Screenshot (= Bildschirmfoto) der Suchmaschine Google mit der Suchanfrage **[Paris]**. Nimm dir Zeit und verschaffe dir zuerst einmal einen Überblick.
   Wozu sind die Funktionen da, auf die die Pfeile zeigen? Fülle die Kästchen aus.



2. Vielleicht hast du dich schon über das Pfeilsymbol » gewundert, das auf dem Screenshot auftaucht.
   Finde selbst im Internet heraus, wozu es da ist.
   Gibt es in anderen Suchmaschinen, wie z. B. **www.bing.de,** auch solche Funktionen?

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

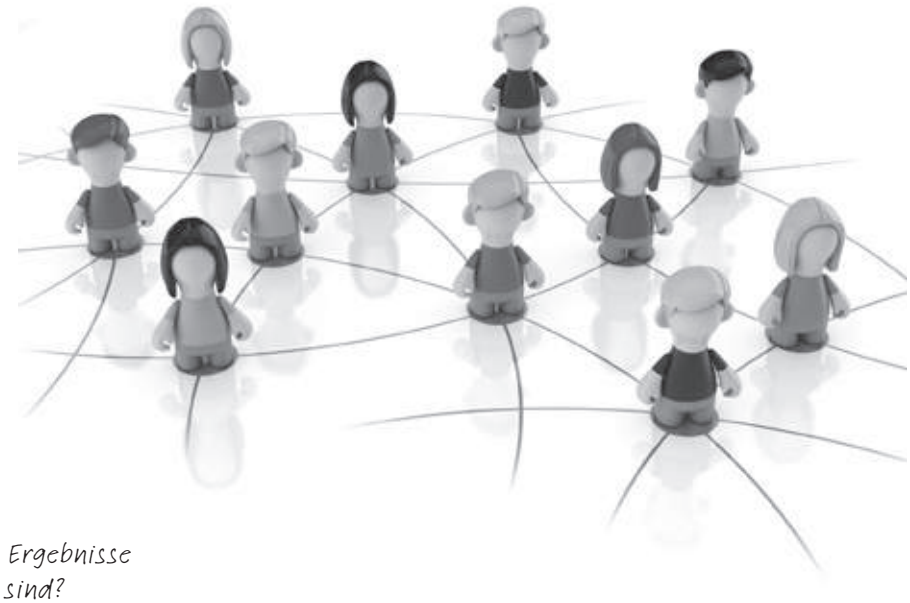
Arbeitsblatt	**AB 5**
Titel	**Suchergebnisse beurteilen: Quellen einschätzen**
Ziele	Schnelle Einordnung und Beurteilung von Ergebnissen in Bezug auf Urheber und Glaubwürdigkeit einer Quelle
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1** Kombinierbar mit AB 4 u. 6
Methodische Hinweise und Lösungen	Es passiert nicht selten, dass Jugendliche ahnungslos falsche Informationen aus dem Internet verwerten, z. B. für Referate. Informationsquellen einzuschätzen, ist ein wichtiger Teil von Informationskompetenz. Es sollte daher versucht werden, die Quelle anhand einfacher Beurteilungskriterien selbst zu bewerten. **Möglicher Einstieg:** Fragen Sie negative (Such-)Erlebnisse in der Klasse, ab z. B. ob die Schüler schon einmal auf Seiten „hereingefallen" sind (z. B. seriöses Aussehen und gutes Design, jedoch unseriöser oder falscher Inhalt). **Lösung Aufgabe 1:** g | | | g | g | g | g g | | | g **Lösung Aufgabe 2:** Beispielgrafik als PDF auf ⓘ **http://www.klicksafe.de/suchmaschinen/**
Methoden und Organisationsformen	Screenshot einer Ergebnisseite, Zuordnen und Bewerten von Quellen; Einzelarbeit, Plenum
Zugang Internet / PC	nein
Kapitel 2	Quellenkritik und Bewertungskompetenz



Die Suchergebnisse sind so nicht aufgelistet. Die Treffer sind zur Anschauung montiert worden.

Hinweis: Homepage einer politischen Gruppierung
Die Webseite „American Nazi Group" existiert so nicht, ist jedoch an den Auftritt einer US-amerikanischen rechten Gruppierung angelehnt. Hier besteht leider keine Möglichkeit, gegen die verantwortliche/n Person/en vorzugehen und rechtliche Schritte einzuleiten, da der Provider der Seite in den USA sitzt und im Ausland die Verbreitung rechtsextremer Inhalte meist zulässig ist.

Es gibt eine Menge Informationen im **WWW**, denn sehr viele Menschen – schätzungsweise vier Milliarden Menschen weltweit – nutzen das Netz. Jeder kann Dinge veröffentlichen, und so gibt es neben richtigen Informationen auch falsche.



Arbeitsaufträge:

1. Wie kannst du nachprüfen, ob die Ergebnisse deiner Internetsuche glaubwürdig sind? Markiere in der Tabelle grün, was dir sinnvoll erscheint. Vergleicht in der Klasse!

Die Information zusätzlich in einem Buch nachschlagen.	Einen Nachbarn fragen, der sonst auch alles weiß.	Nie kontrollieren – das stimmt schon, was im Internet steht.	Wenn möglich, einen Experten zum Thema befragen.
Drei Tage warten und dann erneut suchen.	Die gleiche Information auf zwei unterschiedlichen Seiten suchen.	Nachschauen, wer die Seite ins Netz gestellt hat.	Den gesunden Menschenverstand einschalten.
Verschiedene Medien wie Buch, Internet, Zeitschrift usw. benutzen.	Bei der Internet-Auskunftstelle in New York nachfragen.	Den Bildschirm kurz aus- und sofort wieder einschalten.	Nachschauen, wie alt die Informationen sind.

Ob eine Information glaubwürdig ist oder nicht, kann man manchmal schon daran erkennen, wer sie bereitstellt. Bei Webseiten von großen Tageszeitungen, bekannten Organisationen, vielgelesenen Bloggern usw. kann man davon ausgehen, dass die Informationen einen höheren Wahrheitsgehalt haben.

2. Das Bild zeigt die Ergebnisse einer Suche nach dem Suchwort „Nazi".
Ordne bitte die Informationsquellen der richtigen Stelle auf dem Bild zu.

Online-Enzyklopädie (=Lexikon)

Privater Blog (= Onlinetagebuch), z. B. http://wordpress.com, www.blogger.com

Onlineauftritt einer bekannten Zeitung

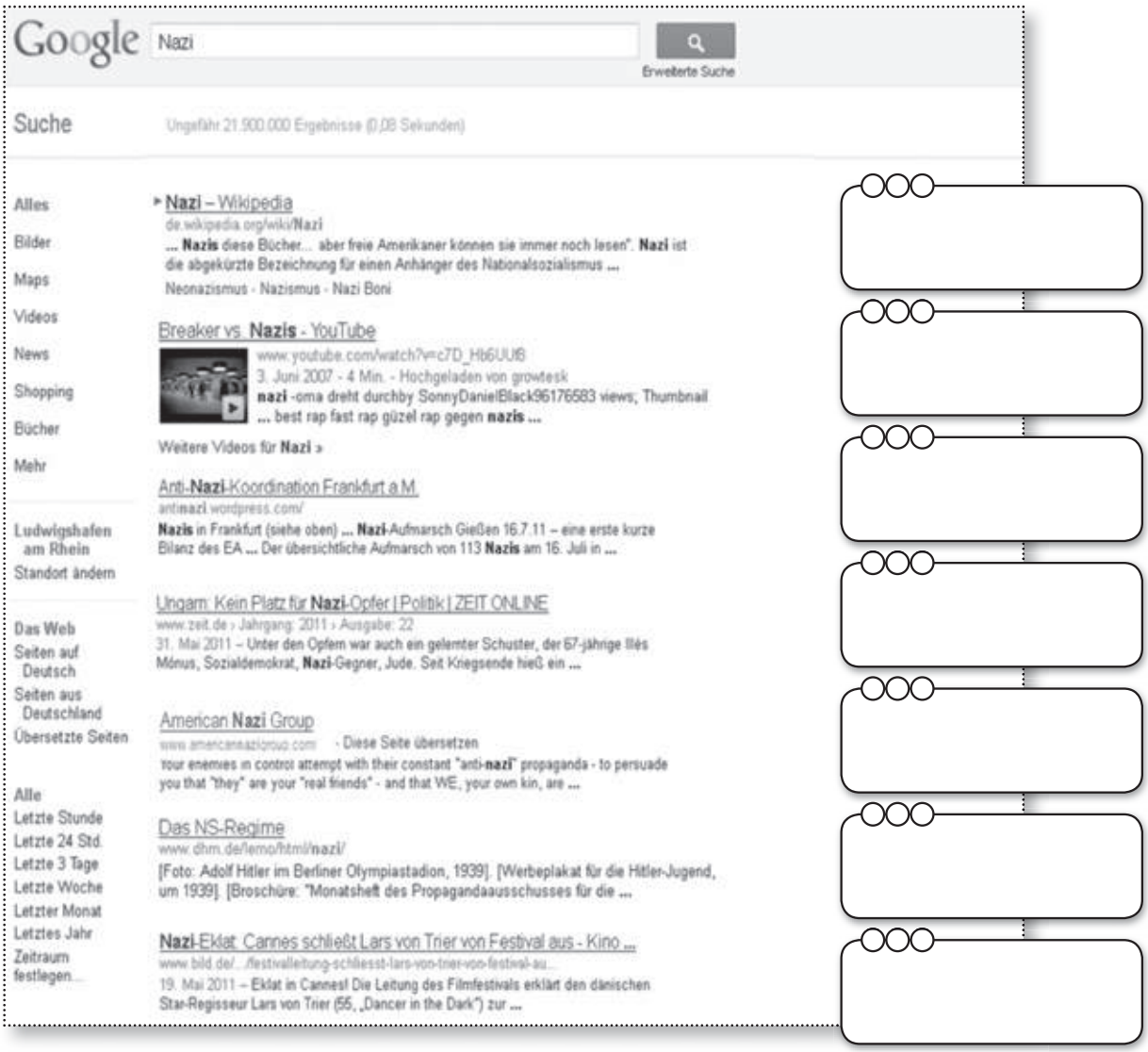
Homepage einer politischen Gruppierung

Onlineauftritt einer bekannten Zeitung

YouTube-Video

Homepage eines Museums

3. Bewerte die Glaubwürdigkeit der einzelnen Onlinequellen, indem du die Kreise über den Kästchen ausmalst (von **nicht glaubwürdig = nicht ausgemalt** bis **glaubwürdig = 3 Kreise ausgemalt**)
Vergleicht nun in der Klasse eure Ergebnisse!



5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 6**
Titel	**Suchergebnisse beurteilen: Der Checkbogen**
Ziele	Tiefergehende Beschäftigung mit einer Internetquelle durch Beurteilung des Urhebers anhand eines Checkbogens
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1** Kombinierbar mit AB 4 u. 5
Methodische Hinweise und Lösungen	**Möglicher Einstieg:** *Stummer Impuls: „Wer, wie, warum? " an Tafel/Whiteboard schreiben. Mögliche Lehreranweisung: „Wenn wir uns für einen Suchtreffer entschieden haben, dann geht es an die Überprüfung der Glaubwürdigkeit der entsprechenden Seite. Der Hintergrund jeder einzelnen Information, sei es ein Bild oder eine einzelne Aussage, sollte immer genau unter die Lupe genommen werden. Und hierfür gibt es einige Dinge, auf die wir achten müssen."* Gehen Sie den Checkbogen im Unterricht zusammen mit Ihren Schülern einmal durch und klären Sie mögliche Fragen im Klassengespräch. Der Checkbogen ist auf Grundlage eines ausführlicheren Bogens von Peter Kühnt entstanden. **Hinweise für den Testbogen im Bereich „WER":** Ermittlung des Inhabers einer Domain bei ⓘ **www.denic.de** (allerdings nur Auskunft über registrierte deutsche Betreiber) **Hinweise für den Testbogen im Bereich „WIE":** Gibt es viele Verlinkungen auf eine Seite, dann spricht das für die Bekanntheit und den Stellenwert einer Seite bei den Nutzern. Dies kann, muss aber nicht ein Indikator für die Qualität einer Seite sein. Meist sind solche Seiten auch auf den ersten zehn Ergebnisseiten einer Websuche zu finden. Machen Sie mit den Schülern den Test, z. B. mit ⓘ **www.klicksafe.de**. Die Google-Abfrage *[link:klicksafe]* (in die Suchleiste eingeben) zeigt beispielsweise die Webseiten an, auf denen ein Link auf ⓘ **www.klicksafe.de** vorkommt. Sie können die gleiche Übung beispielsweise auch mit der Suche nach Verlinkungen auf Ihre Schulhomepage durchführen. **Hinweise für den Testbogen im Bereich „WARUM":** Wenn möglich, AB 5 vorschalten, da es sich mit der Beurteilung einer Quelle aufgrund des Urhebers befasst. Die Schüler sollen nun in Gruppen eine selbst gewählte Webseite mit Hilfe des Checkbogens analysieren. Eindeutigere Ergebnisse erhalten Sie jedoch, wenn Sie die Webseite vorgeben. Danach kurze Vorstellung der Testseite, Begründung der Auswahl und Auswertung anhand des Checkbogens im Plenum. *Alternative:* Geben Sie Webseiten unterschiedlicher Qualität zum Thema Römertum vor. *Negatives Beispiel:* ⓘ **http://www.wib.be.schule.de/kubim/roemer/index.htm** (Fake-Webseite einer Schule mit falschen historischen Fakten zur Römerzeit)
Methoden und Organisationsformen	Checkbogen, Webseitencheck; Plenum, Gruppenarbeit
Zugang Internet / PC	ja
Kapitel 2	Quellenkritik und Bewertungskompetenz

Wer, wie, warum? – Der Checkbogen

Webseite unter der Lupe  ..... (URL der Webseite)

WER hat die Seite verfasst?	
Ist der Verfasser mit Vor- und Zunamen angegeben (im Impressum)?	**ja** ☐ **nein** ☐
Ist der Verfasser oder seine Organisation dem Namen nach bekannt (Recherche in Suchmaschinen, beim Autor z. B. auch in Amazon.de, Thalia.de)?	**ja** ☐ **nein** ☐
WIE gepflegt und aktuell ist die Seite?	
Gibt es ein Impressum?	**ja** ☐ **nein** ☐
Ist die Seite größtenteils frei von Rechtschreibfehlern?	**ja** ☐ **nein** ☐
Sind die Bilder von guter Qualität? Wird sie richtig angezeigt?	**ja** ☐ **nein** ☐
Gibt es keine oder nur wenige Pop-ups und andere Werbung?	**ja** ☐ **nein** ☐
Ist sie klar und übersichtlich strukturiert?	**ja** ☐ **nein** ☐
Befindet sich ein aktuelles Datum auf der Seite?	**ja** ☐ **nein** ☐
Funktionieren die Links?	**ja** ☐ **nein** ☐
Ist die Webseite bei Eingabe eines für die Seite relevanten Suchbegriffes im Ranking der Suchmaschine auf einer der ersten zehn Seiten gelistet?	**ja** ☐ **nein** ☐
WARUM wurde die Seite erstellt?	
Sind die Texte sachlich/informativ geschrieben?	**ja** ☐ **nein** ☐
Stimmen die Inhalte auf der Webseite (andere Quellen als Vergleichsquellen nutzen)?	**ja** ☐ **nein** ☐

Art der Webseite (bitte ankreuzen):

☐ Seite einer einzelnen Person (private/r Blog/Homepage)
☐ Onlineausgabe einer Zeitung
☐ Nachrichtenseite
☐ Werbeseite
☐ bekannte Organisation (Ministerium, Verbraucherzentrale …)
☐ sonstiges: .....

Weshalb wurde diese Seite ins Internet gestellt?
Was möchte der Verfasser mit dieser Seite erreichen?

.....

.....

Wie oft konntet ihr mit „ja" antworten? Zählt zusammen und ordnet die Seite ein:

1–3 × ja ☐	4–6 × ja ☐	7–9 × ja ☐	10–12 × ja ☐

Tipp: Wenn du weniger als 6x ja angekreuzt hast, dann ist die Webseite vielleicht nicht so gut geeignet und du solltest dir noch mindestens eine andere Webseite zum gleichen Thema anschauen!

Kannst du dieser Seite vertrauen oder kommt dir etwas komisch vor?
Deine eigene Einschätzung:

.....

.....

.....

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 7**
Titel	**Methodentraining: Die 4-Schritte-Methode – Suchergebnisse richtig verwenden und ordentlich verwalten**
Ziele	Kennenlernen einer Methode zur Quellenkritik und zur Abspeicherung von Recherchematerial
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**2** Kombinierbar mit AB 5 u. 6
Methodische Hinweise und Lösungen	Diese Methode ist geeignet als Methodentraining und kann in **allen** Fächern, z. B. für die Referatsrecherche, eingesetzt werden. Sie können aber auch ein Musterthema, z. B. über die „Politischen Parteien in Deutschland", vorgeben. **4-Schritte-Methode:** Schritt 1: Internetrecherche Schritt 2: Wer, wie, warum? – Der Checkbogen (Vorlage von AB 6) Schritt 3: Ordner zur Ablage von gefundenen Dateien, Videos oder Bildern Schritt 4: Quellenangaben und evtl. Rechte-Check (Vorlage AB 7) Schüler sollten Methoden zum *Quellenvergleich wie die Nutzung versch. Suchmaschinen/ Quellen* und *Quellenkritik* = Checkbogen kennengelernt haben. Hinzu kommen nun zwei weitere Aspekte, die bei der Abspeicherung von Suchergebnissen eine Rolle spielen: *Ordnerablage:* Übersichtliches Abspeichern von Informationen mit Hilfe von Ordnern. Den Hinweis geben, dass Ordner so gespeichert werden sollen, dass die Schüler sie leicht wiederfinden (z. B. unter Eigene Dateien). Mit älteren Schülern nutzen: Browser-Funktion „Lesezeichen" sowie Social Bookmarking Programme wie xmarks (zum Austausch mit Klassenkameraden und der Synchronisation der eigenen Lesezeichen in verschiedenen Browsern) *Quellenverwaltung und Rechte-Check:* Falls die Referate / Arbeiten z. B. im Internet **veröffentlicht** werden, müssen die Quellen auf die Möglichkeit zur Weiterverwendung überprüft werden: Stehen die Bilder und Videos unter einer Creative-Commons-Lizenz? Bei wem muss man nachfragen, wenn man urheberrechtlich geschützte Inhalte verwenden möchte (siehe auch Zusatzmodul „Nicht alles was geht, ist auch erlaubt", AB 5)?; Richtig zitieren: **http://scidok.sulb.uni-saarland.de/doku/zitieren.php** **Freie Lizenzen:** Man kann Bilder und Videos veröffentlichen, wenn der Urheber sie zur Verwendung durch Fremde freigegeben hat (Creative-Commons-Lizenz): **www.irights.info** (unter Creative Commons + Lizenzen) *Lizenzfreie Bilder:* **www.flickr.de**: Entdecken > Suchbegriff eingeben > Erweiterte Suche > Alle Creative-Commons wählen **www.google.de**: Bilder > Erweiterte Bildersuche > frei zu nutzen oder weiterzugeben *Lizenzfreie Videos:* YouTube-Videos mit CC-Lizenz **http://www.youtube.com/t/creative_commons** Quellen der Screenshots: http://de.yahoo.com/, https://www.ixquick.com/deu/, http://metager2.de/, http://www.bing.com/?cc=de, http://www.google.de/ Stand: 28.11.2012
Methoden und Organisationsformen	4-Schritte-Methode; Gruppen oder Einzelarbeit
Zugang Internet / PC	ja
Kapitel 2	Glaubwürdigkeits-Check

Die 4-Schritte-Methode: Gehe bei deiner Internetrecherche folgendermaßen vor:

1



Vertraue nie nur auf eine Quelle!

Vergleiche deine Ergebnisse in verschiedenen Suchmaschinen, z. B.:
- www.bing.de
- www.yahoo.de
- www.google.de
- www.metager.de
- www.ixquick.de

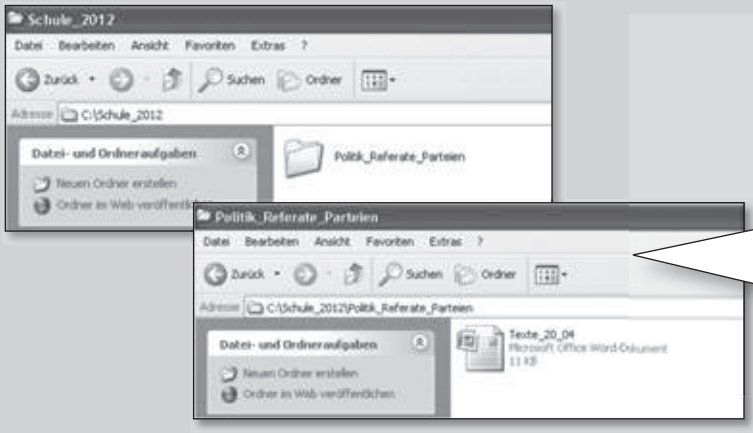
2

Nutze den Checkbogen!

Er hilft dir, gute von schlechten, richtige von falschen und alte von neuen Informationen zu unterscheiden.
Dazu musst du versuchen, etwas über den Verfasser der Seite oder des Textes zu erfahren.
Außerdem schaust du dir die Seite genau an und bewertest sie.



3

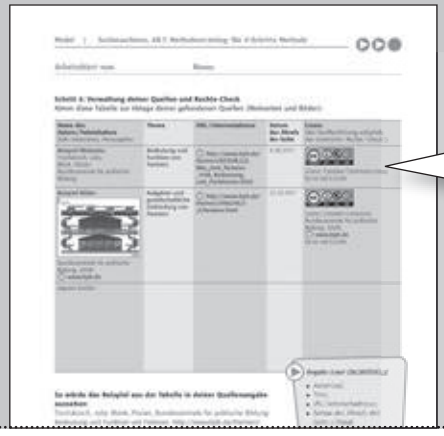


Ordnung ist wichtig!

Erstelle Ordner zur Ablage von gefundenen Dateien, Videos oder Bildern und benenne sie passend, z. B.:
Politik_Referate_Parteien

Zitate oder Textausschnitte kannst du in einem Textdokument speichern, z. B.:
Texte_20_04_2012
(das bedeutet, die Recherche hast du am 20.4.2012 gemacht)

4



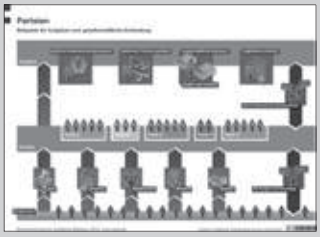
Mache richtige Quellenangaben und überprüfe Verwendungsrechte!

Das Blatt hilft dir, korrekte Quellenangaben zu machen.

Bei Verwendung von fremden Bildern, Videos oder Texten musst du außerdem auf Lizenzen achten und Rechte einholen, wenn du deine Arbeit veröffentlichen willst.

creative commons

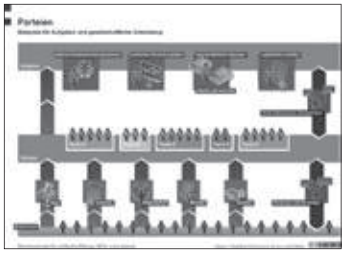
Schritt 4: Verwaltung deiner Quellen und Rechte-Check
Erstelle eine solche Tabelle zur Ablage deiner gefundenen Quellen (Webseiten und Bilder):

Name des Autors / Fotoinhabers (falls erkennbar), **Herausgeber**	**Thema**	**URL / Internetadresse**	**Datum des Abrufs der Seite**	**Lizenz** (Bei Veröffentlichung außerhalb des Unterrichts: Rechte-Check!)
Beispiel Webseite: Oskar Niedermayer Bundeszentrale für politische Bildung	Die Rolle und Funktionen von Parteien in der deutschen Demokratie	http://www.bpb.de/themen/AZJS0R,0,0,Was_sind_Parteien_%96_Bedeutung_und_Funktionen.html	27.04.2016	Lizenz: Creative-Commons-Lizenz by-nc-nd/3.0/de/
Beispiel Bilder:  Bundeszentrale für politische Bildung	Parteien: Beispiele für Aufgaben und gesellschaftliche Einbindung	http://www.bpb.de/politik/grundfragen/24-deutschland/40481/parteien	22.03.2016	Lizenz: cc by-nc-nd/3.0/de/ Bundeszentrale für politische Bildung, 2013, www.bpb.de
eigene Suche:				

Angabe einer Onlinequelle:
- *Autor/en*
- *Titel*
- *URL / Internetadresse*
- *Datum des Abrufs der Seite*
- *Lizenz (nur bei Veröffentlichung von Bildern)*

So würde das Beispiel aus der Tabelle in deiner Quellenangabe aussehen:
Oskar Niedermayer für bpb.de: Die Rolle und Funktionen von Parteien in der deutschen Demokratie. http://www.bpb.de/themen/AZJS0R,0,0,Was_sind_Parteien_%96_Bedeutung_und_Funktionen.html Abruf: 27.04.2016

So würde dein Bild mit Quellenangabe in deiner PowerPoint-Präsentation für das Referat aussehen:



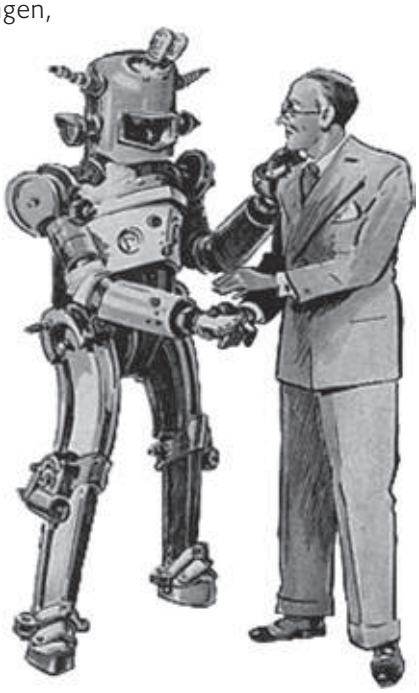
Bundeszentrale für politische Bildung, **Parteien: Beispiele für Aufgaben und gesellschaftliche Einbindung,** http://www.bpb.de/politik/grundfragen/24-deutschland/40481/parteien, Abruf: 22.03.2016
(Lizenz: cc by-nc-nd/3.0/de/ bei Veröffentlichung mit angeben!)

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 8**
Titel	**So funktionieren Suchmaschinen**
Ziele	Verstehen der Funktionsweise von Suchmaschinen durch exemplarisches Betrachten der Suchmaschine Google
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**1 / mit Funktionszeichnung: 2**
Methodische Hinweise und Lösungen	Aufgaben 1 und 2: Die Schüler lesen den Text für sich alleine und beantworten die Fragen. **Tipp:** Zur Vereinfachung lassen Sie wichtige Begriffe, wie z. B. PageRank-Algorithmus, markieren oder die 6 Schritte in kurzen Absätzen von einzelnen Schülern / Gruppen zusammenfassen. Lösung Aufgabe 2: 1. Nein, die Crawler durchsuchen das Netz ständig. Sie legen ihre Ergebnisse auf den Servern ab. Diese werden dann bei einer Suchanfrage abgefragt. 2. Es werden Server angefragt, die räumlich nahe, schneller und weniger ausgelastet sind. Dann geht die Suche schneller. 3. Mit dem PageRank genannten mathematischen Verfahren (Algorithmus) werden miteinander verlinkte Dokumente bewertet und gewichtet. Es wertet mehr als 200 Parameter aus und bestimmt letztlich die Reihenfolge, nach der die Suchergebnisse bei Google aufgelistet werden. 4. Ergebnisse häufiger Suchanfragen werden zwischengespeichert, d. h. nicht jedes Mal aufs Neue im Index gesucht. 5. Ein Snippet ist meistens ein Teil des Textes aus der gefundenen Internetseite, in dem der Suchbegriff enthalten ist. Der Snippet wird unter dem Titel und der URL der gefundenen Internetseite angezeigt. Variation Funktionszeichnung: Die Schüler haben – je nach Leistungsstand - verschiedene Möglichkeiten der Umsetzung des Textes in eine Funktionszeichnung. Danach Vergleich miteinander und mit der Beispielgrafik; siehe Kapitel „Wie funktioniert eine Suchmaschine“ (mit Lösungen und unausgefüllt zum Download auf ⓘ **http://www.klicksafe.de/suchmaschinen**): A. Anfertigen eigener Funktionszeichnungen auf Grundlage des Informationstextes. B. Ausfüllen der unausgefüllten Beispielgrafik. C. Beispielgrafik wird an die Schüler ausgegeben. Die Lösungstexte in den Kästchen werden vorgegeben (Anschrieb oder auf Kärtchen) und die Schüler müssen die Texte der richtigen Stelle auf der Grafik zuordnen. **Aufgabe 3:** Ein Klassen-Ranking kann erstellt und mit den Parametern der Suchmaschine verglichen werden. Lösung z. B. Anzahl der Verlinkungen, Wertigkeit benachbarter bzw. verlinkter Websites, außerdem Faktoren wie Schriftarten, Unterteilungen, genaue Position der Begriffe auf der Webseite. **Zusatzaufgabe/Hausaufgabe:** Siehe Infokasten „Suchmaschinenoptimierung“ im Kapitel „Jugendschutz und Suchmaschinen“ – 1. Das Ranking beeinflusst das Geschäft, 2. Problem: Spamming zusammenfassen.
Methoden und Organisationsformen	Textarbeit, Funktionszeichnung; Einzelarbeit, Gruppenarbeit, Plenum
Zugang Internet / PC	ja
Kapitel 1	Wie funktioniert eine Suchmaschine?, Fünf Schritte bis zum Ergebnis, Wie kommt ein Ranking zustande?

Von einer Suche zu einem Ergebnis dauert es meist nur einige Bruchteile einer Sekunde. So schnell könnte ein Mensch niemals in einem Buch nachschlagen, aber Menschen sind ja glücklicherweise auch keine Maschinen.

Weißt du, wie eine Suchmaschine funktioniert?



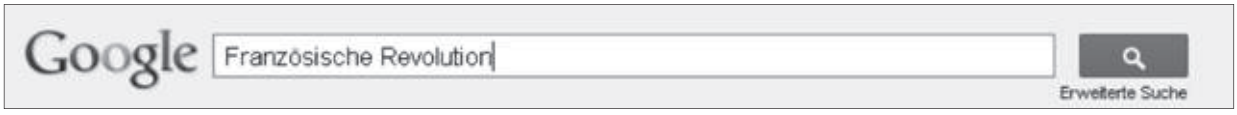
Arbeitsaufträge:

1. Lies bitte den Text über die Arbeitsweise von Suchmaschinen am Beispiel der Suchmaschine Google.
2. Beantworte danach bitte folgende Frage(n) zum Verständnis zunächst alleine schriftlich.
   Vergleicht dann in der Klasse:
   - ❶ Durchforstet Google das Internet bei jeder Suche von Neuem?
   - ❷ Warum arbeitet Google mit vielen Datenzentren weltweit statt mit einem einzigen Datenzentrum?
   - ❸ Wozu dient der sogenannte PageRank-Algorithmus?
   - ❹ Warum bekommt man ein Suchergebnis schneller, wenn man nach etwas sucht, was auch andere häufig suchen?
   - ❺ Was ist ein Snippet und wozu dient es?

Max sucht für ein Referat in der Schule auf ⓘ **www.google.de** Informationen über die „Französische Revolution".

Schritt 1: Eingabe der Suchanfrage

Die Suche beginnt mit der Eingabe eines Suchbegriffs in das Suchfeld, hier also [Französische Revolution].



Schritt 2 (unsichtbar): Die Suche nach dem richtigen Datenzentrum

Die großen Suchmaschinenbetreiber unterhalten weltweit dezentral angeordnete Datenzentren mit Servern, auf denen der Index gespeichert ist. Im Hintergrund werden sofort ein oder mehrere Datenzentren ausgewählt. Bei der Auswahl des richtigen Datenzentrums spielen räumliche Nähe, Geschwindigkeit und Auslastungsgrad eine entscheidende Rolle.

Schritt 3 (unsichtbar): Der Suchlauf durch den Index

Die Suchmaschine durchsucht nun den Index, also Dateien, die (Such-)Wörter und Internetadressen enthält. Dieser Index wurde mit Hilfe von Crawlern erstellt, die vorher das Netz durchforstet haben. Genau genommen sucht eine Suchmaschine nicht nach einem bestimmten Wort, sondern nach Buchstabenmustern. Deshalb überprüft die Suchmaschine, ob sich der Nutzer vertippt hat und eigentlich etwas ganz anderes suchen wollte. So zeigt sie evtl. [Französische Revolution] an, wenn man versehentlich [Franözische Revolution] eingibt.

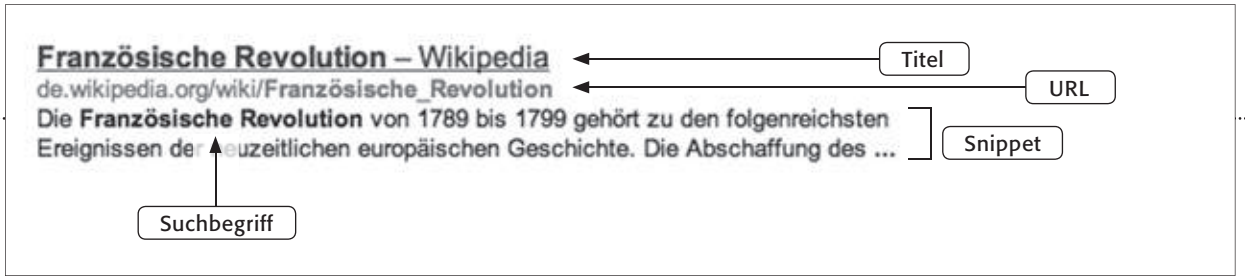


Schritt 4 (unsichtbar): Der Suchlauf nach dem richtigen Dokument

Die Index-Server enthalten ausschließlich Wörter und Adressen. Sie verweisen auf die sogenannten Doc-Server. Auf den Doc-Servern liegen der Titel, Textauszüge und weitere Daten aus den Dokumenten, die beim Durchforsten des Netzes von den Crawlern gefunden wurden. Diese Informationen sind zum einen für die Ausgabe nützlich (z. B. für die kurzen Textauszüge unter den Adressen, genannt Snippets), zum anderen sind sie die Grundlage für den PageRank-Algorithmus. Ein wichtiger Trick, um den Suchablauf zu beschleunigen, besteht darin, Ergebnisse häufiger Suchanfragen wie z. B. [Berlin] zwischenzuspeichern, d. h. nicht jedes Mal aufs Neue den Index zu durchsuchen, sondern auf bereits „fertige" Suchergebnisse zurückzugreifen.

Schritt 5: Ausgabe der Suchergebnisse

Im letzten Schritt müssen die Suchergebnisse so angezeigt werden, dass auf den ersten Blick die wichtigsten Internetseiten erkennbar sind. Die Reihenfolge der Treffer („Ranking") wird durch einen Algorithmus (bei Google PageRank genannt) festgelegt. Die Informationen werden so angezeigt, dass der Nutzer schnell erkennen kann, ob das Ergebnis für ihn brauchbar ist. Unter dem Titel des Dokuments wird die Webadresse der Seite (also die URL) angezeigt, darunter ein Teil des Textes („Snippet", Englisch für „Schnipsel"), in dem der jetzt fett markierte Suchbegriff enthalten ist.



3. Bei Google spielen mehr als 200 Faktoren eine Rolle bei der Reihenfolge der Auflistung von Suchergebnissen. Nach welchen Kriterien würdet ihr Suchergebnisse anordnen? Besprecht das in der Klasse.

Zusatzaufgabe/Hausaufgabe:

Ein Search Engine Optimizer (SEO) versucht, die Funktionsweise von Suchmaschinen zu verstehen und die Webseiten seiner Kunden so einzurichten, dass diese bei der Suche hoch bewertet (gerankt) werden, d. h. auf einer der ersten Ergebnisseiten zu finden sind.

1. Was glaubst du, warum das für Firmen wichtig ist?
2. Welche Probleme können dabei entstehen?

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 9**
Titel	**Einfluss von Suchmaschinen**
Ziele	Reflexion über den Einfluss von Suchmaschinen
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**2**
Methodische Hinweise und Lösungen	**Ablauf:** Drei Szenarien ermöglichen eine Auseinandersetzung mit dem Einfluss von Suchmaschinen, den Regierungen und Wirtschaftsunternehmen (aus)nutzen könn(t)en. Auch auf das Individuum haben Suchmaschinen einen Einfluss, der hier reflektiert werden kann. *Möglicher Einstieg:* „Wie wichtig sind Suchmaschinen für uns? Welchen Einfluss haben Suchmaschinen?" Das Arbeitsblatt 9 mit der Themenübersicht sowie der Methodenbeschreibung wird als Folie /auf Whiteboard gezeigt. Die Schüler werden in drei Gruppen eingeteilt oder melden sich für ein Thema ihrer Wahl. Die Gruppen bearbeiten ihren Text mit der Methode „Think – Pair – Share" (zu dieser kooperativen Lernform siehe z. B. ⓘ **http://lehrerfortbildung-bw.de/bs/bsa/bej/englisch/uebung/**). Am Ende jedes Textes befinden sich Textverständnisfragen für die Diskussion in der Gruppe. In einem kurzen Vortrag (mündlich) stellen die Gruppen ihr Thema nacheinander vor. Zur Strukturierung des Vortrags können sich die Schüler an vier Einstiegssätzen orientieren. **Mögliche Abschlussdiskussion:** *Zukunftsszenario:* Wie sehen Suchmaschinen im Jahr 2025 aus? Wie funktionieren sie? *Stichwörter:* Web 3.0 oder Semantisches Web. Suchmaschinen liefern die optimalen Ergebnisse einer Suche, weil sie in *intelligenter Weise* eine Anfrage mit den Informationen verknüpfen können. *Beispiel:* Man sucht nach einer Pizzeria in seiner Nähe. Die Verknüpfung von Geodiensten, das Rating in Bewertungsportalen und bisherige (Such-)Vorlieben ergeben das „optimale" Ergebnis (z. B. Google+ Local). *Keine Link-Weiterleitung* mehr auf andere Webseiten, sondern Antworten direkt auf der Ergebnisseite. *Beitrag auf Deutschlandfunk:* „Nutzer fragt, Google antwortet"; 24.3.2012: ⓘ **http://www.dradio.de/dlf/sendungen/computer/1712944/** *oder* *Beispiel einer semantischen Suchmaschine:* ⓘ **http://www.wolframalpha.com/** *oder* „Was Google nicht findet, gibt es nicht"–, die Grenzen von Suchmaschinen; Stichwort: „Das unsichtbare Netz". *Information:* ⓘ **http://www.ub.uni-bielefeld.de/biblio/search/help/invisibleweb.htm**
Methoden und Organisationsformen	Textarbeit, Think – Pair – Share; Gruppen, Plenum
Zugang Internet / PC	nein
Kapitel 1	Vollständigkeit: Welche Seiten führt der Suchindex auf?, Ausblick: Personalisierte Suche

1. Sucht euch eine Gruppe aus:

Stell dir vor …

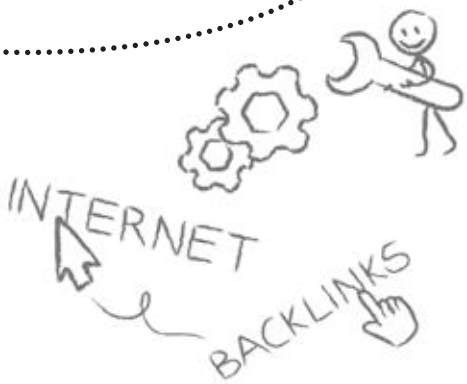


Gruppe 1
… du bist Diktator Alleinherrscher eines Staates.
Du willst das Internet für den Machterhalt einsetzen.
Wie können dir Suchmaschinen von Nutzen sein?



Gruppe 2
… du bist Internetnutzer in Deutschland im Jahr 2016.
Welche Vorteile oder Nachteile hast du persönlich durch die Suchmaschinennutzung?

Gruppe 3
… du bist Manager in einer großen Autofirma.
Wie könntest du eine Suchmaschine für die Geschäfte deiner Firma nutzen?



2. Arbeitet in der Gruppe mit der Methode Think – Pair – Share:

Methodenkasten Think – Pair – Share:

THINK: Denke leise über deine Antwort nach. Notiere Stichpunkte auf einem Zettel (Zeit: 2 Min.).
PAIR: Suche dir einen Partner in deiner Gruppe. Teile ihm deine Antworten mit. Höre auch deinem Partner zu (Zeit: 5 Min.). Lies den Text zu eurer Situation durch.
SHARE: Sammelt gemeinsam in der gesamten Gruppe eure Ideen und Gedanken für eure Situation (Zeit: 15 Min.).

3. So könnt ihr euren Vortrag vor der Klasse strukturieren:

Wir haben die Situation …
Unser Text ging darüber …
Die ideale Suchmaschine unserer Situation sähe so aus …
Wir haben über folgende Fragen diskutiert …

Gruppe 1: Zensur von Informationen

… du bist Diktator (Alleinherrscher) eines Staates.
Du willst das Internet für den Machterhalt einsetzen.
Wie können dir Suchmaschinen von Nutzen sein?

Text 1: Google beendet Selbstzensur in China

Der Streit zwischen dem Internetkonzern Google und der chinesischen Regierung eskaliert: Google bietet ab sofort für China eine unzensierte Suchmaschine an. Die Regierung in Peking reagiert empört und verhindert nun mit anderen Mitteln den Zugang zu vorher zensierten Informationen.

Bereits im Januar hatte Google aus Protest gegen Zensur mit seinem Rückzug aus dem Chinageschäft gedroht. Jetzt hat der Konzern seinen Worten Taten folgen lassen. Besucher der chinesischen Webseite ⓘ **www.google.cn** fanden erstmal nicht mehr ihre gewohnte Suchmaske. Diese wurde gestoppt. Auf Informationen mussten die Chinesen trotzdem nicht verzichten. Der amerikanische Google-Konzern hat seine chinesische Webseite nach Hongkong verlegt. Wer wie gewohnt das chinesischsprachige google.cn anklickt, wird automatisch umgeleitet nach google.com.hk. HK steht dabei für Hongkong. Die Stadt hat einen Sonderstatus. Hier gelten nicht die strengen Zensurbestimmungen wie auf dem kommunistischen Festland.
(Anm. d. Red.: Mittlerweile ist auch google.cn wieder abrufbar.)

Chinas Regierung reagiert empört
Als Google im Jahr 2006 seine chinesische Webseite startete, verpflichtete sich das Unternehmen, sich den chinesischen Zensurbestimmungen zu unterwerfen. Suchbegriffe, die in den Augen der Zensoren sensibel sind, werden gefiltert.
Auf die Ausweichtaktik, die chinesische Google-Webseite nach Hongkong zu verlegen, reagierte Peking prompt.

Filtersysteme greifen
Dabei bleibt eigentlich alles beim Alten. Sofort, nachdem Google seine chinesische Webseite nach Hongkong verlegte, wurden die chinesischen Filtersysteme aktiv. In Hongkong kann man alle Seiten problemlos unter www.google.com.hk öffnen. Chinesen vom kommunistischen Festland aber scheitern, wenn sie versuchen, über die neue Hongkonger Google-Webseite an zensierte Informationen zu kommen. Internetnutzerin Ren hat es versucht: „Über die Hongkonger Version kann man auch keine zensierten Seiten öffnen. Wenn man da Begriffe wie „Platz des Himmlischen Friedens" oder „Tibet" eingibt, dann bekommt man zwar viele Ergebnisse, aber die Seiten lassen sich nicht öffnen", erzählt sie. (…)

Internet-Zensur in China
Das chinesische Internet wird systematisch nach Begriffen wie „Opposition", „Tibet" oder „Taiwan" durchsucht. Mehr als 30.000 „Internetpolizisten" durchkämmen inländische und ausländische Webseiten, Mails und Diskussionsforen nach verbotenen Inhalten. Unliebsame Seiten werden gelöscht.
Wer Texte ins Netz stellt, die nach Ansicht der kommunistischen Regierung die Staatssicherheit gefährden, macht sich eines Kapitalverbrechens schuldig. Dutzende Internet-Dissidenten sitzen in Haft. Bis zu zehn Jahre Gefängnis drohen demjenigen, der die strengen Richtlinien verletzt. (…)

(Von Petra Aldenrath, ARD-Hörfunkstudio Peking,
Quelle: www.tagesschau.de, Stand 5.12.2011)

VERSTÄNDNISFRAGEN:

Zensieren bedeutet ☐ Schulnoten vergeben ☐ unerwünschte Informationen zurückhalten
☐ unterdrücken ☐ alle dürfen sagen, was sie denken

In China werden Suchergebnisse zensiert ☐ richtig ☐ falsch

In China bekommt man über Google alle vorhandenen Seiten angezeigt ☐ richtig ☐ falsch

Google bietet in China keine Seiten mehr an ☐ weil es in Hongkong billiger ist
☐ weil China nicht alle Seiten zulässt

Denkanstöße: Wo findet Zensur heute statt? Was kann man gegen Zensur tun?
Was bedeutet in diesem Zusammenhang Propaganda?

Schaut auch hier: ⓘ **http://www.google.com/transparencyreport/**

Gruppe 2: Personalisierung von Suchergebnissen

… du bist Internetnutzer in Deutschland im Jahr 2016.
Welche Vorteile hast du persönlich durch die Suchmaschinennutzung?

Text 2: Ein Kommentar zur zunehmenden Personalisierung von Suchergebnissen

Ist Ihnen bewusst, dass Ihr Google anders aussieht als mein Google? Oder das Ihres Nachbarn? Ihrer Kollegen? Die gleiche Suchanfrage und doch andere Ergebnisse? Undenkbar? So erstaunlich das klingen mag, es ist die Realität für viele heutige Suchanfragen. Die Annahme, die Google-Ergebnisse seien für alle gleich und dabei immer objektiv, ist in Zeiten zunehmender Personalisierung im Internet ein gefährlicher Irrglaube. (…)

Personalisierte Ergebnisse dämpfen Informationsflut

Von außen betrachtet erscheint die Vorgehensweise von Google sinnvoll. Eine persönlichere Ergebnisliste, zugeschnitten auf die jeweiligen Interessen und Bedürfnisse des Nutzers, ist in der Tat begrüßenswert. Werden doch auf diese Weise in der Informationsflut Streuverluste gemindert und sehr oft passendere Ergebnisse angezeigt. Personalisierung kann daher ein Vorteil für den Nutzer sein.

Das Problem ist aus diesem Grund nicht so sehr das „Ob", sondern das „Wie" und auch das „Wieviel". Man muss sich bewusst machen, wie die Suchmaschine es schafft, uns passende personalisierte Treffer anzuzeigen. Denn dazu muss Google eine Menge über uns wissen. Google nutzt zu diesem Zweck die unterschiedlichsten Quellen und Daten. (…) Grundsätzlich gilt: je mehr Daten ein Nutzer öffentlich verfügbar macht und je öfter er bei Google mit eigenem Nutzerkonto, beispielsweise für Google Mail, eingeloggt ist, desto personalisierter werden die Suchergebnisse sein.

Personalisierung schafft Tunnelblick

Anhand dieser Daten „glaubt" Google zu wissen, was für unsere Suchanfrage die bestmöglichen Ergebnisse sind. Doch in vielen Fällen kann diese Annahme des Suchalgorithmus ein Irrglaube sein. Nicht immer spiegeln die im Web über uns verfügbaren Informationen unsere wirkliche oder aktuelle Interessenslage wider. Nur weil man während der Bundestagswahl intensiv das Wahlprogramm einer bestimmten Partei in Google recherchiert hat, muss dies noch lange nicht bedeuten, dass man später verstärkt Nachrichtenergebnisse erhalten möchte, die im Zusammenhang mit dieser Partei stehen. Interessen von Menschen ändern sich. Auch können Suchanfragen vielleicht gar nicht für den Nutzer selbst durchgeführt werden, sondern für dessen Partner oder Kollegen. (…)

Je personalisierter Suchergebnisse werden, desto weniger zeigen sie von dem, was im Web außerhalb meines Interessens- und Meinungsumfeldes existiert. Eine Art Tunnelblick entsteht. Auch führt dies dazu, dass sich das Web ein Stück weit in Richtung klassischer Medien wie TV oder Print entwickelt. Nicht mehr der Nutzer zieht sich die Informationen selbst, sondern er bekommt geliefert. (…)

http://www.teltarif.de/mein-google-dein-google

(Quelle: Auszüge von Nils Merker, http://www.teltarif.de/Google-personalisierung-suchmaschine-kritik/news/44584.html; Stand: 13.11.2011)

VERSTÄNDNISFRAGEN:

Suchergebnisse werden „personalisiert", bedeutet

☐ Google zeigt alle Seiten zum Thema.
☐ Google sortiert die Ergebnisse nach den Interessen der Nutzer.
☐ Alle Menschen erhalten bei Google auf den gleichen Suchbegriff die gleichen Ergebnisse.

Markiere Vorteile der personalisierten Suche mit +, Nachteile mit –

☐ Man findet schneller Dinge, die einen interessieren.
☐ Google trifft Annahmen, was uns interessieren könnte.
☐ Je mehr eine Suchmaschine nur meine Interessen beachtet, desto weniger erfahre ich über die Welt.
☐ Man muss sich nicht durch viele uninteressante Seiten wühlen.

Denkanstöße:

Was passiert mit dem Mensch, wenn Suchmaschinen nur noch liefern, was Menschen sehen, lesen und hören wollen?
Was geschieht, wenn nur massentaugliche Ergebnisse angezeigt werden (z. B. Google Autocomplete)?

Gruppe 3: Search Engine Optimization (SEO)

… du bist Manager in einer großen Autofirma. Wie könntest du eine Suchmaschine für die Geschäfte deiner Firma nutzen?

Text 3: Google sperrt nun auch deutsche Webseiten mit versteckten Suchwörtern aus

Man kann es auch in den deutschen Richtlinien des Suchmaschinenbetreibers nachlesen, dass Webseiten mit versteckten Wörtern und anderen Tricks zur Erhöhung des Trefferrankings unerwünscht sind. Bisher hatte Google sich auf die Sperrung englischsprachiger Sites beschränkt, in diesem Jahr sollen auch alle ausländischen Seiten mit unerwünschten Manipulationen vom Suchergebnis ausgeschlossen werden, kündigte der Chef-Entwickler von Google Matt Cutts in seinem Blog an.

Einer der ersten Betroffenen ist der deutsche Autobauer BMW, dessen auf Java-Skript basierende Startseite nun nicht mehr unter den Google-Treffern auftaucht. BMW benutzt eine sogenannte Doorway Page, die allerdings mit unsichtbarem Text unterlegt ist, in dem recht sinnlos zusammengereimt dutzendweise die Wörter Gebrauchtwagen, Jahreswagen und BMW vorkommen. Ein solches Vorgehen dient nach Ansicht von Google nicht dem Leser einer Seite, sondern nur dem Betreiber, der künstlich Surfer auf sein Web-Angebot lockt. Ebenfalls ausgesperrt wird die Gebrauchtwagen-Plattform Automobile.de.

Sie fühlt sich allerdings zu Unrecht ausgeschlossen. Suchte man nämlich bei Google nach bestimmten Autos, erhielt man bei den Automobile.de-Treffern nach dem ersten Klick einen Auszug aus deren Datenbank, der auch Dutzende von immergleichen Wörtern enthält – allerdings den wirklich gesuchten. Die Angaben stammen von unterschiedlichen Angeboten, darunter auch kostenlosen Privatinseraten. Der Fehler von Automobile.de war nach deren Angaben, mit sogenannten Brückenseiten zu arbeiten, die nicht den Google-Richtlinien entsprechen. Automobile.de sei von Google aufgefordert worden, seine Seiten zu überarbeiten und sich anschließend bei Google zu melden – was man getan habe. In einer Erklärung heißt es: „Auch wenn wir der Ansicht sind, dass Automobile.de die Fahrzeugsuchenden nicht in die Irre geführt hat, wurden die Brückenseiten von uns umgehend gelöscht." Nun hoffe man auf eine baldige Wiederaufnahme in den Index.

(Quelle: http://www.heise.de/newsticker/meldung/Google-sperrt-nun-auch-deutsche-Webseiten-mit-versteckten-Suchwoertern-aus-172419.html, Stand: 5.2.2006)

VERSTÄNDNISFRAGEN:

Google hat kurzzeitig die Seiten von BMW nicht angezeigt, weil

☐ BMW versucht hat, sich auf der Trefferseite nach oben zu schummeln.
☐ BMW versucht hat, Google zu kaufen.

Firmen möchten in den Suchergebnissen weit oben genannt werden, weil

☐ viele Menschen nur die oberen Treffer ansehen.
☐ man dafür einen Preis erhalten kann.

Denkanstöße:

Wer kontrolliert Suchmaschinen?
Was können Suchmaschinenbetreiber gegen Spamming unternehmen?
Ist SEO Manipulation oder Optimierung?

5_1 Internet – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 10**
Titel	**Datenschutz und Nutzerinformationen in Suchmaschinen**
Ziele	Kennenlernen von Datenschutzaspekten und Anstoß zu einem kritischen Nutzungsverhaltens
Ungefähre Zeitangabe (Unterrichtsstunden à 45 Min.)	**3**
Allgemeine Methodische Hinweise zum Ablauf	**Möglicher Einstieg:** Der Textausschnitt aus den Datenschutzerklärungen von Google auf dem Blatt „Datenschutz in Suchmaschinen" kann gemeinsam gelesen und von den Schülern in eigenen Worten erklärt werden. Bei „Google Trends" finden sich Informationen darüber, welche Suchbegriffe in Google wie oft eingegeben wurden. Mit diesem Dienst können Rückschlüsse auf Trends in der Gesellschaft gezogen werden, wie bspw. die Vorhersage einer Grippewelle (https://de.wikipedia.org/wiki/Google_Trends, abgerufen am 29.03.2016): **https://www.google.com/trends/home/all/DE** **Mögliche Frage:** „Welche Vor- oder Nachteile kann es haben, wenn Suchmaschinen unsere Daten speichern?" Die Jugendlichen teilen sich in 2 Gruppen und bearbeiten je ein Arbeitsblatt. Die Rechercheergebnisse werden auf Plakaten dargestellt und präsentiert. Die Aufgaben auf den Blättern können innerhalb der Gruppen auch arbeitsteilig vergeben werden, um Zeit zu sparen.
Methoden und Organisationsformen	Gruppen
Zugang Internet / PC	ja (für alle Gruppen nötig)
Kapitel 3	Datenschutz und Suchmaschinen

Gruppe 1: Datenschutz in Suchmaschinen **Methodische Hinweise und Lösungen**	**Lösung Aufgabe 1:** verwendeter Browser; Sprache, die du verwendest; Zeitpunkt der Anfrage; IP-Adresse; Cookies; Suchbegriffe; Ort der Anfrage; Datum *Quellen (bitte immer Aktualität prüfen!):* **Google:** Lösung Aufg. 1 gilt bei einfacher Suche, d. h. ohne Anmeldung in einem Benutzerkonto: (https://www.google.de/intl/de/policies/privacy/, Stand 29.03.2016) Bei Besitz eines Google-Accounts: Unsere automatisierten Systeme analysieren Ihre Inhalte (einschließlich E-Mails), um Ihnen für Sie relevante Produktfunktionen wie personalisierte Suchergebnisse, personalisierte Werbung sowie Spam- und Malwareerkennung bereitzustellen. (https://www.google.de/intl/de/policies/privacy/, Stand 29.03.2016) Und: Unter Umständen verknüpfen wir personenbezogene Daten aus einem Dienst mit Informationen und personenbezogenen Daten aus anderen Google-Diensten. (https://www.google.de/intl/de/policies/privacy/, Stand 29.03.2016) **Bing:** (https://privacy.microsoft.com/de-de/privacystatement/, Stand 30.03.2016) **Mögliche Lösungen Aufgabe 2:** *Auskunftsrecht nutzen:* bei Besitz eines Google-Kontos Dashboard regelmäßig kontrollieren **https://www.google.com/dashboard/?hl=de**, Persönliche Daten & Privatsphäre > Aktivitätseinstellungen – Ihre Suchanfragen und Browseraktivitäten – Verlauf verwalten – Web- & App- Aktivitäten – Löschoptionen (siehe Reiter rechts oben „...") *Cookies löschen:* siehe Gruppe 2 Tipp: Als Nutzer kann man sich von Google daran erinnern lassen, monatlich seine Kontoaktivität zu überprüfen. Einfach im Dahsboard das entsprechende Häckchen setzen. *Browser Plug-ins installieren:* Neben „Track me not" gibt es noch andere Browser-Add-ons wie z. B. Ghostery, die über Tracking-Cookies und Social Plug-ins der besuchten Webseite u. a. informieren. Infos: **https://www.datenschutzzentrum.de/tracking/schutz-vor-tracking.html** *Suchmaschinen wechseln:* Metager (https://www.metager.de/datenschutz/) ist – neben ixquick bzw. startpage (**https://www.ixquick.com/deu/protect-privacy.html**) oder DuckDuckGo (**https://duckduckgo.com/privacy**) – eine Suchmaschine, die verspricht, keine IP-Adressen und personenbezogenen Daten der Anwender/innen zu erheben.

Gruppe 1: Datenschutz in Suchmaschinen

Methodische Hinweise und Lösungen

Lösung Aufgabe 3:
Die Standardeinstellung bei der Facebook-Anmeldung ist derzeit (30.03.2016) so, dass man über Suchmaschinen gefunden werden kann! Bei unter 18-Jährigen ist die Auffindbarkeit über externe Suchmaschinen generell gesperrt, d. h. dies kann nicht vom Nutzer verändert werden (Der Nutzer kann hier lediglich anklicken „Aktivieren, wenn ich 18 werde").
Privatsphäre-Verknüpfungen – Weitere Einstellungen anzeigen –> Wer kann nach mir suchen? - Möchtest du, dass Suchmaschinen außerhalb von Facebook dein Profil anzeigen? (es darf kein Häkchen gemacht werden, sonst Aktivierung!)

Gruppe 2: Werbung in Suchmaschinen und Cookies

Methodische Hinweise und Lösungen

Lösung Aufgabe 1:
Cookies sind kurze Textinformationen, die Webserver in Browsern speichern und später wieder abrufen können. Diese Informationen haben eine festgelegte Lebensdauer und werden für verschiedene Funktionen verwendet, wie persönliche Einstellungen (Schriftgröße oder Sprache auf einer Webseite), aber auch zur Aufzeichnung des Surfverhaltens. So können benutzerspezifische Profile erstellt werden, die zu Werbezwecken genutzt werden können → Stichwort „personalisierte Werbung".

Lösung Aufgabe 2:
Vor- und Nachteile von Cookies:

+	–
Durch Cookies kann sich eine Webseite Vorlieben merken, die man nicht jedes Mal wieder neu angeben will, wie z. B. die Sprache oder Schriftgröße.	Es ist möglich, durch Cookies das Surfverhalten einer Person über einen langen Zeitraum hinweg zu dokumentiere. Das kann ein Eingriff in die Privatsphäre sein.
Durch Cookies ist es möglich, personalisierte Werbung zu schalten, wodurch man im Idealfall wirklich nur über das informiert wird, was einen auch interessiert.	Benutzen mehrere Personen einen Computer, kann es sein, dass anderen Personen die eigenen Nutzerdaten beim Anmeldevorgang angezeigt werden.
Cookies machen das sichere Einkaufen über einen Online-Shop erst möglich, da die Seite den Nutzer über den gesamten Einkaufsvorgang hinweg eindeutig zuordnen kann.	Viele Websites verlangen heute, dass Cookies akzeptiert werden, sonst lässt sich die Seite nicht aufrufen.

Fazit: Cookies sind nicht perse schlecht. Man sollte aber wissen, wozu sie da sind, und beim Surfen darauf achten, sie bei Bedarf zu blockieren oder nach jeder Sitzung zu löschen.
Es empfiehlt sich auch, Browser-Add-ons zu installieren, wie z. B. Ghostery.

Lösung Aufgabe 3:
Aktuelle Anleitungen zum Löschen von Cookies finden sich im Internet unter dem Suchbegriff „Cookies löschen" (Internet Explorer, Mozilla Firefox, Google Chrome, iPhone, Samsung etc.)
Sollten einige Jugendliche über Smartphones verfügen, macht es natürlich Sinn, die Anleitung für die entsprechenden Geräte zu recherchieren und zu nutzen!



Tipp: In schulischen Netzwerken haben die Nutzer oft nicht die Rechte, Cookies zu löschen, hier können stattdessen Anleitungen für Smartphones erstellt werden.

Lösung Aufgabe 4:
Der QR-Code verweist auf folgende Seite*:*
Bei Google: *Datenschutzerklärung und Nutzungsbedingungen – Transparenz und Wahlmöglichkeit – Anzeigeneinstellung – Interessensbezogene Werbung ausschalten*
Bei Bing: *Anzeigen auf Bing – Personalisierte Werbung in diesem Browser – ausschalten*

Gruppe 1: Datenschutz in Suchmaschinen

Suchmaschinen werden manchmal als Datensammler bezeichnet.

Google schreibt:
Sie können unsere Dienste auf vielfältige Weise nutzen – um Informationen zu suchen und zu teilen, um mit anderen zu kommunizieren oder um neue Inhalte zu erstellen. Wenn Sie uns Informationen mitteilen, zum Beispiel durch Erstellung eines Google-Kontos, können wir damit diese Dienste noch weiter verbessern – indem wir Ihnen relevantere Suchergebnisse und Werbung anzeigen, Ihnen dabei helfen, mit anderen in Kontakt zu treten oder schneller und einfacher Inhalte mit anderen zu teilen. .

https://www.google.de/intl/de/policies/privacy/, Stand 29.03.2016

Arbeitsaufträge:

1. Welche Daten werden bei einer Suchanfrage gesammelt? Was vermutet ihr? Unterstreicht!

   Geburtstag · Lieblingsmusik · verwendeter Browser · Vorname · Beruf · Adresse · Körpergröße
   Telefonnummer · Aufenthaltsort · Krankheiten · Sprache, die du verwendest · Nachname
   E-Mail-Adresse · Geschlecht · Zeitpunkt der Anfrage · IP-Adresse · Cookies · Kreditkartennummer
   Name der Eltern · Suchbegriffe · Ort der Anfrage · Temperatur · Datum · Haarfarbe · Hobbies · Schule

   Überprüft eure Vermutungen hier:

   Google: **https://www.google.de/intl/de/policies/privacy/**

   Bing: **https://privacy.microsoft.com/de-de/privacystatement/**

   Ist das o.k. oder nicht? Diskutiert in eurer Gruppe!

2. Erstellt auf einem Plakat Datenschutztipps für die Nutzung von Suchmaschinen. Ihr könnt dafür im Internet recherchieren.

3. Soziale Netzwerke sind Datenschätze! Und viele Informationen, die man ins Netzwerk stellt, sind von Suchmaschinen auffindbar. Wie kann man bei dem Sozialen Netzwerk Facebook einstellen, dass das eigene Profil nicht von Suchmaschinen aufgefunden wird? Erstellt eine Anleitung für eure Klassenkameraden.

Gruppe 2: Werbung in Suchmaschinen und Cookies



Suchmaschinen sind für euch kostenlos, aber warum ist das so?
Viele Suchmaschinen verdienen Geld durch die Werbung, die ihr neben den Suchergebnissen angezeigt bekommt. Spricht man von personalisierter Werbung, bedeutet das, dass sich die Werbung auf Dinge bezieht, nach denen ihr schon einmal im Internet gesucht habt. Dafür nutzt die Suchmaschine Cookies. Aber sind Cookies nicht eigentlich KEKSE?

Arbeitsaufträge:

1. Was sind Cookies? Recherchiert in Partnerarbeit auf der Seite „Surfer haben Rechte" und findet die Antwort im Text!

   http://www.surfer-haben-rechte.de → Themen → Cookies

   Erklärt euch gegenseitig, was Cookies sind, dann besprecht es in eurer Gruppe und findet gemeinsam eine Definition, die ihr auf das Plakat schreibt.

2. Welche Vor- und Nachteile haben Cookies? Stellt sie in einer Tabelle auf dem Plakat zusammen!

+	–
…	…

3. Wie kann man die Cookies im Browser löschen? Erstellt eine Anleitung für einen der Browser (Mozilla Firefox, Internet Explorer, Google Chrome) oder euer Handy, die eure Klassenkameraden testen und beurteilen sollen. Ihr könnt entweder schriftlich nur den Weg beschreiben, oder ihr fertigt Screenshots an.

4. Was kann man tun, wenn man keine personalisierte Werbung haben möchte? Informiert euch dazu auf den Seiten der Suchmaschinenanbieter und zeigt den anderen, wie man das verhindern kann.

   Falls ihr Hilfe braucht:
   (Oder fragt eure Lehrkraft nach dem Link.)

Tipp: So fertigst du einen Screenshot („Bildschirmfoto") an

Drücke auf deiner Tastatur die „Druck"- oder „Print"-Taste. So kopierst du das, was dein Bildschirm gerade anzeigt, in die Zwischenablage. Öffne ein Textverarbeitungsprogramm wie „Word", das Programm „Paint" oder ein anderes Bildbearbeitungsprogramm (Start > Programme > Zubehör > Paint) und füge deinen Screenshot ein („Strg" + „V"). Speichere das Bild so ab, dass du es wiederfindest, wenn du es jemandem zeigen willst.

Unter **Mac OS X** können Bildschirmfotos durch die Tastenkombination cmd + Shift + 3 (gesamter Bildschirm) bzw. cmd+Shift + 4 (rechteckiger Teil eines Bildschirms, mit der Maus „aufgezogen") erzeugt werden. Die Bilddateien werden standardmäßig als Bilddateien im PDF-Format oder PNG-Format auf dem Schreibtisch abgelegt.



5_2 PC-Sicherheit – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ◐●	**AB 2** ◐◐
Titel	**Online – was soll nicht in fremde Hände**	**Euer Funknetz – ist es sicher?**
Kompetenzen	Die Schülerinnen und Schüler kennen die Bedeutung von Verlauf, Cookies, Passwörtern und Cache im Zusammenhang mit einem Browser. Sie können Einstellungen verändern und gespeicherte Daten löschen.	Die Schülerinnen und Schüler organisieren ein Interview mit einem Funknetz-Betreiber und werten es nach einem Fragenkatalog zur WLAN-Sicherheit aus.
Methoden	Internet-Recherche, Partnerarbeit, Unterrichtsgespräch	Interview, Recherche, Fragenkatalog, Checkliste, Einzelarbeit, Partnerarbeit, Unterrichtsgespräch
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	Ja (evtl. zur Recherche der Fach-Fragen)

Hinweise für die Durchführung

AB 1: Online – was soll nicht in fremde Hände	Verlauf, Cookies, Passwörter und Cache sind Stichworte, bei denen die Browser Daten über das Surfverhalten speichern. Im „Verlauf", auch „History" oder „Besuchte Seiten" o. ä. genannt, werden die Seiten gespeichert, die aufgerufen wurden. Dies hat den Vorteil, dass man einmal besuchte Seiten schneller wiederfindet. Es hat den Nachteil, dass jeder mit Einblick in das System sehen kann, welche Seiten ich aufgerufen habe. Die „Cookies" sind kleine Dateien, die die Anbieter von Internetseiten auf den Computern hinterlassen können (mehr darüber in den Sachinformationen). Sie enthalten Informationen darüber, auf welchen Seiten man war, wie lange, was man genau gesucht hat etc. Leider wird oft die Möglichkeit genutzt, Passwörter von Browsern verwalten zu lassen. Der Sinn dahinter ist, dass man es beim Aufruf einer passwortgeschützten Seite nicht einzugeben braucht. Leider mit einer großen Unsicherheit, denn der Browser stellt eine potenzielle Sicherheitslücke dar, wie viele Beispiele der Vergangenheit zeigen. Der „Cache" schließlich ist eine Art Zwischenspeicher auf dem eigenen Computer, wo Dateien wie Internetseiten mit Text, Bildern, Videos usw. abgelegt werden. Dies soll ein schnelleres Surfen ermöglichen, da diese Daten nicht erneut aus dem Internet geladen werden müssen. In Zeiten des Breitbands eigentlich nicht mehr so wichtig. Alle diese Daten ermöglichen es, Informationen über mein Surfverhalten zu erhalten. Bei problematischen Dingen (zum Beispiel illegale oder strafbare Downloads) kann darüber sogar strafrechtlich Relevantes erkannt werden. Alle Browser ermöglichen aber eine Löschung der Daten oder gar ein „privates Surfen" (oder ähnlich genannt), bei dem die Daten nicht gespeichert werden. Entsprechende Anleitungen finden sich sicherlich auf YouTube. Das Arbeitsblatt beinhaltet viele Rechercheaufgaben, ausreichend PCs für die Schülerinnen und Schüler sind hier notwendig.

AB 2: Euer Funknetz – ist es sicher?

Möchten Sie einen sehr eindrucksvollen Einstieg gestalten, dann nennen Sie die Funktion „Persönlicher Hotspot" Ihres Handy mit einem üblichen WLAN-Namen, zum Beispiel der Restaurant-Kette McDonalds oder Subways … und schalten es ein. Sofort taucht auf den Handys der Schüler dieses WLAN auf mit der Frage, sich zu verbinden. Wäre (DAS sollten Sie natürlich NICHT tun) nun das WLAN offen, wären die Handys mit dem Netz verbunden und ließen einen Zugriff zu.

Offene, unverschlüsselte WLAN-Netze bergen Risiken. So ist der Datenverkehr unter Umständen für Dritte auslesbar, wodurch Zugangsdaten mitgelesen werden könnten, z.B. wenn Internetseiten selbst nicht HTTPS-verschlüsselt sind.

Public Spot Betreiber die ihr WLAN Anderen zur Verfügung stellen, haften grundsätzlich nicht als sogenannte Störer für Urheberrechtsverstöße Dritter. WLAN-Betreiber können jedoch unter Umständen zu Inhaltssperren verpflichtet werden. Als Public Spot Betreiber sollte man Nutzungsbedingungen erstellen und diese den Nutzern zur Verfügung stellen oder noch besser die Nutzung des Public WLAN von der Zustimmung der Nutzungsbedingungen abhängig machen. Das heimische WLAN sollte weiterhin grundsätzlich mit einem Passwort und einer Verschlüsselung versehen werden. Für Gäste sollte ein separates Gäste WLAN eingerichtet werden, damit das WLAN Passwort nicht bekannt gegeben werden muss.

Bei diesem Arbeitsblatt sind Erwachsene nötig. Die Schülerinnen und Schüler sollen anhand eines Fragenkatalogs die Sicherheit eines Funknetzes kontrollieren, indem sie einen Betreiber eines Funknetzes (das kann auch der Nachbar sein) interviewen. Als Sicherung sollen sie eine Checkliste erstellen, die die Frage beantwortet: „Worauf muss ich achten, wenn ich in ein Funknetz gehe?"

Die Möglichkeit, das Interview auch per Video zu führen ist sicherlich motivierend und mit einem Handy leicht zu bewerkstelligen. Wenn das Einverständnis der interviewten Person vorliegt, sollen die Schülerinnen und Schüler das Ergebnis präsentieren.

Lust auf mehr?

- Das Thema WLAN ist immer wieder spannend und wird immer aktueller, was sich auch den Bemühungen vieler Kommunen erkennen lässt, kostenlose WLAN-Zugänge zum Beispiel vor Touristenattraktionen zur Verfügung zu stellen.

Hier finden Sie gute Videos zum Thema:

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/FremdeWLAN/fremdeWLAN_node.html

https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/stoererhaftung-besserer-schutz-fuer-wlanbetreiber-19261

Online – was soll nicht in fremde Hände?

Arbeitest du an einem Computer, den mehrere Personen benutzen? Zu Hause oder in der Schule? Dann solltest du einige Dinge unbedingt wissen. Deine Browser (vom englischen „to browse“: blättern, schmökern), wie zum Beispiel der **Internet Explorer, Google Chrome, Safari** oder der **Mozilla Firefox**, sind ganz schön speicherwütig. Daten über dein Internet-Surfen werden von ihnen automatisch gespeichert. Vor allem Folgende:

- **Verlauf (oder auch Chronik)**
  Hier werden deine besuchten Seiten gespeichert. Der nächste Benutzer kann also sehen, welche Seiten du aufgerufen hattest.
- **Cookies**
  Cookies (vom englischen „Kekse“) sind kleine Dateien, die von Internetseiten auf deinem Computer abgelegt werden können. Darin kann stehen, wann du das letzte Mal auf der Seite warst, welche deine Lieblingsseite ist und vieles andere.
- **Passwörter**
  Die Browser ermöglichen es, Passwörter zu speichern, sodass du sie beim Aufrufen einer Internetseite nicht mehr eingeben musst. Diese Passwörter sind also auf dem Computer gespeichert.
- **Cache**
  Der „Cache“ ist ein Speicherplatz auf deinem Computer. Darin legt der Browser ganze Internetseiten ab, um darauf beim nächsten Aufruf schneller zugreifen zu können. Das war besonders notwendig, als es noch keine schnellen Internetverbindungen gab. Also sind ganze Seiten inklusive aller Bilder, Videos und Texte auf deinem Computer gespeichert.

Tipp: Die Browser ändern sich ständig, aber wenn du eine aktuelle Anleitung suchst, wie du die gespeicherten Daten löschen kannst, dann gib doch bei YouTube folgendes als Suchbegriffe ein: „browser daten löschen“. Hier findest du sicherlich eine Anleitung für deinen Lieblings-Browser!



Quelle: Screenshot klicksafe

Arbeitsaufträge:

1. Überlege und schreibe auf, warum diese Daten nicht in fremde Hände fallen sollten:

a. Verlauf

.....

b. Cookies

.....

c. Passwörter

.....

d. Cache

.....

2. Schaue nach, wie und wo du sie löschen kannst!

3. Kannst du einstellen, dass diese Daten automatisch beim Schließen gelöscht werden? Oder kannst du einstellen, dass die Daten gar nicht gespeichert werden (dies wird oft „privates Surfen“ oder ähnlich genannt)? Erkläre deiner Nachbarin/deinem Nachbarn, wie dies geht!

4. In deinem Handy passiert übrigens genau das gleiche. Abhängig von deinem Betriebssystem (zum Beispiel iOS, Android oder Windows) speichert dein Handy viele Daten darüber, wo du wann auf welchen Seiten im Internet warst. Findet euch in kleinen Gruppen mit dem gleichen Betriebssystem zusammen. Recherchiert, wie ihr die Spuren beim Internet-Surfen löschen könnt und probiert es aus! (Aber Vorsicht: Es gibt auch Einstellungen, alle Daten, also auch Adressen, Telefonnummern und Fotos etc. auf dem Handy zu löschen!)

Euer Funknetz – ist es sicher?

Funknetze oder auf Englisch „WLAN" – sind der absolute Renner in der digitalen Welt. Man findet sie mittlerweile überall: In Restaurants, auf Flughäfen, in Fußgängerzonen und im Fußballstadion – und vielleicht auch bei dir Zuhause?
Doch gerade bei Funknetzen kann viel passieren. So kann jemand in das Funknetz „einbrechen" und zum Beispiel alles lesen, was in deinem Computer / Handy gespeichert ist oder jemand kann das Funknetz „abhören" und möglicherweise die Passwörter stehlen, die man eingibt. Und weil es auch um deine Daten geht, darfst du mal jemandem (Mitschülerin / -schüler, Lehrerin / Lehrer, Nachbarin / Nachbar in deiner Straße …), der ein Funknetz zu Hause hat, ein paar unangenehme Fragen stellen.

Arbeitsaufträge:

1. Führe das Interview durch und notiere die Antworten in der dritten Spalte! Die richtigen Antworten findest du in der zweiten Spalte! Du darfst das Interview auch per Video (mit dem Handy) führen und der Klasse zeigen, wenn die interviewte Person das Einverständnis dazu gegeben hat.

Ist das Funknetz einbruchssicher? Wenn ja, wie?	Hier müssen die Begriffe WEP (ein altes, schlechtes System) oder WPA (gut!) fallen.	
Sendet es automatisch seinen Namen aus? (SSID genannt)	Jedes Funknetz hat einen Namen, der normalerweise ausgesendet wird. Dadurch kann z. B. Windows melden „Funknetz erkannt". Dies kann man abstellen, was sicherer ist, denn nun kann sich niemand automatisch einwählen.	
Ist der Name (SSID) verändert worden oder hat es noch den Standardnamen?	Normalerweise haben die Funknetze schon Namen wie die Firma (zum Beispiel „Netgear"). Besser ist ein eigener Name!	
Ist die Funkübertragung verschlüsselt?	Wie oben, hier gibt es zwei Systeme: WEP (schlecht) und WPA (gut!), WPA2 oder sofern verfügbar WPA3 (gut!). Wer nicht verschlüsselt, der kann „abgehört" werden und riskiert, dass zum Beispiel seine Passwörter entschlüsselt werden.	
Mit welchem Passwort?	Wer sein Passwort verrät, hat nichts von Sicherheit kapiert ;-). Sofort ändern lassen!	
Benutzt es den MAC-Filter?	Jeder Computer (genauer die Netzwerkkarte) hat eine Kennung aus 12 Zahlen oder Buchstaben. Diese ist eindeutig und man kann ein Funknetz so einrichten, dass nur die bekannten Kennungen (die man vorher eingeben muss) hineindürfen.	

2. Klärt danach offene Fragen und erstellt schriftlich eine Checkliste auf der Rückseite des Arbeitsblattes, was ihr beachten müsst, wenn ihr in ein Funknetz geht.

3. Lies die Tipps sorgfältig. Arbeite mit einem Partner zusammen und erstelle dir einen kleinen Merkzettel mit Symbolen, der die genaue Größe deines Handys haben sollte!

- *WLAN immer ausschalten, wenn es nicht benötigt wird (spart auch Akku)*
- *Unterwegs kein Onlinebanking, Onlineshopping und auch kein facebook über das fremde WLAN!*
- *Datei- und Verzeichnisfreigabe in den Geräten deaktivieren*
- *Automatische Anmeldung an bekannten Hotspots deaktivieren! Hier gibt es böse Menschen, die öffentliche WLANs mit gleichem Namen vortäuschen, in Wahrheit aber Daten stehlen!*

5_2 PC-Sicherheit – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▷●	**AB 2** ▷▷
Titel	**Und in 1000 Jahren?**	**Daten für die Ewigkeit**
Kompetenzen	Die Schülerinnen und Schüler übertragen den Beginn einer Fantasiegeschichte über die Speicherung von Daten auf eine eigene Fortführung der Geschichte.	Die Schülerinnen und Schüler vergleichen die Speichermöglichkeiten ausgewählter Medien und übertragen die Kenntnisse in eine grafische Übersicht.
Methoden	Schreibwerkstatt (versch. Möglichkeiten: Cluster, Fließband-Geschichte, Demokratie, Zeitung), Gruppenarbeit, Textanalyse	Tabelle, Internet-Recherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	Ja

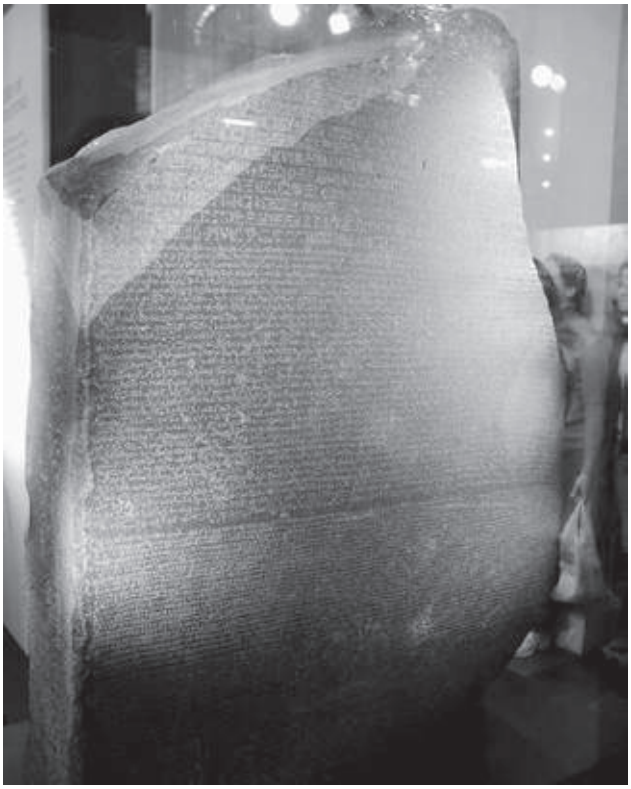
Hinweise für die Durchführung

AB 1: Und in 1000 Jahren?	Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler kreativ mit dem Problem der Datensicherung auseinandersetzen. Den Aufhänger bietet der „Stein von Rosetta" (siehe Informationen auf dem Arbeitsblatt), mit dessen Hilfe die ägyptischen Hieroglyphen übersetzt werden konnten. Die Schülerinnen und Schüler sollen eine Science-Fiction-Geschichte weitererzählen, wenn jemand in 2000 Jahren eine CD von heute findet. Die Methode der „Schreibwerkstatt" soll ein strukturiertes Arbeiten ermöglichen. So ist das „Clustern" eine eher kreativ-chaotische Methode, die sehr viel Spaß macht. Weitaus anstrengender, aber nicht weniger lustig, ist die „Fließband-Geschichte", da dort immer wieder auf die Fortführungen der anderen Gruppenmitglieder reagiert werden muss. In sehr gut funktionierenden Gruppen eignet sich die Form „Demokratie", wo jeder etwas schreibt und gemeinsam entschieden wird. Etwas stringenter ist „Zeitung", da dort die Form einer Zeitungsmeldung eingehalten werden muss. Vielleicht lassen Sie die Gruppen selbst entscheiden, welche Form sie wählen.
AB 2: Daten für die Ewigkeit	Auf der „Sound of Earth" ist folgendes gespeichert: „Der Anfang der Datenspur enthält 115 analog gespeicherte Bilder. Der Rest besteht aus Audiodaten. Dazu gehören gesprochene Grüße in 55 verschiedenen Sprachen (deutscher Text: „Herzliche Grüße an alle") sowie verschiedene Töne wie Wind, Donner und Tiergeräusche. Darauf folgen 90 Minuten ausgewählter Musik, neben ethnischer Musik auch bekannte Titel von Johann Sebastian Bach, Wolfgang Amadeus Mozart, Chuck Berry (mit dem Titel Johnny B. Goode) und anderen. Zusätzlich zu den Grüßen in verschiedenen Sprachen befindet sich neben einer geschriebenen Nachricht des U. N. Generalsekretärs Kurt Waldheim auch noch eine von US-Präsident Jimmy Carter: „This is a present from a small, distant world, a token of our sounds, our science, our images, our music, our thoughts and our feelings. We are attempting to survive our time so we may live into yours." („Dies ist ein Geschenk einer kleinen, weit entfernten Welt, Beispiele unserer Geräusche, unserer Wissenschaft, unserer Bilder, unserer Musik, unserer Gedanken und unserer Gefühle. Wir hoffen, unser Zeitalter zu überleben, so dass wir ihres erleben können.") (Quelle: ⓘ **http://de.wikipedia.org/wiki/Sounds_of_Earth**). Man darf gespannt sein, welche Erkenntnisse die Außerirdischen daraus ziehen.

Lust auf mehr?

- Das Thema Daten in der Cloud kann zusätzlich behandelt werden. Lassen Sie die Schüler hierzu recherchieren. Beispielsweise: „Was bedeutet Clouding?", „Welche Dienste bieten es an?", „Wo werden die Daten gespeichert?", „Wo liegen die Risiken?", „Wie können die Daten in einer Cloud zusätzlich geschützt werden?" etc.
- Auf einer ganz anderen Ebene ist die spannende Frage, was aus unserer digitalen Zeit als kulturelles Erbe übrig bleibt … oder – etwas praktischer – was würden wir heute auf eine „Sound of Earth"-CD spielen?

Und in 1000 Jahren?



Der Stein von Rosetta ist knapp 115 Zentimeter groß, wiegt aber über 750 Kilogramm. Er ist rund 2200 Jahre alt, steht im Britischen Museum in London, und noch immer kann man seine Inschrift lesen. Seine Erschaffer haben darin einen Text in drei Sprachen hinterlassen und mit seiner Hilfe konnte man die ägyptischen Hieroglyphen entziffern.

Quelle: ***http://upload.wikimedia.org/wikipedia/commons/8/89/Rosetta_stone.jpg***

Stelle dir das mal mit einer CD von heute vor!
Stelle dir vor, sie wird in 2000 Jahren gefunden!

Arbeitsauftrag:
Schreibe folgende Geschichte weiter!

Minux7 war ein Kind wie alle anderen, sein Computerchip im Kopf unterschied sich kein bisschen von denen seiner älteren Geschwister **Minux1** bis **Minux6** und seiner jüngeren, **Minux8** bis **Minux11**. Aber trotzdem war **Minux7** anders, er hatte diese Liebe zu allen Dingen, die alt waren. Und beim letzten Besuch der Erde war er doch aus der Überlebenskuppel herausgeschlichen und hatte in einem Bernsteinblock ein glänzendes rundes Ding von ungefähr 34 kyrometer (er wusste, das waren früher einmal 12 Zentimeter oder so ähnlich!) gefunden. Ganz undeutlich stand etwas darauf, aber das konnte er beim besten Willen nicht ohne seinen Sprachenchip „1000 Jahre und älter" entziffern. Zurück auf dem Mars wollte er das Rätsel lösen. …

Ihr dürft dazu eine **„Schreibwerkstatt"** durchführen. Findet euch in 4er-Gruppen zusammen und sucht euch eine der folgenden Formen aus:

A **Clustern.** Jeder schreibt spontan auf, was ihm dazu einfällt. Danach werden die Ideen sortiert und gemeinsam wird am Text weitergeschrieben

B **Fließband-Geschichte.** Einer beginnt mit einem Satz, der nächste schreibt weiter und so weiter

C **Demokratie.** Jeder schreibt den nächsten Satz der Geschichte, alle werden vorgelesen und danach wird gemeinsam ausgesucht, welcher am besten ist, dieser wird verwendet. Dann der nächste Satz…

D **Zeitung.** Ihr schreibt die Geschichte wie einen Zeitungsartikel.

Daten für die Ewigkeit?



1977 startete die NASA (die amerikanische Raumfahrtbehörde: National Aeronautics and Space Administration) eine Mission, die auf lange Dauer ausgerichtet war. Innerhalb von 16 Tagen startete sie die beiden Sonden Voyager 2 und Voyager 1 (in dieser Reihenfolge, weil die zweite eine andere Route hatte und schneller war). Der Start innerhalb von wenigen Tagen war kein Zufall – die Planeten standen günstig – um unser Sonnensystem zu erkunden. Am 15.8.2006 hatte Voyager 1 etwa 15 Milliarden km (oder 100 Astronomische Einheiten) zurückgelegt. Etwa 2017 wird die Sonde den interstellaren Raum erreichen.

An Bord beider Voyager-Sonden befindet sich eine Schallplatte aus Gold mit den „Sounds of Earth" (Klänge der Welt) mit Bildern und Tönen von der Erde und eine eingravierte Bedienungsanleitung. Diese Schallplatte hat eine geschätzte Lebensdauer von 500 Millionen Jahren.

„The Sounds of Earth Record Cover – GPN-2000-001978" von NASA/JPL ⓘ http://grin.hq.nasa.gov/ABSTRACTS/GPN-2000-001978.html. Lizenziert unter Gemeinfrei über Wikimedia Commons - ⓘ http://commons.wikimedia.org/wiki/File:The_Sounds_of_Earth_Record_Cover_-_GPN-2000-001978.jpg#/media/File:The_Sounds_of_Earth_Record_Cover_-_GPN-2000-001978.jpg

Arbeitsaufträge:

1. Informiere dich darüber, was auf der Schallplatte der Voyager gespeichert ist! Überlege, warum die Menschen dies Außerirdischen mitteilen wollten! (Spezialaufgabe: hättest du es genau so gemacht?)

Hier findest du durchschnittliche Haltbarkeitsdauer verschiedener Datenträger:

■ 5–10 Jahre	Informationen auf Magnetbändern, Magnetplatten, Disketten
■ 20–50 Jahre	Magneto-Optical Disks, WORM, CD-ROM, CD-R
■ 30 Jahre	Recycling-Papier
■ * Jahre	* Wie lange ein USB-Stick haltbar ist, hängt von der Benutzung ab!
■ 50 Jahre	Blu-Ray-Discs
■ 100 Jahre	Chromogene Farbfilme, Diazo- und Vesicular-Mikrofilme
■ 100 Jahre	Holzschliffhaltiges, säurehaltiges Papier
■ 250 Jahre	Chromogene Farbfilme, gekühlt
■ 300 Jahre	Silberhalogenid-Mikrofilme auf Acetat-Basis
■ 400 Jahre	Farbfilme im Farbbleichverfahren (Iifochcrome Micrographic)
■ Mehrere Hundert Jahre	säure- und ligninfreies, gepuffertes „alterungsbeständiges" Papier
■ 1000 Jahre	Pergamente, Papyri, Tontafeln

Quelle: „Archive und ihre kulturelle Überlieferung – Digitale Archive", Prof. Christian Wolff Universität Regensburg

2. Wie lange etwas haltbar ist, ist sehr unterschiedlich. Übertrage die Liste mit den Haltbarkeitsdauern in ein Säulendiagramm (Du kannst auch MS Excel oder OpenOffice.calc dazu nutzen)! Wie sollte man wichtige Daten speichern?

3. Jetzt wird es noch mal schwierig: Was kannst du tun, wenn du eine CD mit Urlaubsfotos noch deinen Enkeln zeigen möchtest? Diskutiert verschiedene Möglichkeiten in der Klasse und haltet die Ergebnisse auf der Tafel fest!

5_2 PC-Sicherheit – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Spam-Mails – wie schützt du dich?**	**Ein ganzer Zoo im Computer und auf dem Handy?**
Kompetenzen	Die Schülerinnen und Schüler erarbeiten die Möglichkeiten zum Schutz vor unerwünschten E-Mails (sogenannten Spam-Mails).	Die Schülerinnen und Schüler lernen verschiedene Formen von Schadsoftware kennen und können eine Übersicht anfertigen.
Methoden	Einzelarbeit, Partnerarbeit, Unterrichtsgespräch, Ergänzungs-Übung	Partnerinterview, Plakat, Experte (optional), Partnerarbeit, Einzelarbeit
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja (nur für das Video von Monty Python notwendig)	ja

Hinweise für die Durchführung

AB 1: Spam-Mails – wie schützt du dich?

Anhand dieses Arbeitsblattes sollen die Schülerinnen und Schüler die drei „goldenen" Regeln des E-Mailing kennen lernen und begründen können. Die Form des E-Mailing kann dabei gewählt werden, wenn die Möglichkeiten dazu bestehen, ansonsten lassen Sie die Begründung vielleicht einfach als zusammenhängenden Text schreiben.

Die Ergänzungen zu den Sätzen soll eine kleine Wissensabfrage zum E-Mailing sein, denn oft beherrschen Schülerinnen und Schüler das E-Mailing, wissen aber nichts mit CC oder BCC o. ä. anzufangen:

Mögliche Antworten:

- Der Betreff einer E-Mail ist wichtig, weil … der Empfänger daran sofort sehen kann, ob es eine Spam-Mail ist oder nicht, auch ohne sie zu öffnen.
- Wenn ich mehrere Empfänger habe, mache ich Folgendes … Ich schreibe sie in die Empfängerzeile, getrennt durch ein Komma (Dies kann von Programm zu Programm variieren).
- Das BCC beim E-Mailing steht für … Blind Carbon Copy, also eine „blinde" Kopie. Die anderen Empfänger der E-Mail können diesen BCC-Empfänger nicht sehen.
- Anhänge öffne ich nur von ... Bekannten oder Freunden oder wenn ich weiß, von wem er stammt.
- Große Dateien über 10 MB verschicke ich nur, wenn … es unbedingt notwendig ist und ich beim Empfänger nachgefragt habe.
- Ich habe zwei E-Mail-Adressen, weil … ich eine private benutze für meine Freunde und Bekannten.
- Eine andere gebe ich öffentlich weiter. Die privaten E-Mail-Adressen bekommen nur … meine Freunde und Bekannten.
- Das mache ich mit blöden E-Mails … Ich lösche sie sofort oder ich markiere sie als SPAM.
- E-Mails von Unbekannten behandele ich so: Ich öffne nie Anhänge und bin vorsichtig mit dem Inhalt. Wenn mir etwas komisch vorkommt, lösche ich sie. Vor allem antworte ich nicht ohne weiteres.
- Auch in E-Mails bin ich höflich, weil … auf der anderen Seite keine Maschinen, sondern Menschen sitzen.

AB 2: Ein ganzer Zoo im Computer und auf dem Handy?

Die Auflistung möglicher Schädlinge für digitale Geräte ist didaktisch reduziert (s. Sachinformationen), bietet aber einen guten Einstieg in das Thema. Die Schülerinnen und Schüler sollen im ersten Arbeitsauftrag eine eigenständige Recherche auf den Seiten von klicksafe und dem Bundesamt für Sicherheit in der Informationstechnik – das sie auf diese Weise kennenlernen – vornehmen. Hier ist vielleicht etwas Hilfestellung und Vorarbeit notwendig, da diese Seiten sehr umfangreich sind und immer wieder aktualisiert werden.
Im zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler nach der Informationsbeschaffung ihren Partner/ihre Partnerin informieren. Dies kann in Form eines „Partnerinterviews" geschehen: Als Synthese soll dann eine Seite mit den wichtigsten Informationen entstehen. Vielleicht besteht die Möglichkeit, auch andere Klassen über das Problem in Form eines Stationenlernens zu informieren.

Spam-Mails – wie schützt du dich?

„Spam-Mails sind eine wahre Plage, oder? Bestimmt hast du auch schon solche unerwünschten E-Mails bekommen. Der Name stammt wahrscheinlich von „SPiced hAM" (englisch für „gewürzter Schinken") was früher der Name eines Dosenfleischs war. Als Begriff für „massenhaft" und „unerwünscht" soll das Wort aus einem alten Fernsehsketch der Komikergruppe „Monty Python" stammen.
Du kannst dir den Spot hier anschauen: **http://bit.ly/19PeUMn**

Spam-Mails sind nicht nur lästig, sondern können auch gefährlich werden. Deshalb gibt es drei goldene Regeln des E-Mailing:

- niemals auf eine Spam-Mail reagieren
- den Spam-Filter „trainieren"
- die E-Mail-Adresse nicht überall angeben und immer eine zweite E-Mail-Adresse anlegen

Arbeitsaufträge:

1. Überlege, warum diese Regeln sinnvoll sind! Schreibe eine E-Mail an eine Freundin/einen Freund, in der du ihr/ihm diese Regeln erklärst. Wenn du keine Möglichkeit hast eine E-Mail zu schreiben, schreibe die Erklärung auf die Rückseite des Arbeitsblattes!

2. Aber es gibt noch weitere wichtige Dinge, die man beachten sollte. Hier findest du Hinweise, ergänze sie zu ganzen Sätzen:

Der Betreff einer E-Mail ist wichtig, weil …
Wenn ich mehrere Empfänger habe, mache ich folgendes …
Das BCC beim E-Mailing steht für …
Anhänge öffne ich nur von …
Große Dateien über 10 MB verschicke ich nur, wenn …
Ich habe zwei E-Mail-Adressen, weil …
Die privaten E-Mail-Adressen bekommen nur …
Das mache ich mit blöden E-Mails …
E-Mails von Unbekannten behandele ich so:
Auch in E-Mails bin ich höflich, weil …

5_3 Passwörter – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Informationelle Selbstbestimmung – was ist das denn?**	**Sichere Passwörter – wie geht das?**
Kompetenzen	Die Schülerinnen und Schüler wählen aus Beispielen aus, welche Daten aus Sicht einer „informationellen Selbstbestimmung" schützenswert und welche unproblematisch zu veröffentlichen sind.	Die Schülerinnen und Schüler beurteilen ein System zur Erstellung sicherer Passwörter und setzen es mit einem eigenen Beispiel um.
Methoden	Stichwortliste, Plakat, Einzelarbeit, Unterrichtsgespräch	Passwortsystem erfinden, Passwort-Check, Einzelarbeit, Unterrichtsgespräch.
Material	Arbeitsblatt, großes Papier, bunte Stifte	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	ja

Hinweise für die Durchführung

AB 1: Informationelle Selbstbestimmung – was ist das denn?

Der Hinweis auf „informationelle Selbstbestimmung" dient als Einstieg und könnte vielleicht später noch vertieft werden (s. „Lust auf mehr"). Die Schülerinnen und Schüler sollen hier verschiedene Stichwörter zu persönlichen Angaben ausschneiden und bewerten. Dazu kleben Sie die Stichwörter auf, je weiter links desto problematischer wäre eine Angabe, je weiter rechts desto problemloser. Dabei gibt es sicherlich Dinge, die man nie ohne Weiteres weitergeben sollte (z. B. Handynummer) und die Dinge, die von Fall zu Fall weder hochproblematisch noch ungefährlich sind (z. B. Postleitzahl) sowie Fakten, die ohne Personenbezug unwichtig sind (z. B. Schuhgröße). Hier könnten Sie weitere Beispiele einfügen, die von den Schülerinnen und Schüler genannt werden.

Der zweite Arbeitsauftrag ist je nach Altersstufe nicht ganz einfach zu beantworten, denn die Interessen hinter der Datensammelwut sind für Schülerinnen und Schüler nicht immer einsichtig. Hier hilft der Hinweis auf die kommerziellen Interessen, z. B. für gezielte Werbung. Zum Schluss soll das Wichtigste in Form eines Plakats festgehalten werden.

AB 2: Sichere Passwörter – wie geht das?

Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler dem Thema Passwortschutz spielerisch über den Einstieg „Geheimsprache" nähern, der hier mit einer Nummerierung des Alphabets gemacht ist.
Schreiben Sie das Beispiel an die Tafel und die Lösung / den „Schlüssel" auf eine zugeklappte Seite. **Hier ist ein Beispiel für eine Geheimsprache:**

160119192315051820051814090513011219 2205181801200514

Und die dazugehörige Lösung, also der „Schlüssel": **a01 b02 c03 d04 e05 f06 g07 h08 i09 j10 k11 l12 m13 n14 o15 p16 q17 r18 s19 t20 u21 v22 w23 x24 y25 z26**

Lösung: Passwörter niemals verraten



Tipp:
Immer 2 Zahlen zusammen nehmen und den Buchstaben davor wählen
(Bsp: 16 = p; 01= a)

Ihre Schülerinnen und Schüler erfinden sicherlich eine schwierigere Geheimsprache (s. Arbeitsauftrag). Die Tipps für gute Passwörter können auch die jüngeren Schülerinnen und Schüler nachvollziehen, vielleicht sollten Sie die einzelnen Punkte verdeutlichen. Der letzte Punkt dient der Überprüfung, wobei selbstverständlich das Ziel sein sollte, dass niemand das Passwort „knacken" kann. Hier ist der Spagat wichtig zwischen der Notwendigkeit, sich Passwörter gut merken zu können und ihrem Schutz.

5_3 Passwörter – Arbeitsblätter
methodisch-didaktische Hinweise

Erfahrungsgemäß brauchen die Schülerinnen und Schüler ein wenig Unterstützung bei der „Geheimsprache" des folgenden Arbeitsauftrages. Hier sollen sie für sich ein System entwickeln, mit dem die Wörter gut zu merken sind. Das Beispiel auf dem Arbeitsblatt kann als Modell für die Erstellung und Memorierung von Passwörtern dienen. Danach können sie sehr schnell einsehen, dass man mit diesem System viele verschiedene, gute Passwörter erstellen kann, denn man braucht nur den Ausgangsnamen verändern (eigener Name, Name der Mutter, des Vaters, der Haustiere etc.). In diesem Fall ist auch eine kleine Notiz „Hund" nicht schlimm, denn niemand kennt das System.

Lösung:

Merken	**Passwort**	**Beschreibung**
Mein Hund heißt:	Naischa	Leicht zu merken.
Alle Vokale in Großschreibung:	nAIschA	Die Selbstlaute sind groß geschrieben, alles andere klein.
Meine Telefonnummer lautet 765499; immer abwechselnd ein Buchstabe und ein Zahl:	N7A6I5s4c9h9A	Die Telefonnummer ist eingebaut.
Das Ganze immer in Klammern, damit der Hund nicht wegläuft:	(N7A6I5s4c9h9A)	Es wurden Klammern gesetzt.

Mit der Adresse **https://checkdeinpasswort.de** steht ein Tool zur Verfügung, sein Passwort zu testen. Dabei sollte den Schülerinnen und Schülern klar gemacht werden, dass man nie sein tatsächliches Passwort dort eingibt, denn trotz der Seriosität dieses Anbieters sollte man im Internet nie auf einer unbekannten Webseite sein richtiges Passwort eingeben.

Lust auf mehr?

- Im Zusatzmodul „Ethik macht klick – Werte-Navi fürs digitale Leben" finden sich weitere Materialien zum Thema unter Baustein 1 Projekt 6 „Aktiv werden":
  http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf
- Das Recht auf informationelle Selbstbestimmung könnte ein schöner Aufhänger zu einer Fortführung des Themas sein. Dabei sind sowohl historische Fragen interessant – erinnert sei an das „Volkszählungsurteil" des Bundesverfassungsgerichts, in dem erstmals dieses Recht fixiert wurde – als auch ganz aktuelle. Die Datensammelwut lässt heutzutage eine fast lückenlose „Beobachtung" zu, siehe Kapitel 8_3 „Digitaler Fußabdruck".
- Hacker versuchen ständig Passwörter zu knacken. Sie gehen dabei ausgesprochen listig vor. Die Schüler können sich über folgende Methoden informieren:
  Programmierbare Tastatur auf einem USB-Stick, „Rainbow"-Tabellen, Passwortlisten aus Wörterbüchern, Passwortlisten aus gestohlenen Passwortlisten, Software-Manipulationen, Vor- und Nachnamen ausprobieren, Kombinationen mit dem Namen des Angebots (z. B. youtube123), Ersatz von Buchstaben mit ähnlichen Ziffern (z. B. N3isch3).

Informationelle Selbstbestimmung – was ist das denn?



*Du hast das Recht auf **„informationelle Selbstbestimmung"**. Dieses Recht sagt: Du hast das Recht zu wissen, wer was wann über dich weiß. Normalerweise ist das kein Problem, denn natürlich muss deine Schule dein Geburtsdatum, deinen Namen und deine Adresse wissen und auch im Sportverein musst du all dies angeben. Aber muss deine Schule auch wissen, welche Haustiere du hast oder dass dein Lieblingsverein der FC Schalke 04 ist?*

Im Internet ist die Sache noch schlimmer! Bei vielen Internetseiten musst du dich anmelden und wirst alles Mögliche gefragt.

Arbeitsaufträge:

1. Überlege genau, welche persönlichen Dinge du problemlos von dir weitergeben kannst. Unten findest du eine Stichwortliste. Bei welchen Dingen musst du unbedingt deine Eltern fragen? Schneide die Stichworte aus und sortiere sie entlang dieser Linie (je weiter links, desto problematischer, je weiter rechts, desto weniger problematisch ist eine Angabe).

Immer Eltern fragen					**kein Problem**

Name	Geburts-datum	Spitzname	Alter	Wohnort	Straße
Postleitzahl	Handy-nummer	Telefon-nummer	Größe	Name der Mutter	Name des Vaters
Schuhgröße	Einkommen der Eltern	Geschwister-zahl	Vorname	Taschengeld-höhe	Name des Freundes
Foto von dir	Lieblings-tier	Lieblings-essen	Lieblings-Sportverein	Haustiere	Haarfarbe

2. Diskutiert gemeinsam im Klassenverband darüber, warum die Menschen, die diese Internetseiten machen, all das wissen wollen.

3. Überlegt auch, wie ihr euch das nächste Mal bei einer solchen Anmeldung verhalten könnt! Ihr findet sicherlich gute Tipps! Fasst diese auf einem Plakat zusammen!

Sichere Passwörter – wie geht das? (1/2)

„Statt vom Computerzeitalter sollte man lieber vom Passwortzeitalter sprechen", stöhnt Jasmin beim Abrufen ihrer E-Mails. „Ich verwende immer das gleiche: Nicolo – so heißt mein Meerschweinchen und das vergesse ich niemals". „Danke für die Information", antwortet ihr jüngerer Bruder, „Ich habe mir ein todsicheres System ausgedacht". „Lass mal hören!" … „Liebste Schwester – dann wäre es kein todsicheres System mehr!"

Gute Passwörter erfüllen folgende Bedingungen:

- *Gute Passwörter sind mindestens 12 Zeichen lang!*
- *Gute Passwörter enthalten sowohl Klein- und Großbuchstaben als auch Zahlen!*
- *Gute Passwörter enthalten Sonderzeichen (-+.,;:_#/*%&?$\{\}[]()!*
- *Gute Passwörter bestehen nicht aus echten Wörtern oder Namen!*
- *Gute Passwörter sind trotzdem gut zu merken!*

Erfinden wir doch einfach eine Geheimsprache:

Die Kunst der Geheimsprache wird seit Jahrtausenden gepflegt.
Früher war sie nur für Könige und Generäle interessant,
aber im Computerzeitalter brauchen wir alle eine Geheimsprache.
Wir brauchen sie für die vielen Passwörter.
Übrigens … Kennwörter ist nur ein anderer Name für Passwörter!

Arbeitsaufträge:

1. Erfinde eine eigene Geheimsprache, in der auch Zahlen vorkommen können.
2. Zeige sie deiner Nachbarin/deinem Nachbarn und lasse sie „entschlüsseln"!

Sichere Passwörter – wie geht das? (2/2)

Und wie soll man sich so etwas merken? Wie kann man sich **IwidB_65uhJ** merken?
Das funktioniert am besten über ein System, hier ist ein Satz abgekürzt:
„Ich wohne in der Bunsengasse _65 und heiße Jan".

Wie funktioniert folgendes System? Findest du es heraus?

Merken	Passwort	Beschreibung der Veränderung
Mein Hund heißt:	Naischa	
?	nAIschA	
Meine Telefonnummer lautet 765499	N7A6I5s4c9h9A	
?	(N7A6I5s4c9h9A)	

3. Beschreibe das System oben! Probiere es mit zwei anderen Wörtern aus (zum Beispiel mit deinem eigenen Namen oder deinem Haustier)!

4. Erfinde ein eigenes System, wie du gute Passwörter machst und sie dir trotzdem merken kannst! Dann kannst du auch ein Stichwort notieren (oben dürfte man „Hund" notieren, oder?)

5. Ausnahmsweise darfst du dein System NICHT mit den anderen austauschen! Denke an Jasmin und ihren jüngeren Bruder!

Teste es im Internet unter: **www.checkdeinpasswort.de**

Denke daran, dass du nicht dein echtes Passwort verwendest!

Ein ganzer Zoo im Computer und auf dem Handy?

Ein wenig digitale Biologie?
Auf unserem Computer, Smartphone oder Tablet können sich zahllose Schädlinge tummeln.

Computerviren
Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

Rogueware
Rogueware ist besonders perfide: Diese Software gaukelt vor, andere Schadsoftware zu entfernen, tut aber das Gegenteil.

SpyApps
SpyApps zeichnen unbemerkt die Kommunikation auf, schalten Mikrofon und Kamera ein oder leiten den Standort des Handys weiter.

Scareware werden gefälschte Warnmeldungen u. ä. bezeichnet, die den Nutzer verunsichern und dazu verleiten sollen, andere Software zu installieren.

„Würmer"
Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.

„Trojaner" – Trojanische Pferde
(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

Hoaxes
Ein Hoax (zu Deutsch: „Jux", „Schabernack" oder „Schwindel") ist nichts anderes als eine Falschmeldung, die von Person zu Person verbreitet wird (z. B. via SMS, WhatsApp- oder Facebook-Nachricht). Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer und in dein Handy? Und wie kannst du dich davor schützen?

Arbeitsaufträge:

1. Informiere dich über das Problem auf den folgenden Seiten:

klicksafe: **www.klicksafe.de/themen/technische-schutzmassnahmen/den-pc-schuetzen/**
Bundesamt für Sicherheit in der Informationstechnik: **https://www.bsi-fuer-buerger.de/**

2. Wie sieht ein wirksamer Schutz aus? Erkläre es deiner Nachbarin/deinem Nachbarn und umgekehrt!

3. Erstelle eine Übersicht mit den wichtigsten Informationen über Viren und den Schutzmaßnahmen! Versuche doch bitte, Symbole und Bilder in deine Übersicht einzubringen.
Erstelle in einem Textbearbeitungsprogramm ein Merkblatt mit Symbolen!



Cybertreffen, Sexting und Selfie

6

6|1 Cybertreffen

6|2 Sexting

6|3 Selfie

Übersicht der Bausteine:

- **Cybertreffen** | **Arbeitsblätter**
- **Sexting** | **Arbeitsblätter**
- **Selfie** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Ethik macht klick – Werte-Navi fürs digitale Leben
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf



Selfie, Sexting und Selbstdarstellung
https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/Selfies_Sexting_Selbstdarstellung_Mobile_Medien_3.pdf



Let's talk about Porno! Jugendsexualität, Internet und Pornographie
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Porno/LH_Zusatzmodul_Porno_klicksafe_gesamt.pdf



Cybertreffen, Sexting und Selfie



6_1 Cybertreffen – Arbeitsblätter methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**„Wer ist wer? Ein Spiel zum Nicht-Kennenlernen!"**	**Freunde**
Kompetenzen	Die Schülerinnen und Schüler hinterfragen „Profile" im Internet.	Die Schülerinnen und Schüler erörtern den Begriff Freundschaft und differenzieren zwischen „Freunden", „Kumpels" und „Bekannten" anhand von Fallbeispielen.
Methoden	Spiel, Partnerarbeit, Plenum	Placemat, Fallbeispiele, Kleingruppen, Plenum
Material	Arbeitsblatt (mit Fotos), Schere, Kleber, leere Blätter	Arbeitsblatt, großes Papier
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	nein

Hinweise für die Durchführung

AB 1: „Wer ist wer? Ein Spiel zum Nicht-Kennen-lernen!"

Das Arbeitsblatt soll spielerisch hinführen zur Problematik der Virtualität und Realität. Die Fotos der Tiere sind so gewählt, dass bestimmte Assoziationen, bspw. aus Fabeln, möglich sind wie Löwe=stark oder Esel=stur o.ä. Dies sind selbstverständlich keine Wahrheiten, können aber im Spiel genau dazu benutzt werden, sich zu verstecken oder darzustellen. Die anschließende Diskussion dient der eigentlichen Reflexion und Übertragung auf die Realität. So sollen die Schülerinnen und Schüler erkennen, dass die Profile in den meisten Anwendungen wie WhatsApp oder Facebook etc. von den Usern selbst erstellt sind und genauso fantasievoll sein können wie die Profile des Spiels. Der Merksatz an der Tafel könnte lauten: „Jedes Profil ist selbst erstellt und muss nicht wahr sein!" o. ä.

AB 2: Freunde

Die Schülerinnen und Schüler sollen darüber nachdenken können, was ein Freund/eine Freundin ist und anschließend diese – eigene – Definition an Beispielen anwenden.
Der Einstieg erfolgt am Beispiel der üblichen Social Communities, die die Schülerinnen und Schüler leicht nachvollziehen können. Daran knüpft die Frage an, was ein Freund/eine Freundin überhaupt ist. Mithilfe der Methode „Placemat" (s. u.) sollen sie in Kleingruppen eine Definition erarbeiten. Diese kann je nach Gruppe ganz unterschiedlich sein. Es bietet sich an, hier einen ausführlichen Austausch nach der Gruppenphase zu ermöglichen.
Mit der Unterscheidung von „echten Freunden", „Kumpels" und „Bekannte" soll versucht werden, die drei Kategorien „echte Freunde", „kenne ich persönlich" und „kenne ich nicht persönlich" zu definieren. Die Schülerinnen und Schüler sollen in der Tabelle die Beispiele diskutieren (vielleicht kommen sie zu einer anderen Einschätzung, s.u.) und eigene Beispiele finden. Es bietet sich an, einige an die Tafel zu schreiben und zu besprechen. Die Bearbeitung der Tabelle ist sicherlich individuell, aber vielleicht dient dies der Orientierung:

Das würde ich mit ihnen tun / ihnen erzählen:	Mit echten Freunden: „Freunde"	Mit anderen, die ich persönlich kenne: „Kumpels"	Mit Menschen, die ich nur aus dem Internet kenne: „Bekannte"
A. Meine heimliche Liebe verraten	Ja	Nein	Nein
B. Über den Streit mit meinen Eltern berichten	Ja	Vielleicht	Nein
C. Ins Kino gehen	Ja	Ja	Nein
D. Einen Blick in das Tagebuch werfen lassen	Nein	Nein	Nein
E. Meinen Spitznamen verraten	Ja	Ja	Vielleicht

Lust auf mehr?
Lassen Sie die Schülerinnen und Schüler mit einem Avatar-Creator wie bspw. der App Bitstrips oder dem South Park Creator Studio (ⓘ **www.sp-studio.de/**) Comic-Avatare von sich erstellen. Spannend ist hier ein Vergleich: Wie ähnlich sind sie den Schülerinnen und Schülern?
Die Avatare können auch als Profilbild in den Sozialen Netzwerken weiter verwendet werden.

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (1/3)

Im Netz trifft man schon manchmal komische Typen … willi123 und susi17 sind dabei wohl eher normale Spitznamen, die im Internet „Nicknames" heißen. Es ist so einfach eine fremde Identität anzunehmen und in eine Rolle zu schlüpfen. Umso schwerer ist es, diese zu entlarven und man kann sich nie ganz sicher sein, wer wer ist. Wie es zugehen kann, das dürft ihr in einem kleinen Spiel erfahren.

Ziel des Spiels:
Finde heraus, wer sich hinter dem Steckbrief verbirgt!

Tipp:
Alle dürfen lügen, aber vielleicht kann man aus diesen Lügen auch etwas über die Person erfahren!

Spielregeln:
Jeder darf ein Profil erstellen und in drei Runden ergänzen.

1. Runde: Suche dir ein Foto eines Tieres aus, das du auf deinen Steckbrief klebst.
Erfinde dir dazu einen Nickname, den du gut lesbar dort einträgst.

Mischt die Profile heimlich und legt sie alle aus.
Jeder darf nun raten (bitte den Tipp auf dem unteren Feld eintragen),
wer sich hinter den Steckbriefen verbirgt.
Diejenigen, deren Profil erraten wurde, scheiden aus.

2. Runde: Ergänze deinen Steckbrief um die Beschreibung deines Aussehens und deiner Körper-Merkmale.
Selbstverständlich darfst du flunkern!

Wie oben … mischen und erraten!

3. Runde: Ergänze deinen Steckbrief um deine Hobbys und Vorlieben.

Wie oben… mischen und erraten!

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (2/3)

Das Profil

Foto	
Dein Nickname:	
Dein Aussehen:	
Deine Hobbys/ Vorlieben:	
Hinter diesem Profil versteckt sich:	

Arbeitsaufträge:

1. Spielt das Spiel!
2. Wertet anschließend das Ergebnis aus!
   War es schwer, ein Profil einer Mitschülerin / einem Mitschüler zuzuordnen?
   Woran habt ihr sie / ihn erkannt?
   Wann war es unmöglich?
3. Übertragt die Beispiele auf das Internet.
   Diskutiert in der Klasse die Frage, wie man mit (fremden) Profilen umgehen sollte!
4. Formuliert dazu einen Merksatz an der Tafel.

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (3/3)



Quellen:

1. *Schmetterling: M. Großmann / pixelio.de*
2. *Specht: uschi dreiucker / pixelio.de*
3. *Kuh: Joujou / pixelio.de*
4. *Fliege: uschi dreiucker / pixelio.de*
5. *Pferd: Rainer Sturm / pixelio.de*
6. *Katze: berggeist007 / pixelio.de*
7. *Hund: uschi dreiucker / pixelio.de*
8. *Gans: Albedo / pixelio.de*
9. *Frosch: Sommaruga Fabio / pixelio.de*
10. *Löwin: Dieter Schütz / pixelio.de*
11. *Trampeltier: Klaus Mackenbach / pixelio.de*
12. *Esel: Lisa Schwarz / pixelio.de*
13. *Ziege: Ruth Rudolph / pixelio.de*
14. *Adler: Willi Haimerl / pixelio.de*
15. *Wolf: saskia wend / pixelio.de*
16. *Lamm: daniel stricker / pixelio.de*



6_2 Sexting – Arbeitsblätter
methodisch-didaktische Hinweise

Beschreibung zu Projekt 2: „Show yourself!“

Kompetenzen	**Die SuS können Folgen aufreizender Selbstdarstellung in Sozialen Medien erkennen.**
Zeit	45 Minuten
Methoden	Fallbeispiele
Material	Einstieg Screenshots, Fallbeispiele ausdrucken
Zugang Internet/PC	Nein
Einstieg	Zeigen Sie die Bilder 1–3. Bild 1 steht für mediale Aufmerksamkeit („Show yourself“), Bild 2 steht für politische Aufmerksamkeit („Sextremismus“) und Bild 3 für digitale Aufmerksamkeit („Likes“).



Bild 1: Show yourself
Klum-Werbung für Germany's Next Topmodel 2014
Quelle: klicksafe



Bild 2: Femen
By Joseph Paris (Own work) [FAL], via Wikimedia Commons
Quelle: Wikipedia, Stand: 5.3.2014

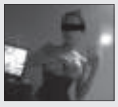


Bild 3: Sexy Selfie
Gruppe Facebookschlampen
Quelle: www.facebook.com, Stand: 13.11.2013

Die Bilder stehen zum Download auf ⓘ **www.klicksafe.de/medienethik** zur Verfügung.

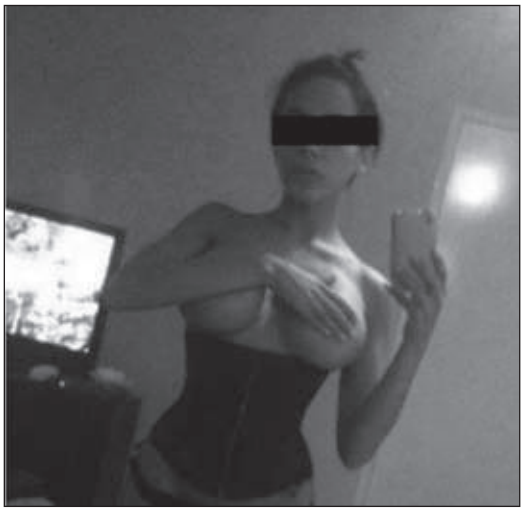
Fragen Sie die SuS nach ihrer Einschätzung zu den drei Darstellungen, z. B.: Wie wirken diese Darstellungen auf euch? Was wollen die Darsteller erreichen? Wie schätzt ihr die Folgen für die Abgebildeten ein? Wie könnten Bild 1 und 3 zusammen hängen?
Alternative: Zeigen Sie den Spot: „Ein Selfie wird zum Alptraum“ ⓘ **http://bit.ly/1uvXdNu** und fragen Sie die SuS nach weiteren Beispielen für aufreizende Selbstdarstellung mit Folgen. Dabei sollen keine Personen namentlich genannt werden.

Erarbeitung	Teilen Sie die Vorlage mit den Fallbeispielen und das Arbeitsblatt zu Projekt 2 an alle SuS aus. Die SuS teilen sich in mindestens 3 Gruppen und bearbeiten jeweils ein Fallbeispiel mithilfe des Arbeitsblattes. Das Fragezeichen in der Blattmitte ist ein Platzhalter für das jeweilige Fallbeispiel. Es kann auch ein eigenes Beispiel besprochen werden.
Sicherung	Die SuS präsentieren ihre Ergebnisse. Die Gruppen können sich gegenseitig ergänzen. Das Blatt mit Lösungsvorschlägen kann ausgeteilt werden. Folgende Themen sollten bei der Auswertung angesprochen werden: ***Victim blaming*** Jugendliche sprechen Opfern, die sich freizügig zeigen, häufig eine Mitschuld zu („Victim blaming“, dt. Opferbeschuldigung, oder auch „Täter-Opfer-Umkehr“). Das Gespräch über die Verantwortung der Beteiligten und die Folgen von Schuldzuweisungen ist wichtig, denn durch Zuweisung von Mitschuld wird häufig verhindert, dass Mitwisser Partei für das Opfer ergreifen. Durch die Fokussierung auf das Opfer wird die Verantwortung des Täters aus dem Blick verloren. Nicht zuletzt verhindert die Sorge des Opfers um ein vermeintlich eigenes Fehlverhalten sowie die Scham über die Onlineaktivitäten zu berichten, dass sich ein Opfer Hilfe sucht. ***Eine Frage des Vertrauens?*** Das Versenden vieler Bilder erfolgt im Vertrauen, welches missbraucht wird. Besprechen Sie hier: Was bedeutet es, jemandem zu vertrauen? Wodurch kann Vertrauen missbraucht werden? Wann ist besser Vorsicht geboten? ***Erotische Selfies von Jungen*** Diskutieren Sie auch über erotische Selfies von Jungen: Wie unterscheiden sie sich sich von denen der Mädchen? Haben Jungen die gleichen Konsequenzen zu erwarten wie Mädchen (Gibt es eine männliche Entsprechung zum „Schlampenimage“)? **Zusatzaufgabe/Hausaufgabe:** Die SuS formulieren mind. fünf Tipps, die sie jüngeren Mitschülern in Bezug auf erotische Selbstdarstellung geben würden. Es kann auch ein kurzer Informationsflyer entstehen.

Fallbeispiele

Fallbeispiel 1: Lisa hat ein aufreizendes Bild von sich auf der Facebook-Seite „Hot or Not“ gepostet.

Quelle: Screenshot facebook; URL: https://www.facebook.com, Seite FB Schlampen, Stand: 13.8.2013



Fallbeispiel 2: Doreen hat über Snapchat ihren besten Freundinnen ein Unterwäschebild von sich geschickt. Obwohl sich das Bild eigentlich von alleine löschen sollte, ist es in fremde Hände geraten und in einem Netzwerk gepostet worden. Nun wird sie durch Kommentare öffentlich gedemütigt.

Quelle: Screenshot facebook; URL: https://www.facebook.com, Seite FB Schlampen, Stand: 13.8.2013



Fallbeispiel 3: Ein Nacktbild von Luca macht über die WhatsApp-Klassengruppe in seiner Klasse die Runde. Seine Freundin hatte ihn dazu aufgefordert mit den Worten: Wenn du mich wirklich liebst, dann schick mir so ein Bild von dir!

Quelle: Screenshot facebook; URL: https://www.facebook.com, Stand: 13.8.2013



„Show yourself!“

Alternativen:

Motivation:

Was könnte man stattdessen machen?

Warum soll das Bild versendet oder gepostet werden?

Erste Hilfe:



Mache ich mich strafbar? Infos bei **www.klicksafe.de** oder **www.juuuport.de**

Wenn es schon passiert ist, was kann man jetzt tun?

Gesetz:

Welche Folgen kann das für einen Menschen haben?

Folgen:

Vorschläge zum Arbeitsblatt Projekt 2

Motivation:

- *Viele Likes bekommen*
- *Nette Kommentare bekommen*
- *Fame (berühmt sein)*
- *Dazu gehören*
- *Der Welt zeigen, wie man ist*
- *Langeweile*
- *Dem Schatz etwas Schönes schenken*

Alternativen:

- *Andere Formen des Ausdrucks wählen (nicht aufreizend, sondern ausdrucksstark)*
- *Wenn man es dennoch tun möchte: „Safer Sexting"*
- *Fotos so gestalten, dass man nicht zu erkennen ist*
- *Möglichst wenige Verbindungen zu dir: kein Sexting über Accounts, deren Kennung die eigene Handynummer ist, Dienste verwenden, bei denen auf Screenshots der eigene Nickname nicht zu sehen ist*

Was könnte man stattdessen machen?

Warum soll das Bild versendet oder gepostet werden?



Erste Hilfe:

- *Wenn jemand anderes das Bild gepostet hat: die Person direkt bitten, das Bild sofort zu löschen*
- *Löschen mit den technischen Mitteln des Dienstes*
- *Den Betreiber bitten, zu löschen*
- *Hilfe suchen (Freunde, Eltern, Nummer gegen Kummer, …)*
- *Polizei*

Wenn es schon passiert ist, was kann man jetzt tun?

Mache ich mich strafbar?

Gesetz:
Das darfst du nicht posten oder weiterleiten:

- *Bilder, auf denen andere ohne deren Zustimmung zu sehen sind*
- *Bilder, die andere ohne deren Zustimmung gemacht haben*
- *Bilder, die pornografisch sind (z. B. Geschlechtsteile zeigen oder deutliche Anmachposen) anderen Minderjährigen weitergeben*
- *Bilder, die im „höchstpersönlichen Lebensbereich" (Toilette, Umkleide) aufgenommen wurden*

Welche Folgen kann das für einen Menschen haben?

Folgen:

- *Große Öffentlichkeit: Rufschädigung („Schlampenimage"); vgl. „Revenge Porn"*
- *Unerwünschte Rückmeldung bis hin zu Shitstorm, Hasskommentaren*
- *Sexuelle Übergriffe im Netz (Cyber-Grooming, Cyber-Stalking) oder reale Übergriffe*
- *Erpressung*
- *Weiterverwendung in einem anderen Kontext (z. B. Fremdverwendung auf pornografischen Webseiten etc.)*



6_2 Sexting – Arbeitsblätter
methodisch-didaktische Hinweise

Beschreibung zu Projekt 10: Sexualisierte Selbstdarstellung

Thema	Unter dem Begriff „Sexting" versteht man das Verbreiten erotischen Bild- oder Filmmaterials des eigenen Körpers. Erotisches Material oder Nacktaufnahmen können natürlich auch ohne Wissen der abgelichteten Person von anderen verbreitet werden (Verstoß gegen das Recht am eigenen Bild oder § 201a StGB Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen). Viele Jugendliche gehen davon aus, dass sie selbst nicht in solche Situationen geraten, sondern dass es nur naive Personen treffen kann. Oft wird den Opfern deshalb auch eine Mitschuld an der Situation gegeben. Die Jugendlichen lernen hier, sexualisierte Selbstdarstellung präventiv kritisch zu reflektieren.
Zielgruppe	ab 14 Jahren
Organisationsform	Einzelarbeit, Gesamtgruppe, Gruppenarbeit
Zeit	45 Minuten
Vorbereitung	Vorbereitungen treffen zum Abspielen des Spots „Everyone knows your name" auf der Seite: **http://multivu.prnewswire.com/mnr/adcouncil/26474/**
Methodische Hinweise	Ablauf: **Aufgabe 1:** Die Jugendlichen schauen den Spot „Everyone knows your name" an. Hier wird ein Mädchen namens Sarah von (vielen) männlichen Personen erkannt und angesprochen. Das ist zum einen angenehm und schmeichelhaft („Der ist aber süß."), zum anderen erschreckt diese Tatsache („Welche Farbe hat deine Unterwäsche heute?"). Vermutlich hat Sarah freizügige Bilder von sich ins Netz gestellt. Auf dem Arbeitsmaterial sollen die Jugendlichen Reaktionen des Umfeldes auf Sarahs Selbstdarstellung formulieren. *Mögliche Auswertungsfragen:* ■ Wie kam es, dass diese Personen das Bild gesehen haben? ■ Unterscheidung zwischen den Begriffen „privat" und „öffentlich" ■ Welche Nachteile kann das Veröffentlichen von Bildern haben? ■ Werden Jungen hierbei mehr Freiheiten zugestanden als Mädchen? **Aufgabe 2:** Hier entscheiden die Jugendlichen, ob die Fotos eher als privat zu bewerten sind oder auch öffentlich im Internet genutzt werden können. *Lösung:* Am unproblematischsten sind die Bilder 1, 2 und 5. Die anderen drei Bilder sind sehr deutlich einem privaten Lebensbereich zuzuordnen und daher für eine breite Öffentlichkeit nicht geeignet. **Aufgabe 3:** Anhand der Fallbeispiele wird auch das Problem der Veröffentlichung durch Dritte thematisiert. Die Jugendlichen wählen in drei Gruppen jeweils einen der vorgestellten Fälle und versuchen, die Fragen auf dem Arbeitsmaterial für diese Situation zu beantworten. *Mögliche Lösungen:*

Was muss jetzt getan werden? Mit den Verursachern sprechen, sie bitten, das Material zu löschen. Dem Betreiber der Seite den Verstoß melden. Anzeige erstatten. Dem Opfer zur Seite stehen.	**Welcher Schaden entsteht?** Über die Person wird negativ geredet. Es könnte Konsequenzen für Bewerbungen, Arbeitsstellen usw. haben.	**Was sagen Recht und Gesetz?** **Fall 1** Verstoß gegen das Recht am eigenen Bild **Fall 2** Verstoß gegen § 201a (StGB) Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen und deren Weitergabe an Dritte **Fall 3** Solange sie das Bild nicht veröffentlicht, nicht strafbar
Wer ist MittäterIn? Jeder, der Bilder oder Filme, die andere bloßstellen können, weitergibt oder weiterzeigt.	**Wer hat Schuld?** Den Opfern solcher Vorfälle wird von Jugendlichen häufig eine Mitverantwortung unterstellt (Grimm 2010, Kapitel 23, S. 202).	**Wie kann man solche Vorfälle verhindern?** Private Dinge niemals ins Netz stellen. Andere nicht in privaten Situationen fotografieren oder filmen. Bilder oder Filme, die andere bloßstellen, nicht weitergeben, sondern löschen.

Zugang Internet / PC	ja

Projekt 10/1: Sexualisierte Selbstdarstellung

Aufgabe 1:
Seht euch den Spot „Everyone knows your name" an.
Sarah hat sehr private Bilder von sich ins Netz gestellt.
Überlegt, was folgende Personen dazu sagen werden.

Tina aus Sarahs Klasse, mit der sie seit Wochen Stress hat

Lehrerin



Chef (Ferienjob)

Mama

Sarahs Freund

Weißt du eigentlich, dass in Deutschland die Zustimmung der Erziehungsberechtigten notwendig ist, wenn ein Jugendlicher unter 16 Jahren ein Bild von sich veröffentlichen will? Es wird bei Jugendlichen aber davon ausgegangen, dass sie die Reife besitzen, die Konsequenzen ihres Handelns abwägen zu können und daher wird z.B. in sozialen Netzwerken nicht das Einverständnis der Eltern beim Hochladen eines Bildes gefordert.

Projekt 10/2: Sexualisierte Selbstdarstellung

Aufgabe 2:
Bist du reif genug? Entscheide: Welche der Bilder sind okay?

						
Okay?						
Begründe:						

Aufgabe 3:

Es kann auch passieren, dass andere ganz private Bilder oder Filme von euch öffentlich machen. Bearbeitet in drei Gruppen einen der genannten Fälle anhand folgender Fragen:

a. Was muss jetzt getan werden?
b. Welcher Schaden entsteht?
c. Was sagen Recht und Gesetz?
d. Wer ist Mittäterln?
e. Wer hat Schuld?
f. Wie kann man solche Vorfälle verhindern?

Fall 1:

Lena hatte vor ein paar Wochen mit ihrem Freund Schluss gemacht. Der ist total von der Rolle und stellt einen Film in ein Videoportal ein, der bei einem gemeinsamen Wochenende entstanden ist und Lena nackt zeigt.

Fall 2:

Michelle und Yasemin fotografieren Jana beim Umziehen in der Mädchenumkleide und verschicken die Bilder per Handy. Bald sind sie an der ganzen Schule herumgereicht.

Fall 3:

Jeanette hat mit Dani und den anderen Mädels gewettet, dass sie bei Tom zum Zug kommt. Sie macht ein Beweisfoto von sich und Tom küssend auf einer Party und zeigt es Dani und den anderen.

Beschreibung zu Projekt 21: Sexy Chat

Thema	Das Arbeitsblatt „Sexy Chat" will auf sexuelle Anmache in Netzwerken vorbereiten und den Jugendlichen Handlungsoptionen an die Hand geben.
Zielgruppe	ab 12 Jahren
Organisationsform	Einzelarbeit, Gesamtgruppe
Zeit	45 Minuten
Vorbereitung	Spot „Cybersex" auf ⓘ **https://www.klicksafe.de/spots** herunterladen und den Jugendlichen vorführen.
Methodische Hinweise	**Ablauf:** Einstieg mit dem Spot „Cybersex". Dieser Spot aus den Niederlanden verdeutlicht auf eine ironische Art und Weise, dass man oft nicht weiß, mit wem man gerade über das Internet kommuniziert. Die Jugendlichen geben den Inhalt des Spots wieder und erklären die Botschaft. **Aufgabe 1:** Hier wird der Aspekt der Anonymität im Netz noch einmal aufgegriffen. Letzlich kann jede der Personen hinter dem Namen stecken. Die meisten Jugendlichen werden jedoch der Person auf dem ersten Bild den Namen zuordnen. Die gewählten Nicknames oder die gewählten Selbstdarstellungen lassen bei anderen immer ein bestimmtes Bild der Person entstehen, manchmal vielleicht nicht das, welches man intendiert hat. *Mögliche Auswertungsfragen:* ■ Wieso hast du diese Person gewählt? Kannst du dir sicher sein? ■ Man vermittelt mit einem Namen immer ein Bild von sich. Welche Person hättet ihr für den Nickname „Sonnenblümchen" gewählt? *Mögliche Lösungen für Aufgabe 2* (Die alarmverdächtigen Fragen sind *kursiv* gekennzeichnet.) „Auf welche Schule gehst du?" „Wie siehst du aus?" *„Bist du gerade alleine?"* *„Was hast du an?"* „Was machst du gerade?" „Hast du schon mal einen Freund gehabt?" „Hast du ein Haustier?" *„Hast du dich schon mal befingert?"* *„Hast du schon Busen/Schamhaare?"* *„Magst du Pics?"* *„Willst du auf meine Cam kommen?"* „Welche Hobbys hast du?" *„Willst du mir zusehen?"* „Kennst du ein Videoportal?" *„Willst du dir Taschengeld verdienen?"* *„Magst du dich mit mir treffen?"* „Kennst du Google?" *Mögliche Lösungen Aufgabe 3:* Was tun bei sexueller Anmache in Netzwerken**?** ☒ 2 Die Person auf die Ignorierliste setzen. ☐ Die Sprüche oder Bilder an einen Freund/eine Freundin weiterschicken und mit ihr darüber lachen. ☒ 1 Chat sofort abbrechen. ☒ 3 Erwachsene informieren. ☐ Den User übel beschimpfen. ☐ Nie mehr in diesen Chat gehen. ☒ 5 Die Polizei verständigen. ☐ Dem User zurückschreiben, dass er/sie mich in Ruhe lassen soll. ☐ Einen Privatdetektiv beauftragen. ☒ 4 Den User beim Betreiber der Seite melden. **Aufgabe 4:** Das Stehgreifspiel soll die Jugendlichen dazu anregen, Tipps und Handlungsoptionen für den Fall der sexuellen Anmache zu entwickeln. **Hinweis:** Die Jugendlichen sollen nicht den Eindruck bekommen, dass sie sexuelle Anmachen selbst verschuldet haben. Schuld ist immer die/der TäterIn. Zwar werden Mädchen, welche sich in Erwachsenenchats tummeln, bei ihren Angaben gezielt schwindeln und versuchen, sich interessant zu machen, eher sexuell belästigt. Allerdings kann jeder Jugendliche zum Opfer werden, daher ist eine Schuldzuweisung an die Opfer nicht angemessen. Für die medienpädagogische Arbeit existieren für den Themenbereich Chat schon ausführliche Materialsammlungen, die von PädagogInnen und Eltern genutzt werden können, z. B. ■ Materialsammlung mit Informationen und didaktischem Material auf den Seiten von Media-Culture-Online: ⓘ **http://www.lmz-bw.de/chatten-ratgeber.html** ■ ebenso auf den Seiten von klicksafe: ⓘ **http://www.klicksafe.de/themen/kommunizieren/chat/**
Zugang Internet / PC	nein

Projekt 21: Sexy Chat

Aufgabe 1:
Wem gehört dieser Nickname: HardCore Barbie?





Wieso hast du diese Person gewählt?
Kannst du dir sicher sein?

Quelle: public domain

Aufgabe 2:
Achtung beim Chatten, bei manchen der Fragen unten sollten bei dir alle Alarmsignale angehen!
Beurteile selbst: Welche Fragen sind alarmverdächtig? Markiere mit Textmarker.

„Auf welche Schule gehst du?"
„Wie siehst du aus?"
„Bist du gerade alleine?"
„Was hast du an?"
„Was machst du gerade?"
„Hast du schon mal einen Freund gehabt?"
„Hast du ein Haustier?"
„Hast du dich schon mal befingert?"
„Hast du schon Busen/Schamhaare?"
„Magst du Pics?" (engl. pictures = Bilder)
„Willst du auf meine Cam kommen?"
„Welche Hobbys hast du?"
„Willst du mir zusehen?"
„Kennst du ein Videoportal?"
„Willst du dir Taschengeld verdienen?"
„Magst du dich mit mir treffen?"
„Kennst du Google?"

Aufgabe 2:
Was tun bei sexueller Anmache in sozialen Netzwerken?
Wähle aus den Möglichkeiten unten die 5 wichtigsten Dinge aus, die du tun solltest, wenn du im Internet sexuell angemacht wirst. Bringe sie danach in eine sinnvolle Reihenfolge.

- ☐ Die Person auf die Ignorierliste setzen.
- ☐ Die Sprüche oder Bilder einer Freundin/einem Freund zeigen und mit ihr/ihm darüber lachen.
- ☐ Chat sofort abbrechen.
- ☐ Erwachsene informieren.
- ☐ Den User übel beschimpfen.
- ☐ Nie mehr in diesen Chat gehen.
- ☐ Die Polizei verständigen.
- ☐ Dem User zurückschreiben, dass er/sie mich in Ruhe lassen soll.
- ☐ Einen Privatdetektiv beauftragen.
- ☐ Den User beim Betreiber der Seite melden.

Aufgabe 4:
Timo wird seit ein paar Tagen im Chat immer wieder von einem User mit dem Namen „sweetdaddy" angemacht. Er hat ihm auch schon über seine Messenger-Nummer und übers Handy eklige Sachen geschrieben. Timo traut sich nicht, es seinen Eltern zu sagen, da er Angst hat, Internetverbot zu bekommen. Was rätst du ihm? Spielt das Gespräch zwischen Timo und dir den anderen vor.



6_2 Sexting – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Chatregeln – kennst du welche?**	**Skypen – praktisch und doch problematisch!**
Kompetenzen	Die Schülerinnen und Schüler übertragen die Chat-Regeln durch eine Zuordnungs-Übung und übertragen sie auf Erfahrungen.	Die Schülerinnen und Schüler erklären Funktionen der Software Skype anhand einer Internet-Recherche und beurteilen die Datenschutzrichtlinien des Unternehmens.
Methoden	Zuordnungs-Übung, Gesprächskreis	Tabelle, Partnerarbeit
Material	Arbeitsblatt	Arbeitsblatt, Skype Zugänge
Zeit (in Minuten)	45	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Chatregeln – kennst du welche?

Hier sollen die Schülerinnen und Schüler die Chat-Regeln zum sicheren Chatten kennen lernen. Dies geschieht spielerisch in Form eines Textpuzzles. Ob Sie den letzten Arbeitsauftrag tatsächlich durchführen wollen und können, bleibt Ihnen überlassen. Aber das Thema „Chatten" ist wichtig und kann schlimme Folgen, gerade für Jüngere, haben, so dass man an das Chatten heranführen sollte – allerdings in sicheren, moderierten Chatrooms. Diese Chatrooms, hier die Beispiele des SWR und ZDF, verlangen aus bekannten Gründen eine kurze Anmeldung, die evtl. mit den Eltern abgesprochen werden sollte. Wenn Sie die Aufgabe als Hausaufgabe geben, weisen Sie ausdrücklich darauf hin, dass die Eltern informiert sein müssen.

Lösung Textpuzzle
Chat-Tipps für Kinder – Sicher Chatten!

1. Chatte am Anfang nicht allein!
   Frag deine Eltern…
2. Such dir einen kleinen Chat, in dem jemand aufpasst!
   Die Aufpasser (Moderatoren) achten darauf, dass…
3. Geh nicht in Chats für Erwachsene!
   Oft werden dort unangenehme Sachen geschrieben…
4. Denk dir einen guten Spitznamen aus!
   Der Nickname sollte reine Fantasie sein: z. B. …
5. Verrate nie deine Adresse, Telefonnummer und deinen Nachnamen.
   Janine (12 Jahre) hat erlebt, was dann passieren kann: …
6. Sei freundlich, aber bleib auch misstrauisch!
   Verhalte dich so freundlich, wie du auch im richtigen Leben bist…
7. Triff dich nicht mit Leuten aus dem Chat!
   Man kann nie wissen, wer sich dahinter versteckt. …

Quelle: Broschüre: Chatten ohne Risiko? Zwischen fettem Grinsen und Cybersex; www.jugendschutz.net

Hinweise für die Durchführung

AB 2: Skypen – praktisch und doch problematisch!

Den Schülerinnen und Schülern ist das „Skypen" sicherlich geläufig. Die vielen zusätzlichen Funktionen, die Skype bietet, sind wahrscheinlich aber nicht allen bekannt. Die Schülerinnen und Schüler können hier die Software etwas genauer kennenlernen, vor allem unter dem technischen und finanziellen Aspekt (was kostet diese Funktion?). Ein Impuls dahingehend, wieso die Grundfunktionen kostenlos sein können, hilft vielleicht beim Einstieg in das Thema.
Hilfen: **www.skype.com/de/features/**
Wie so oft spielt das Thema Datenschutz eine große Rolle. Hier sollen die Schülerinnen und Schüler dafür sensibilisiert werden, indem sie sich die Datenschutzrichtlinien (ein anspruchsvoller Lesestoff) genauer anschauen. Als kleine Motivationshilfe dient vielleicht der Hinweis, dass JEDER, der bereits Skype nutzt, diesen Datenschutzrichtlinien zugestimmt hat, also auch zumindest ein Teil Ihrer Schülerinnen und Schüler! Die Aufteilung und Partnerarbeit in einzelne Punkte der Richtlinien soll die große Aufgabe handhabbar machen. Vielleicht achten Sie auf eine gleichmäßige Verteilung im Umfang.

Lust auf mehr?

- Zur Weiterarbeit bietet sich eine Dokumentation der Ergebnisse in Form eines Plakates, Merkzettels oder einer Info-Broschüre an. Vielleicht können Sie sogar eine Chateinführung für eine andere, jüngere Klasse veranstalten lassen.

  Auf der Seite **http://www.chatten-ohne-risiko.net/** gibt es einen Lehrerbereich mit Unterrichtsmaterialien sowie einen „Chat Atlas" zur Gefahreneinschätzung aktueller Chats, Messengers und Sozialer Netzwerke.
- WhatsApp bietet mit Whats App calls ebenfalls Telefonie über Messenger. Lassen Sie die SuS hier zu Vorteilen aber auch Problemen recherchieren. Sammlung in einer Mindmap +/–

Chatregeln – kennst du welche? (1/2)

Wenn du dich mit deinen Freunden triffst, machst du das vielleicht bei dir zu Hause in deinem Zimmer. Auch im Internet kannst du dich mit anderen treffen: In einem so genannten „Chat". Um zu chatten, musst du dir also zunächst einen Chatroom suchen. Im Internet gibt es viele Seiten, auf denen du chatten kannst.

„(to) chat" [tschet] ist das englische Wort für plaudern oder schwatzen, „room" [ruum] heißt Raum.
*In **Chatrooms** geht es um unterschiedliche Themen wie zum Beispiel Sport oder Tiere! Zum Chatten brauchst du einen Nickname (= Spitznamen), den können die anderen Kinder auf ihrem Bildschirm auch sehen.*

Nun brauchst du nur noch einen Nicknamen und los geht's!

… **Aber Vorsicht!!!**

Arbeitsaufträge

1. Ordne die Tipps und die Beispiele auf der Folgeseite einander zu und schreibe die passende Zahl in das vorgesehene Feld. Vergleicht eure Anordnung in der Klasse!

2. Ist dir schon einmal etwas Ähnliches passiert? Rede im Sitzkreis mit deinen Klassenkameraden darüber!

3. Weißt du, warum die einzelnen Regeln wichtig sind? Findet zu zweit weitere Beispiele und spielt sie der Klasse vor!

4. Hier findest du Chats für Kinder:

   https://www.klick-tipps.net

Tipp:
Probiere die Chat-Tipps doch selbst mal aus. Klebe das Blatt gut sichtbar an deinen Computerbildschirm!

!!! Bei ihnen musst du dich vorher anmelden! Also frage erst deine Eltern, ob du es überhaupt darfst!

Chatregeln – kennst du welche? (2/2)

Hier noch ein paar Tipps, damit dir das Chatten auch Spaß macht.
Ups … die Tipps und die Beispiele dazu sind durcheinander geraten.

Chat-Tipps für Kinder – Sicher Chatten!

1 Chatte am Anfang nicht allein!

Man kann nie wissen, wer sich dahinter versteckt. Darauf ist Cora (11 Jahre) reingefallen: „Ich habe mich mit einem Mädchen aus dem Chat verabredet, das Pferde auch sehr liebte. Es kam aber ein Junge, der schon über 20 war. Zum Glück war meine Mutter dabei. Ich rate allen: Dass sie sich nie mit jemandem treffen, den sie aus dem Chat kennen. Das ist ein großer FEHLER."

3 Geh nicht in Chats für Erwachsene!

Janine (12 Jahre) hat erlebt, was dann passieren kann: „Ich habe jemandem gesagt, wie ich heiße und in welchem Ort ich wohne! Er wohnte auch dort und fragte mich immer: „Wo wohnst du genau?" Ich habe ihm aber nichts gesagt. Ich hatte ziemliche Angst, dass er plötzlich vor der Tür steht."

5 Verrate nie deine Adresse, Telefonnummer und deinen Nachnamen.

Die Aufpasser (Moderatoren) achten darauf, dass alle freundlich sind. Sie helfen dir, wenn du nicht zurechtkommst.

Der Nickname (=Spitzname) sollte reine Fantasie sein: z. B. ein Name aus deinem Lieblingsbuch, Lieblingsfilm oder ein lustiges Wort. Dein richtiger Name ist dein Geheimnis.

2 Suche dir einen kleinen Chat, in dem jemand aufpasst!

Verhalte dich so freundlich, wie du auch im richtigen Leben bist. Aber glaube nicht alles, was jemand im Chat über sich erzählt. Das ist manchmal geflunkert.

4 Denke dir einen guten Spitznamen aus!

Oft werden dort unangenehme Sachen geschrieben. Katrin (14 Jahre) hat Folgendes erlebt: „Einmal hat einer mich mit blöde Kuh und Nutte beschimpft. Da bin ich sofort aus dem Chat. Und obwohl ich schon 14 bin, gehe ich lieber in Kinder-Chats, weil ich dort nie dumm angemacht werde."

6 Sei freundlich, aber bleib auch misstrauisch!

7 Triff dich nicht mit Leuten aus dem Chat!

Frag deine Eltern oder älteren Geschwister, ob sie dir helfen.



6_3 Selfie – Arbeitsblätter
methodisch-didaktische Hinweise

Übersicht über die Projekte

	Projekt 1 Be yourSelfie	Projekt 2 Sexting – Risiken und Nebenwirkungen	Projekt 3 Du bist, was du postest
Ziele	*Die SuS reflektieren den Einfluss von Beauty-Filtern und digitalen Schönheitsbildern auf ihre Vorstellung von Schönheit.*	*Die SuS lernen Reaktionsmöglichkeiten im Fall von missbräuchlichem Sexting kennen. Sie entwickeln eigene Ideen der Aufklärung über das Thema.*	*Die SuS setzen sich mit Do's und Don'ts der Selbstdarstellung in Sozialen Diensten auseinander. Sie können ihre Selbstdarstellung reflektieren.*
Zeit	**45 min.**	**90 min.**	**45 min.**
Methoden	*Stummer Impuls, Textarbeit, Kreatives Schreiben*	*Schreibauftrag, Definition Sexting, Aufklärungsprojekte kennenlernen, eigene Kampagne entwickeln*	*Analyse, Galeriegang*
Material	*Grafik „monopoly"*	*Videos, Bilder, exemplarische Projekte (Beamer), Material für div. Projektideen (Papier, Poster)*	*Rote Klebepunkte oder rote Stifte, Profile, Lösungen Profile, Flyer WhatsApp, Snapchat, Instagram von klicksafe/handysektor, Checkbogen*
Zugang Internet/PC	*Nein*	*Ja (Tablet, Smartphones, PCs)*	*Nein (Video „Selfie" downloaden) www.handysektor.de/mediathek/videos/erklaer-video-selfie.html*

Projekt 1: Be yourSelfie

Ziele	*Die SuS reflektieren den Einfluss von Beauty-Filtern und digitalen Schönheitsbildern auf ihre Vorstellung von Schönheit.*
Methoden	*Stummer Impuls, Textarbeit, Kreatives Schreiben oder Malen*
Material	*Grafik „monopoly“*
Zugang	*Nein*

45 MIN.

Einstieg

Stummer Impuls: Zeigen Sie das Bild mit dem Spruch „Auf Instagram berühmt zu sein ist wie reich zu sein bei Monopoly“ oder schreiben Sie den Spruch an die Tafel (Abbildung im Anhang). Die Behauptung dahinter: Wer auf Instagram berühmt ist, ist genauso wenig berühmt, wie ein Spieler reich ist bei monopoly. Fame (Ruhm) im Netz hat demnach keine wirkliche Bedeutung im analogen Leben. Diskutieren Sie mit Ihren Schülern: *Was bedeutet der Spruch? Könnt ihr der Aussage zustimmen?*



Instagram Fame, vergänglich und unbedeutend?
Quelle Screenshot: facebook.de, Abruf 13.07.2016

Erarbeitung

Die SuS lesen zur Vertiefung in das Thema den Text auf dem Arbeitsblatt, der von den Themen Beauty-Filter, Selbstoptimierungs- und Idealisierungsvorstellungen sowie den Folgen für den einzelnen Menschen, aber auch die Gesellschaft handelt.

Sicherung

Der Text wird anhand der Fragen auf dem Arbeitsblatt besprochen. Problematisierung der Idealisierungsvorstellung durch Beauty-Filter und Co.:

Was ist das Problem an Beauty-Filtern und Co.?

- Veränderte, normierte Schönheitsvorstellung, durch Firmen vorgegeben
- Egalisierungstendenzen (westliche Vorbilder prägend, generell Vorbilder aus den Medien)
- Beauty-Test ansprechen > wenig Raum für Individualität und Diversität, wenn Bots und Algorithmen nach Merkmalen wie Gesichtssymmetrie beurteilen *http://beauty.ai*

Welche Folgen kann es haben, wenn wir dem Druck ausgesetzt sind, schön auszusehen?

- Körperunzufriedenheit bis hin zu Essstörungen und Magersucht, Fitnesswahn, Body-Shaming

Warum ist es besser, auch auf Bildern „man selbst“ (be yourSelfie) zu sein?

- Echtheit schützt vor „Enttäuschung“, sowohl bei einer Bewerbung als auch bei der Partnersuche übers Internet (bspw. über Tinder). Wie denkt ihr darüber?

Tipp: Wunsch nach Bestätigung – um jeden Preis?

Sprechen Sie mit den SuS abschließend über den YouTube-Trend „Pretty or Ugly“ (in UK, USA), bei dem sich vorwiegend junge Mädchen über ein YouTube-Video anderen zur Bewertung stellen (Rückmeldung über Kommentarfunktion). Das Phänomen des „anonymen digitalen Feedbacks“ stellt aktuell in Deutschland mit der Plattform Tellonym ein Problem dar (Mobbing, Beleidigung, Grooming).
https://www.klicksafe.de/tellonym



„Noch nie war es einfacher, ehrliches Feedback zu bekommen“. Werbespruch des Dienstes Tellonym
Quelle: https://tellonym.de/, Abruf 09.05.2017

Zusatzaufgabe/Hausaufgabe Kreatives Schreiben

Die SuS verfassen einen Zeitungsartikel über den neuesten Schönheits-Trend im Jahr 2022 für das fiktive Magazin „Ego-News. Ausgabe 5/2022“.



Quelle: Screenshot facebook.de, Abruf 14.08.17

Aufgaben:

1. Lies den Text.

„Leg mal 'nen Filter drüber": Im Internet sind alle schön, von Teresa Sickert

Tech-Firmen wie Samsung oder Snapchat prägen mit ihren standardisierten Beauty-Filtern das Bild von Schönheit. Weil so viele Menschen sie benutzen, erhöht sich der Druck auf den Einzelnen, mitzuhalten.

Schönheit liegt im Auge des Betrachters. Oder wird von Samsung bewertet: Der Smartphone-Hersteller hat in seiner Kamera-App einen „Beauty-Face-Modus" integriert, der die Selfies der Nutzer verschönern soll.

Samsung gibt seinen Kunden die Möglichkeit, ihre Augen zu vergrößern, das Gesicht zu verschlanken und die Haut weichzuzeichnen. Was früher Prominenten vorbehalten war, kann heute jeder. Einen professionellen Grafiker, der einem die Pausbacken und den dicken Pickel am Kinn wegretouchiert, braucht heute niemand mehr anzuheuern. Foto-Apps erledigen den Job automatisch. Weil sie nach den immer gleichen Vorgaben optimieren, produzieren sie ein standardisiertes Bild von Schönheit – Nutzer kann das unter Druck setzen.

Mit der richtigen App können alle schön sein

Auch Snapchat bietet seinen Nutzern einen Beauty-Filter mit vorgefertigten Schönheitsvorstellungen an – ähnlich denen von Samsung. Das geschönte Selfie kann so weit gehen, dass manche Frauen mit den veränderten Gesichtern kaum noch wiederzuerkennen sind. Im Falle der amerikanischen Serienschauspielerin Laverne Cox dachten andere Nutzer sogar, sie habe sich operieren lassen. Cox' schmale Nase ließ sich aber mit Snapchats Beauty-Filter erklären.

Das führt vor Augen, wie stark Technologiefirmen in das Online-Aussehen ihrer Nutzer eingreifen können.



Große Augen, klare Haut, der Beauty-Filter im Einsatz.
Quelle Screenshot: twitter.com, Abruf 13.07.2016

Nach welchen Regeln die Beauty-Funktionen Gesichter optimieren sollen, bestimmen die Hersteller. Das Schönheitsideal stammt dabei in der Regel aus der westlichen Welt: schlank, schmales Gesicht, schmale Nase, große Augen. Eben wie ein Snapchat-Filter.

Technologien manifestieren Schönheitsideale

Erst kürzlich sorgte ein Online-Schönheitswettbewerb für Aufsehen, bei dem ein Algorithmus die Gesichter von Menschen beurteilte: Unter den Gewinnerinnen und Gewinnern fanden sich fast ausschließlich Weiße – obwohl sich eine bunte Mischung an Menschen angemeldet hatte.

Die Wissenschaftler, die den „Beauty.AI Contest" ausgerichtet hatten, gaben zu, dass die Gründe dafür auch bei der Personalauswahl zu finden seien, als es noch ums Programmieren ging: Eine sehr homogene Gruppe von weißen Menschen hatte den Algorithmus entwickelt.

So erklärt auch der Psychologe und Attraktivitätsforscher Martin Gründl, dass die künstliche Intelligenz sich bei dem Wettbewerb an weißen Schönheitsvorstellungen orientiert hat. „Weiße bevorzugen eher

weiße Gesichter, Schwarze bevorzugen eher schwarze und Asiaten eher asiatische Gesichter. Es ist einfach so, dass man die eigene ethnische Gruppe bevorzugt."

Selbstoptimierung durch Filter und Beauty-Modes

Doch auch nichtweiße Frauen benutzen die westlich geprägten Beauty-Filter und legen damit über ihre Gesichter eine dicke Schicht stereotyper Schönheitsvorstellungen. Dass das westliche Schönheitsideal vielerorts auf dem Vormarsch ist, liegt vermutlich daran, dass es durch die Medien verbreitet wird – das Internet eingeschlossen. Schon lange dominieren amerikanische Serien und Blockbuster, die sehr schlanke Menschen zeigen, den internationalen Markt.

Die Schönheitsfilter der Apps und Smartphones erleichtern es, mitzuhalten. Sie verändern aber laut Attraktivitätsforscher Gründl nicht die Schönheitsvorstellungen als solche. Makellose Haut etwa galt auch schon früher als attraktiv. Technik macht es nur leichter, sich anzupassen. Die Filter und die allgegenwärtigen aufgehübschten Fotos könnten Menschen aber auch unzufriedener machen, mit sich oder dem Partner, glaubt Gründl. Die Anwendungen könnten unter Umständen auch Essstörungen begünstigen.

Denn neu ist, dass man es sich online kaum noch erlauben kann, ein ganz natürliches Bild zu posten. „Das ist wie bei Passfotos: Wenn es Standard ist, dass jeder sein eigenes Aussehen bei Fotografen schon optimieren lässt und jeder makellose Haut hat, dann setzt einen das unter Zugzwang", sagt Gründl. [...]

Quelle: bento, Teresa Sickert, Abruf 05.10.2016 http://www.bento.de/style/schoenheitsideale-in-apps-standardisierte-beauty-filter-praegen-menschen-902168/

2. Was ist das Problem an Beauty-Filtern und Co.?

3. Welche Folgen kann es haben, wenn wir dem Druck ausgesetzt sind, schön auszusehen?

Zusatzaufgabe/Hausaufgabe

Schönheit im Jahr 2022! Welche neuen Entwicklungen, Apps oder Geräte wird es in Zukunft geben? Schreibe einen kurzen Artikel für das Online-Magazin Ego-News im Jahr 2022.

„Ego-News" Ausgabe 5/2022 NEUER TREND!

Projekt 2: Sexting – Risiken und Nebenwirkungen

Ziele	*Die SuS lernen Reaktionsmöglichkeiten im Fall von missbräuchlichem Sexting kennen. Sie entwickeln eigene Ideen der Aufklärung über das Thema.*
Methoden	*Schreibauftrag, Definition Sexting, Aufklärungs-Projekte kennenlernen, eigene Kampagne entwickeln*
Material	*Videos, Bilder, exemplarische Projekte (Beamer), Material für div. Projektideen (Papier, Poster)*
Zugang	*Ja (Tablet, Smartphones, PCs)*

90 MIN.

Einstieg

Steigen Sie direkt mit dem Arbeitsblatt und der Aufgabe 1 „Geschichte von Luna" ein. Die SuS schreiben ihre Version der Geschichte auf. Einige der Geschichten sollen zur Einstimmung auf das Thema in der Klasse vorgelesen werden.

Falls der von Medien und Pädagogen häufig verwendete Begriff „Sexting" bei den SuS nicht bekannt ist, führen Sie ihn zur Begriffsklärung z. B. durch ein Brainstorming (Was ist Sexting?) ein oder lesen Sie die folgende Definition vor.

Infokasten: Definition Sexting

Sexting ist ein Kofferwort aus den beiden Wörtern „Sex" und „Texting". Sexting beschreibt das Versenden von erotischen Fotos oder Videos der eigenen Person mittels Computer oder Smartphone. Erotisches Material können dabei Aufnahmen in Badehose, in Bikini oder in Unterwäsche sein, Nacktbilder bestimmter Körperregionen oder Oben-ohne-Aufnahmen etc.

Quelle: www.klicksafe.de/themen/problematische-inhalte/sexting/sexting-was-ist-das/, Abruf 25.09.2017

Alternative zur Sexting-Definition: Erklärvideo „Sexting" von handysektor zeigen
www.handysektor.de/mediathek/videos/erklaervideo-sexting.html

Erarbeitung *Was kann man tun, um sich vor möglichen negativen Folgen von Sexting zu schützen?*

Hinweis:

Sexting als freiwillige Handlung zwischen sexuell mündigen Jugendlichen gehört heute auch zur digitalen Lebenswelt Heranwachsender. Dieser Tatsache wird auch mit dem Paragrafen § 184c Absatz 4 (StGB) Rechnung getragen, der den Besitz „jugendpornographischer Schriften, ... ausschließlich zum persönlichen Gebrauch mit Einwilligung der dargestellten Personen hergestellt ...“, nicht unter Strafe stellt.

Quelle: https://www.gesetze-im-internet.de/stgb/__184c.html, Abruf 25.09.2017

Aufgabe 2: Die problematischen Aspekte bzw. Folgen von Sexting sollen nun in einem Unterrichtsgespräch herausgearbeitet werden. Die Schülergeschichten von „Luna“ und eine Sammlung an der Tafel können dabei helfen. Mögliche Folgen:

- Unerlaubte Weiterleitung intimer Fotos oder Videos durch Dritte („sekundäres Sexting“). Hier ist darauf einzugehen, dass die unerlaubte Weiterleitung unter Strafe steht, und dass ein Nichtweiterleiten in vielen Fällen Opfern Leid erspart hätte > Verantwortung aller Beteiligten thematisieren.
- Victim Blaming, die unterschiedliche Bewertung von Sextinghandlungen bei Jungen und Mädchen (Schlampenimage, „Selbst Schuld!“) > Rollenbilder und Empathielosigkeit reflektieren.
- „Cyber-Mobbing“ mit massiven seelischen Schädigungen als Folge
- Rechtliche Aspekte, vor allem Unsicherheiten bzgl. kinder- und jugendpornographischen Inhalten bei Sexting-Handlungen (siehe Artikel im Anhang: Ist Sexting strafbar?)
- Sextortion, die Erpressung z. B. mit Nacktbildern
- Vertrauensverlust gegenüber Ex-Partnern, ehem. besten Freunden

Weitere Informationen finden Sie auf *www.klicksafe.de/sexting*

Aufgabe 3: Stellen Sie eine der folgenden europäischen Kampagnen vor, die sich mit dem Thema Sexting-Prävention beschäftigen (Bilder im Anhang). In einem nächsten Schritt entwickeln die SuS eine eigene kleine Aufklärungskampagne.

1. **Schweizer Aufklärungskampagne: Pro Juventute**
   Zeigen Sie die Poster der Schweizer Kampagne Pro Juventute: „Sexting kann dich berühmt machen – auch wenn du es gar nicht willst". Download der Poster: *www.projuventute.ch/index.php?id=2492*



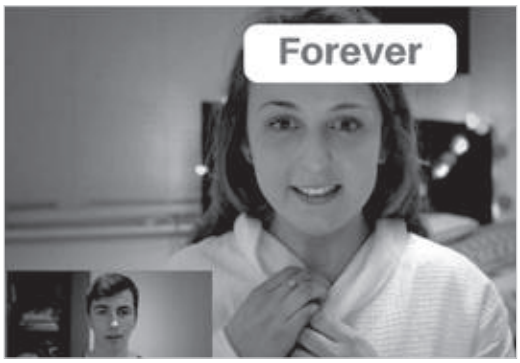
2. **Reaktions-Memes aus UK: App „zipit"**
   Zeigen Sie die App „zipit" des UK-Projekts childline. Hier bekommen SuS Ideen präsentiert, wie sie smart auf explizite Sexting-Anfragen reagieren können.
   www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/zipit-app/

3. **Spot „Forever" aus Irland**



> Tipp:
>
> Weisen Sie die SuS darauf hin, dass sie die Bilder aus der „Gallery" der App in den eigenen Smartphone-Fotospeicher herunterladen können. Sollte man einmal in eine unerwünschte Sexting-Situation kommen, kann man ein Bild als Antwort verschicken.

Zeigen Sie den Spot „Forever" (engl.) von dem irischen Internet-Awareness-Projekt Webwise, unter: *http://www.watchyourspace.ie/forever-campaign/* (+weitere Informationen und Material)



Kampagne Pro Juventute und App zipit
Quellen: www.projuventute.ch, www.childline.org.uk, www.webwise.ie, Abruf 02.10.2017

Anweisung an die SuS:
Ihr dürft eine eigene Aktion/Kampagne/eigenes Infomaterial planen zum Thema „Sexting – Risiken und Nebenwirkungen". Es gibt fünf Möglichkeiten a–e. Sucht euch aus, was euch interessiert und bildet Gruppen. Ihr habt 30 Minuten Zeit. Danach stellt ihr eure Ergebnisse den anderen vor.

a. zweiseitiger Infoflyer (gefaltetes DIN-A4-Papier)
b. Präsentation: drei Folien PPT-Präsentation (Rechner, PPT)
c. Reaktions-Meme (Meme-Generator, Tablet, Smartphone oder PC)
d. ein Poster (DIN-A3-Plakat)
e. 30 Sekunden Videospot/Handyvideo

Tipp: Strafbarkeit von Sexting

Teilen Sie für die Gruppenarbeit einen Artikel von *www.handysektor.de* über die Strafbarkeit von Sexting aus (im Anhang) oder lassen Sie ihn online lesen.

Sicherung

Die SuS stellen ihre Arbeitsergebnisse in einem Galeriegang oder an den Arbeitstischen vor. Es kann überlegt werden, wie man die Kampagne ausweiten und den anderen Schülern der Schule zugängig machen kann.



Quelle: www.handysektor.de

Artikel: Ist Sexting strafbar?
https://www.handysektor.de/porno-gewalt/detailansicht/article/ist-sexting-strafbar.html, Stand 27.06.2017, Abruf 02.10.2017

Sexting ist unter Jugendlichen keine Seltenheit mehr. Sei es zur Selbstdarstellung, zur Beziehungspflege oder als sexuelle Aufreizung – mehr als die Hälfte aller Jugendlichen kennt jemanden, der schon einmal Nacktaufnahmen von sich an andere geschickt hat. Vielleicht hast du auch selbst schon einmal solche Bilder geschickt bekommen? Doch der Trend kann Folgen haben – nicht nur für diejenigen, die Bilder von sich verschicken.

Eine Studie von saferinternet.at zeigt, wie beliebt Sexting bei Jugendlichen ist. Demnach haben 16 Prozent der 14- bis 18-Jährigen schon einmal eine Nacktaufnahme gemacht und 33 Prozent haben schon einmal eine erhalten. Dass Sexting auch unangenehme Folgen haben kann, ist den meisten Jugendlichen klar – allerdings ist es teilweise sogar strafbar! Handysektor macht für dich den Rechts-Check!

Kann ich für das Versenden von Nacktbildern ins Gefängnis kommen?
Zu allererst muss zwischen aufreizenden, erotischen Aufnahmen und pornografischen Darstellungen unterschieden werden. Erotische Aufnahmen zeigen meist Nacktheit ohne Fokussierung auf den Schambereich und sind verbunden mit einem gewissen ästhetischen Anspruch. Pornografie wiederum hat eine Fokussierung der Darstellung auf den Schambereich und zeigt sexuelle Handlungen, die in erster Linie auf die sexuelle Stimulation des Betrachters ausgelegt sind.

Von Kinder- oder Jugendpornografie spricht man, wenn Darstellungen von Kindern (unter 14 Jahren) oder Jugendlichen (14 bis 18 Jahre) hergestellt oder verbreitet werden, die sexuelle Handlungen, Genitalien oder das Gesäß zeigen. Die Herstellung, der Besitz und die Verbreitung von Kinderpornografie sind in jedem Fall strafbar. Ebenfalls unter Strafe gestellt sind Aufnahmen von ganz oder teilweise unbekleideten Kindern in unnatürlicher, geschlechtsbetonter Körperhaltung.

Der Besitz von Jugendpornografie ist nur dann zulässig, wenn nur die dargestellten Personen sie besitzen. Die Verbreitung, also zum Beispiel das Versenden in WhatsApp-Gruppen oder das Hochladen ins Internet sind allerdings in jedem Fall strafbar. Dafür kann man sogar ins Gefängnis kommen. Kinder unter 14 Jahren sind allerdings nicht strafmündig.

Fotos und Videos von über 14-Jährigen in Badehose, Bikini oder Oben-ohne erfüllen allerdings nicht die Definition einer pornografischen Darstellung. Weder Kinder noch Jugendliche machen sich durch das Versenden der selbstaufgenommenen erotischen Bilder und Videos strafbar.

Macht es einen Unterschied, ob ich Bilder von mir oder von anderen verschicke?
Strafbar wird das Versenden erotischer Bilder dann, wenn die Bilder ohne Einverständnis aller dargestellten Personen veröffentlicht oder weitergeleitet werden. Dann spricht man von einer Verletzung des Persönlichkeitsrechtes beziehungsweise des Rechts am eigenen Bild und der Verletzung des „höchstpersönlichen Lebensbereiches". In allen Fällen muss der Täter mit einer Geld- oder Freiheitstrafe oder dem Ableisten von Sozialstunden rechnen. In den meisten Fällen haftet übrigens der Verantwortliche selbst! Nur ganz selten werden die Eltern zur Rechenschaft gezogen.

Was tun, wenn ein anzügliches Foto von mir in Umlauf geraten ist und immer weitergeschickt wird?
Wende dich am besten an einen Erwachsenen, dem du vertraust. Er kann dich bei den weiteren Schritten unterstützen.

Du kannst ...

... die Person bitten, das Bild zu löschen und sie darauf hinweisen, dass ihr Handeln strafbar ist.
... den Anbieter bitten, das Bild zu löschen. Kontaktdaten findest du im Impressum oder im Hilfebereich.
... Strafanzeige gegen den/die Versender bei der Polizei stellen. Dafür solltest du alle Informationen sichern, die du hast, zum Beispiel in Form von Screenshots.
... zivilrechtlich mit einem Anwalt gegen den/die Versender vorgehen. So kannst du einen Unterlassungsanspruch und möglicherweise Schadensersatz erwirken.

Wie soll ich reagieren, wenn mir solche Sexting-Bilder (ungewollt) zugeschickt werden?
Bei kinder- und jugendpornografischen Bildern oder Videos solltest du sofort Anzeige bei der Polizei erstatten. Anschließend musst du die Bilder direkt löschen, denn auch der Besitz der Materialien kann strafbar sein. Auf keinen Fall darfst du die Fotos weiterschicken! Dasselbe gilt für erotische Darstellungen – weiterleiten ist verboten! Informiere die Person, die auf dem Bild zu sehen ist, darüber, dass ihr Bild in Umlauf geraten ist und bitte den Versender, das Bild zu löschen. Weise sie auch darauf hin, dass es strafbar ist, Bilder ohne Einwilligung der abgebildeten Personen zu verschicken.

Wenn du noch weitere Fragen zum Thema hast, dann wende dich z. B. an die Scouts von *www.juuuport.de*.



Quelle: © www.projuventute.ch, Abruf 28.02.2017



Quelle: App zipit, iOS Version; Stand 28.02.2017, Abruf 02.10.2017

Aufgaben:

„Mit nichts machst du dich verletzlicher als mit Nacktbildern von dir“ (Luna, 15).

1. Was könnte Luna passiert sein? Schreibe ihre Geschichte auf.

2. Was können negative Folgen von Sexting sein?
Sammelt an der Tafel.

3. Wie kann man sich davor schützen?
Hier dürft ihr selbst eine kleine Aufklärungskampagne entwickeln, um negativen Folgen von Sexting vorzubeugen. Wählt aus zwischen **a**–**e**.

- **a.** zweiseitiger Infoflyer (gefaltetes DIN-A4-Papier)
- **b.** Präsentation: drei Folien PPT-Präsentation (Rechner, PPT)
- **c.** Reaktions-Meme (Meme-Generator, Tablet, Smartphone oder PC)
- **d.** Informations-Poster (DIN-A3-Plakat)
- **e.** 30 Sekunden Handyvideo

Sextortion – Erpressung mit Nacktbildern

Sextortion ist die Erpressung mit Nacktbildern und häufig eine negative Folge von Sexting. Die Täter drohen, die Nacktbilder zu veröffentlichen [...]. Lass dich deshalb gar nicht erst dazu überreden, Nacktbilder zu versenden, oder dich in einem Chat auszuziehen. Besonders vorsichtig musst du bei völlig fremden Menschen sein, die Kontakt zu dir aufnehmen und nach kurzer Zeit mit dir skypen oder Bilder von dir haben wollen.

Quelle: www.handysektor.de/porno-gewalt/detailansicht/article/ist-sexting-strafbar.html, Abruf 28.02.2017

Projekt 3: Du bist, was du postest

Ziele	*Die SuS setzen sich mit Do's und Don'ts der Selbstdarstellung in Sozialen Diensten auseinander. Sie können ihre Selbstdarstellung reflektieren.*
Methoden	*Analyse, Galeriegang*
Material	*Rote Klebepunkte oder rote Stifte, Profile, Lösungen Profile, Flyer WhatsApp, Snapchat, Instagram von klicksafe/handysektor, Checkbogen auf www.klicksafe.de/mobilemedien*
Zugang	*Nein (Video „Selfie" downloaden)* *www.handysektor.de/mediathek/videos/erklaervideo-selfie.html*

45 MIN.

Einstieg

Zeigen Sie das Handysektor Erklärvideo „Selfie"
www.handysektor.de/mediathek/videos/erklaervideo-selfie.html

Fragen an die SUS: *Welche Art Selfies habt ihr schon gemacht? Welche Selfies sollte man besser nicht veröffentlichen? Was muss man heute bei der Selbstdarstellung im Internet, und vor allem bei Bildern, besonders beachten?*



Quelle: Screenshot handysektor, Abruf 14.08.2017

Erarbeitung

Hängen Sie die Fake-Profile von Dennis Müller (Instagram) und Leandra Kovac (Snapchat; beide im Anhang) im Klassenraum auf oder zeigen Sie sie über Beamer. Das Profil von Dennis Müller finden Sie zu Demonstrationszwecken auch als reales Profil auf Instagram unter *www.instagram.com/dennizz0931*. Die SuS sollen nun auf den beiden Profilen die Bereiche mit einem Punkt markieren, die ihrer Meinung nach in Bezug auf Selbstdarstellung und Selbstschutz problematisch sind. Teilen Sie den SuS dazu rote Klebe-Punkte aus, die SuS können alternativ dazu rote Stifte benutzen. Besprechen Sie mit den SuS die Markierungen und lassen Sie diese begründen.

Mögliche Aspekte

- Verletzung von Bildrechten anderer auf Fotos, urheberrechtliche Vergehen bei Verwendung von Bildern und Videos aus dem Internet
- Negative Selbstpräsentation (Sexting, Feiern, Gewaltinhalte)
- Cyber-Mobbing, Hasskommentare
- Fehlender Selbst- und Fremdschutz: unzureichende Datenschutzeinstellungen (öffentliches Profil, Standortangabe, Nutzernamen in anderen Diensten, Klarname > Veröffentlichung vieler privater Informationen)

Hinweis:

Es kann sein, dass die SuS „glattgebügelte" Profile ablehnen, weil sie „keinen Spaß machen" und es in den Netzwerken, der primär ein Ort der Jugendlichen unter sich ist, um Anerkennung, auch durch gelegentliche Grenzüberschreitungen geht. Die „verhaltensoptimierten" Beispiele sind Vorschläge, von denen natürlich auch abgewichen werden kann. Es ist jedoch wichtig, dass die Beispiele die SuS zum Nachdenken anregen.

Sicherung

Lösungen: Zeigen Sie die beiden Profile in optimierter Version am Beamer oder hängen Sie sie ausgedruckt neben die anderen Profile (im Anhang). Die SuS diskutieren darüber.

Was müsst ihr bei der Selbstdarstellung beachten?

Sammeln Sie zum Abschluss die **Do's and Dont's** der digitalen Selbstdarstellung. Formulieren Sie dazu mit den SuS fünf bis sechs Regeln an der Tafel. Sie können auch die folgenden Tipps per Beamer zeigen oder austeilen.

Tipps für die digitale Selbstdarstellung

1. Bildrechte: Achte die Rechte anderer. Frag nach, ob du Bilder posten darfst, auf denen auch andere zu sehen sind. Jeder hat das Recht am eigenen Bild. Auch beim Markieren anderer vorsichtig sein!

2. Datenschutz! Sei sparsam mit privaten Informationen für die Öffentlichkeit. Nicht jeder muss wissen, dass du gerade von deiner großen Liebe getrennt bist. Und auch deine Kontaktdaten wie Handynummer etc. sind nichts für die Öffentlichkeit.

3. Privatsphäre! Wer Intimes, zum Beispiel Nacktbilder, postet oder verschickt, macht sich besonders verletzlich.

4. Fairness! Hasskommentare oder Mobbing haben in den Netzwerken nichts zu suchen! Streitigkeiten besser nicht digital austragen!

5. Echtheit! Filter sind eine tolle Sache, aber sie killen die Echtheit. Echt ist manchmal einfach besser als künstliche Nachbearbeitung, denn kaum einer sieht real so aus wie auf den Bildern – auch Prominente nicht!
   Finde Alternativen zum Filter (z. B. tolle Lichtverhältnisse nutzen, Perspektiven beim Fotografieren ausprobieren).

6. Generell: Be **yourSelf**ie! – denk darüber nach, wer du bist und wer du sein willst, und präsentiere dich auch digital so. Denke auch an zukünftige Arbeitgeber, die dich im Netz finden werden.



Zusatzaufgabe/Hausaufgabe

- Teilen Sie zum Abschluss der Stunde die Flyer Instagram, Snapchat, musical.ly, facebook, YouTube und WhatsApp aus, bestellbar im Klassensatz auf *www.klicksafe.de/materialien*

- In Partnerarbeit schauen sich die SuS gegenseitig die eigenen Social Media-Profile an. Vorsicht: Vertrauen zwischen den SuS ist hier Voraussetzung, da Profile u. U. sehr persönliche Inhalte haben können.

Schnelle Variante: Selbstcheck der eigenen Bilder im Fotospeicher des Smartphones.

Dazu Check-Bogen **„Digitale Selbstdarstellung“** austeilen, zum Download auf *www.klicksafe.de/mobilemedien*



Check-Bogen „Digitale Selbstdarstellung“

Bildrechte

Datenschutz

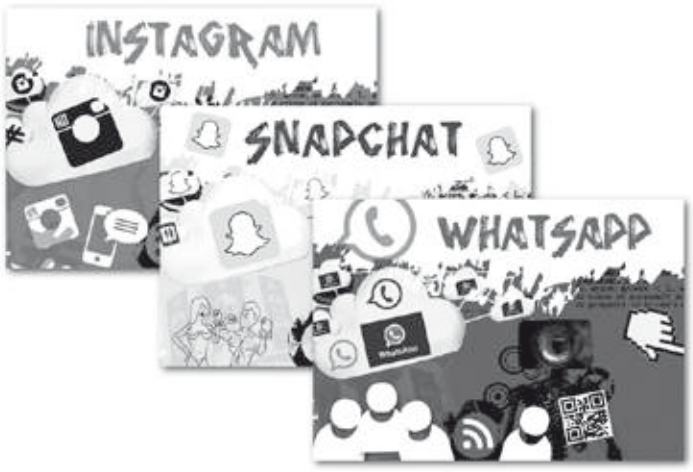
Privatsphäre

Fairness

Echtheit

Better be good

Auswertung



Ansicht Check-Bogen „Digitale Selbstdarstellung“

Profil Dennis Müller (Instagram)



Bild 1: Profilbeispiel Dennis Müller

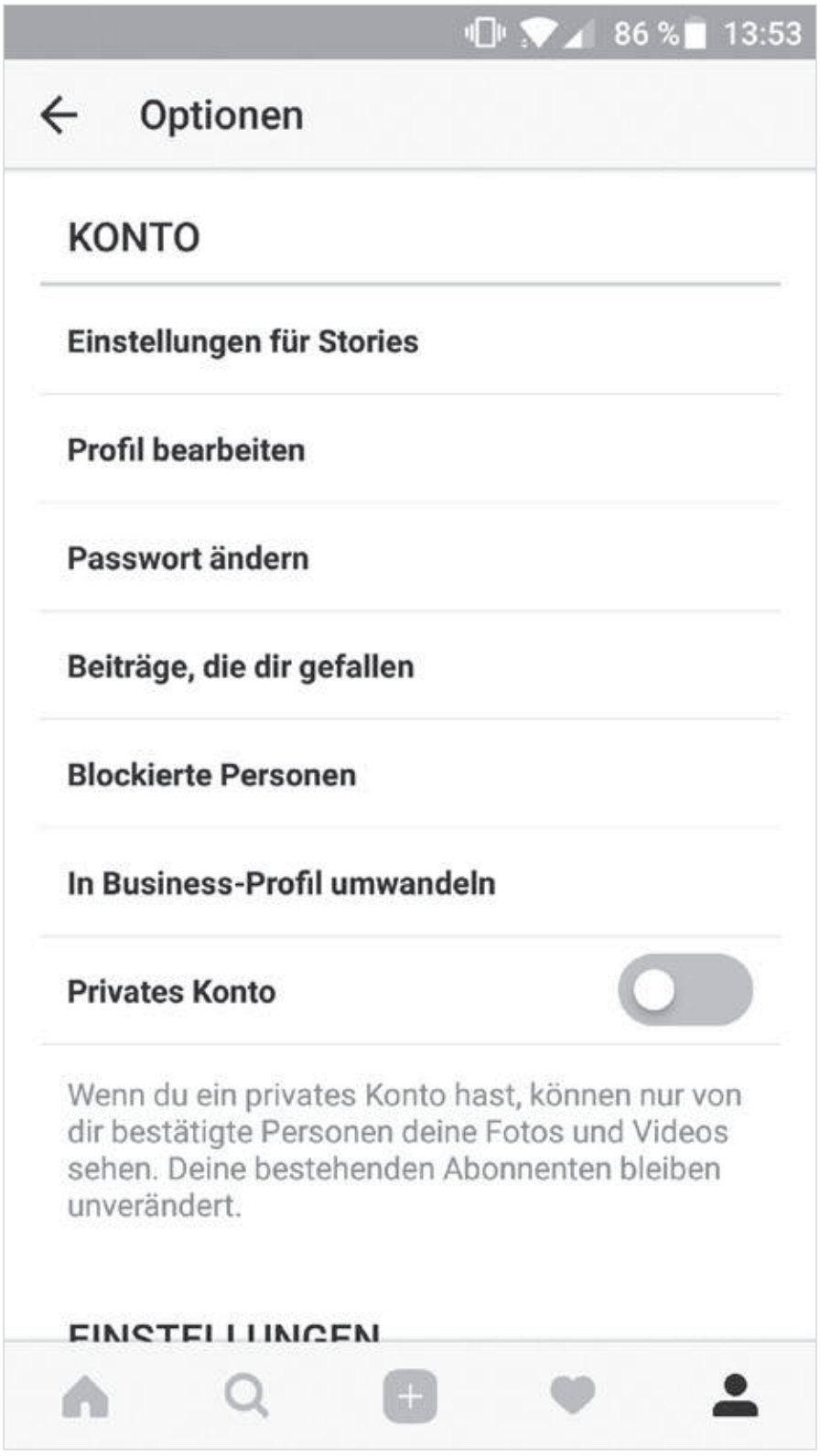


Bild 2: Einstellungen Privatsphäre



Bild 3: Profilbeispiel



Bild 4: Profilbeispiel



Bild 5: Lösung Profilbeispiel Dennis Müller

1. Öffentliches Profil: Das Profil ist für alle Instagram-Nutzer sichtbar, ohne dass diese zuvor eine Anfrage stellen müssen. In den Einstellungen sollte das Profil auf „Privat" umgestellt werden.

2. Klarname: Der vollständige Name des Nutzers ist sichtbar. Besser: Nur der Vor- oder ein Spitzname, den nur Freunde kennen.

3. Private Informationen: Der Sportverein wird genannt. Mit diesen Informationen kann im Netz zum Nutzer eventuell mehr herausgefunden werden (z. B. Wohnort, Trainings- und Spielzeiten der Mannschaft etc.).

4. Snapchat-Nutzername: Damit können andere u. U. auch die Bilder in der Snapchat-Story betrachten (abhängig von den Privatsphäre-Einstellungen in Snapchat). Datenschutz-Grundsatz im Netz: Verknüpfung von Datensätzen/Profilen durch Fremde möglichst vermeiden.

5. Inhalt der Beiträge: Einige der Bilder sind nicht für die Öffentlichkeit gedacht (Partyfotos, Rauchen, Sprüche über Alkohol, Gewalt in Computerspielen etc.). Auch bei einem privaten Profil gilt: Dieser Nutzer wird von 90 Personen abonniert, d. h. sie können seine Beiträge sehen und diese auch abspeichern und verbreiten. Sind wirklich alle so gute Freunde, dass sie diese Beiträge sehen sollten?

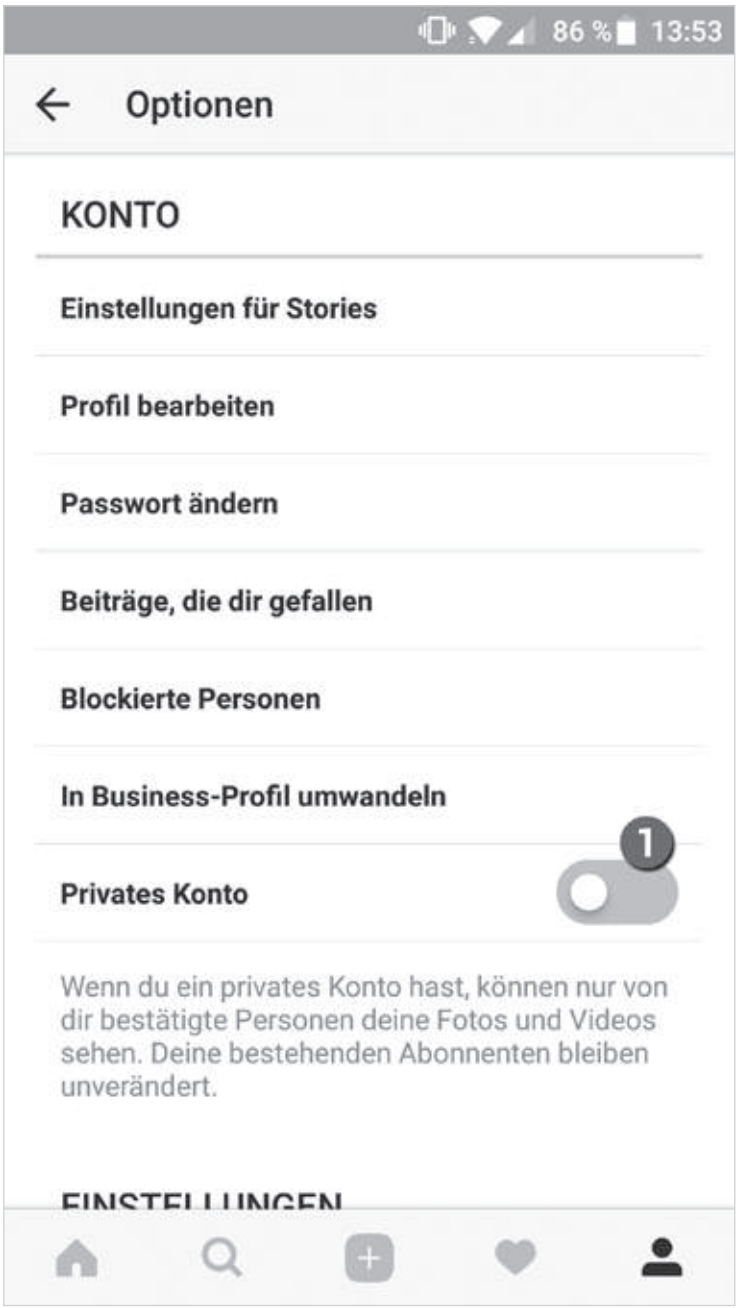


Bild 6: Lösung Einstellungen Privatsphäre

1. Öffentliches Profil: Das Profil ist für alle Instagram-Nutzer sichtbar, ohne dass diese zuvor eine Anfrage stellen müssen. In den Einstellungen sollte das Profil auf „Privat“ umgestellt werden.



Bild 7: Lösung Profilbeispiel

1. Ort markiert: zeigt anderen Nutzern genau an, wo das Bild aufgenommen wurde. Detaillierte Geodaten sollten grundsätzlich nicht öffentlich geteilt werden (in den Einstellungen löschen).

2. Personen erkennbar: Die aufgenommenen Personen sind nicht unkenntlich gemacht (Stichwort: Recht am eigenen Bild).

3. Negative Äußerung: Gerade bei einem öffentlichen Profil machen solche Äußerungen keinen besonders guten Eindruck.



Bild 8: Lösung Profilbeispiel

1. Ort markiert: zeigt anderen Nutzern genau an, wo das Bild aufgenommen wurde. Detaillierte Geodaten sollten grundsätzlich nicht öffentlich geteilt werden.

2. Personen erkennbar: Die aufgenommenen Personen sind nicht unkenntlich gemacht (Stichwort: Recht am eigenen Bild).

3. Nutzer markiert: Eine andere Person wurde auf dem Bild markiert, d.h. das Profil dieses Nutzers kann von dieser Markierung aus direkt aufgerufen werden. Andere Nutzer sollten nur markiert werden, wenn sie zuvor gefragt wurden und zustimmen.

4. Private Informationen: Der Sportverein wird genannt. Mit diesen Informationen kann im Netz zum Nutzer eventuell mehr herausgefunden werden (z.B. Wohnort, Trainings- und Spielzeiten der Mannschaft etc.).

5. Beleidigungen: Weder privat noch öffentlich sind solche Beleidigungen in Ordnung. Doch gerade so öffentlich und nachweisbar können sie für den Äußernden ernste Konsequenzen haben.

Leandra Kovac (Snapchat)

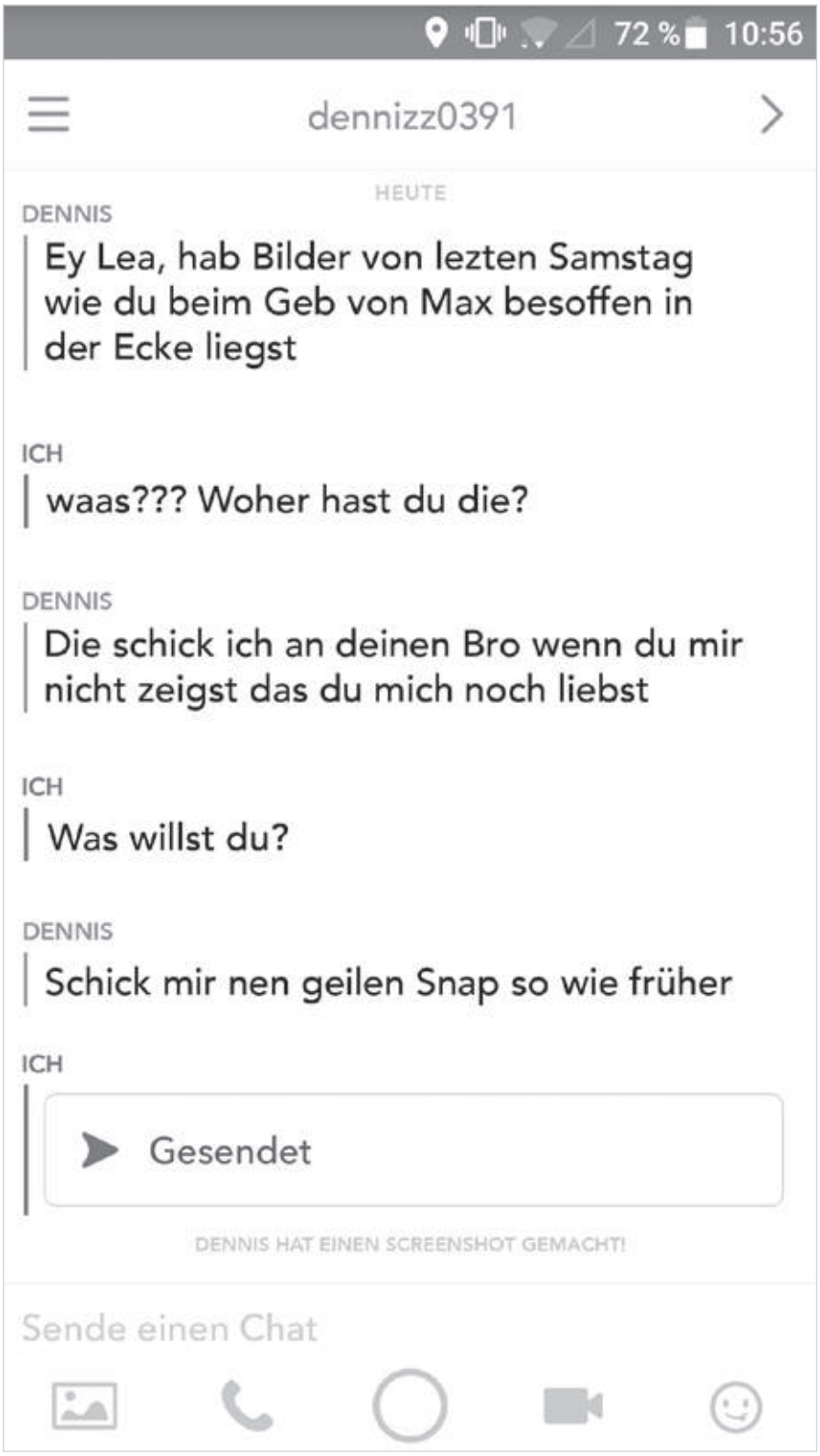


Bild 1: Beispiel Snapchat-Chat

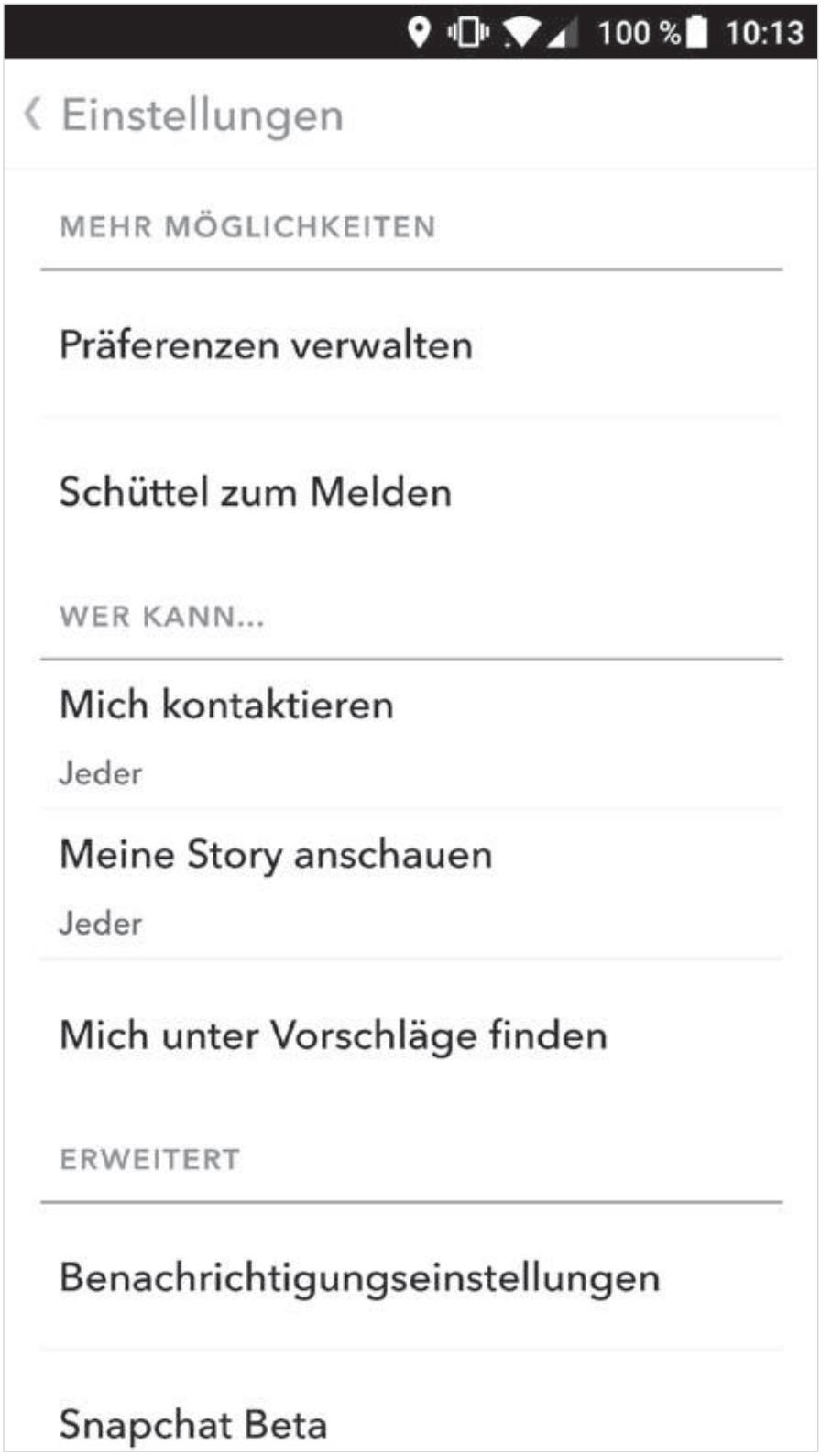


Bild 2: Snapchat-Einstellungen



Bild 3: Einstellungen Blockieren/Entfernen



Bild 4: Lösung Snapchat-Chat

1. Reaktion: Besser als auf die Forderung einzugehen wäre es, auf die offensichtliche Erpressung hinzuweisen.

2. Bild gesendet: In keinem Fall sollte das geforderte Bild geschickt werden. Der Empfänger (Dennis) hat es per Screenshot gespeichert und könnte es nun sogar weiterverbreiten. Besser: Selbst einen Screenshot des Chatverlaufs machen und mit Eltern sprechen.

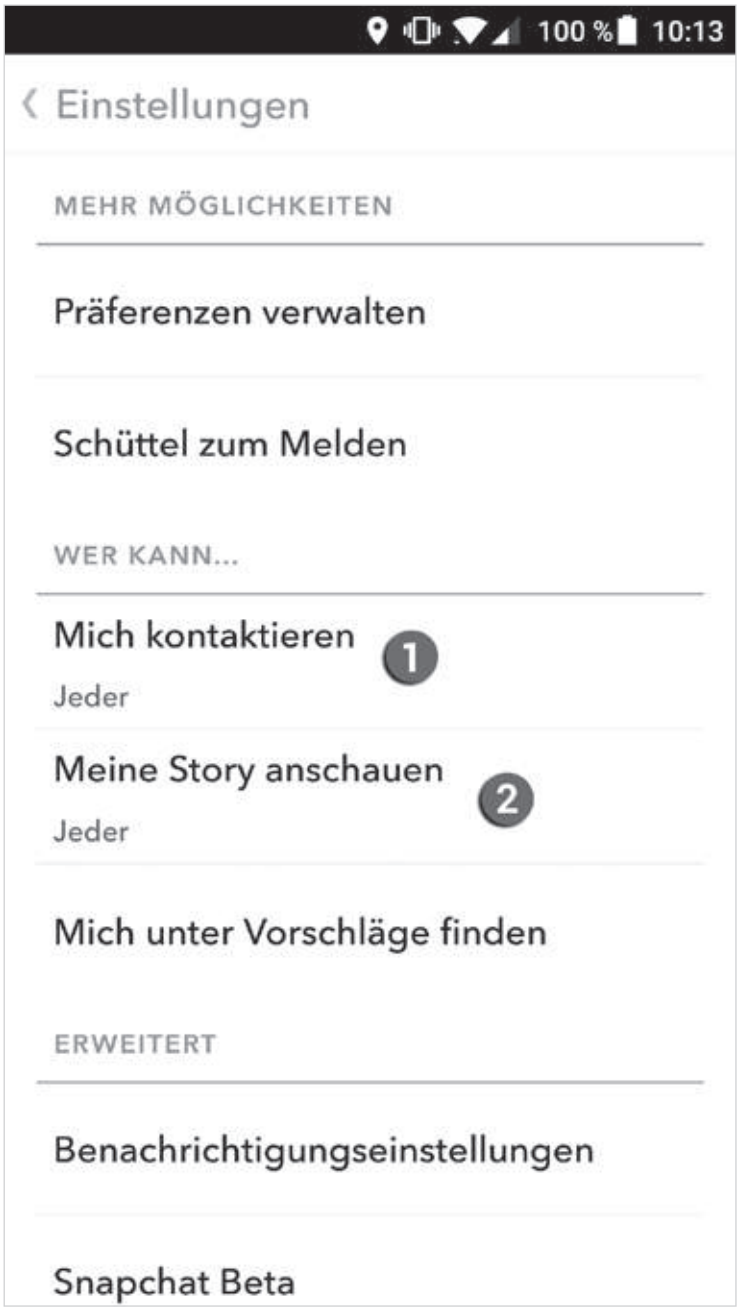


Bild 5: Lösung Snapchat-Einstellungen

1. Jeder kann Kontakt aufnehmen: Jede Person kann das Profil „adden", also als Freund hinzufügen. Dazu reicht es aus, den Nutzernamen in Snapchat zu kennen. Hier sollte eingestellt werden, dass nur Personen im Adressbuch Kontakt aufnehmen dürfen.

2. Jeder kann die Story anschauen: Diese Option steht in Zusammenhang mit der obigen. Kann jeder Kontakt aufnehmen, dann kann mit dieser Einstellung auch jeder Beiträge aus der Story sehen. Besser ist auch hier eine Beschränkung, z. B. auf Personen im Adressbuch.



Bild 6: Lösung Einstellungen Blockieren/Entfernen

1. Blockieren: Nach Beleidigungen, Drohungen oder Erpressungsversuchen sollten entsprechende Profile nach der Beweissicherung durch Screenshot blockiert werden.

   Der Nutzer/Freund kann auch entfernt werden!

7



Freizeit – Gaming und Drohnen

7|1 Gaming

7|2 Drohnen

Übersicht der Bausteine:

- **Gaming** | **Arbeitsblätter**
- **Drohnen** | **Arbeitsblätter**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Handreichung zur Durchführung von Elternabenden: Computerspiele
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_HR_Computer/HR_Computerspiele_klicksafe.pdf



Digitale Spiele
http://www.klicksafe.de/themen/spielen/digitale-spiele/

7

Freizeit – Gaming und Drohnen



7_1 Gaming – Arbeitsblätter
methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Was ist so schön an Handy-Spielen?**	**Online-Spiele – was hältst du von diesen Tipps?**
Kompetenzen	Die Schülerinnen und Schüler fassen ihre Erfahrungen mit Handy-Spielen zusammen und setzen ein gemeinsames Spielen, auch mit den Eltern, um.	Die Schülerinnen und Schüler beurteilen die klicksafe-Tipps für Eltern zum Thema Computerspiele.
Methoden	Tabelle, Partnerarbeit	Stufenleiter, Tabelle
Material	Arbeitsblatt, eigenes Handy, evtl. Elternbrief	Arbeitsblatt
Zeit (in Minuten)	90 (plus Hausaufgabe)	90
Zugang Internet/PC	nein	nein

Hinweise für die Durchführung

AB 1: Was ist so schön an Handy-Spielen?

Über Handy-Spiele zu reden ohne sie zu spielen ist nicht wirklich sinnvoll. Sicherlich finden sich zahlreiche Spiele auf den Handys Ihrer Schülerinnen und Schüler. Sie sollen darüber nachdenken, was ihnen an dieser Art der Spiele gefällt und was nicht. Im zweiten Schritt sollen sie sich untereinander **und** mit Erwachsenen austauschen. Diesen Schritt sollten Sie vielleicht im Vorfeld den Eltern kommunizieren (Per Elternbrief Bescheid geben, was auf die Eltern zukommt!). Kinder haben einen großen Spaß daran und genießen ihre Rolle als „Experten", wenn sie Erwachsenen etwas am Computer, Tablet oder Handy vorführen können. Viele der Reaktionen werden typisch sein. Kinder gehen sehr viel selbstverständlicher, unbefangener damit um, Eltern sehen oft vor allem die Risiken.

Hier eine Formulierungshilfe für einen Elternbrief:

Liebe Eltern der Klasse x,
das Spielen am Handy gehört sicherlich auch für Ihr Kind inzwischen zum Alltag. Wir wollen in der Schule dieses Phänomen thematisieren. Dazu betrachten wir kleine Handy-Spiele, die die Kinder üblicherweise spielen und die für die Altersgruppe geeignet sind. In einem zweiten Schritt sollen die Schülerinnen und Schüler diese Spiele (zu Hause) mit Ihnen, den Großeltern oder anderen Erwachsenen spielen und darüber sprechen. Bitte unterstützen Sie Ihr Kind dabei. Danke.

AB 2: Online-Spiele – was hältst du von diesen Tipps?

Mit dem kleinen Fallbeispiel zum Einstieg sollen die Schülerinnen und Schüler die Tipps von klicksafe zu dem Thema kennen lernen. Dabei sollen sie in die Rolle des Vaters schlüpfen und so einen Rollentausch erleben. Mithilfe der **„Stufenleiter"** können die Schüler eine Bewertung der Tipps vornehmen, die als wichtigstes Kriterium die Teilhabe haben wird. Vielleicht können Sie Ihre Schülerinnen und Schüler anregen, die Tipps auch zu Hause weiterzugeben. Die letzte Phase, die Diskussion des Problems, könnte in Form eines Rollenspiels geschehen oder auch in einem Klassengespräch oder einer Podiumsdiskussion. Vielleicht bietet sich die Methode der „Talking Chips" an, wo jede Schülerin/jeder Schüler zwei „Talking Chips" erhält und für eine Meldung einsetzen muss. Sind alle Chips verbraucht, gibt es eventuell neue. Auf diese Weise erreichen Sie, dass sich alle Schülerinnen und Schüler genau zweimal beteiligen (müssen).
Flyer: **www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Flyer_ComSpiel_Eltern_klicksafe.pdf**

Lust auf mehr?

- Die Online-Spiele boomen und sind, auch wegen ihrer schlechten rechtlichen Fassbarkeit, manchmal problematisch. Gerade die Bereiche „Datenschutz" und „Kostenfallen" bieten sich für eine Vertiefung an, evtl. auch das Problem „Spielsucht".
- Anhand des Flyers „Social Games – Online spielen in Communitys" oder der Webseite **http://www.klicksafe.de/themen/spielen/digitale-spiele/social-gaming-tipps-fuer-kinder/** können Sie die Schüler Tipps für Jugendliche erarbeiten lassen:

  Flyer: **www.klicksafe.de/service/materialien/broschueren-ratgeber/social-games-online-spielen-in-communitys/s/spiele/**
- klicksafe-Online Quiz zu „Digitalen Spielen": **www.klicksafe.de/quiz/**

Was ist so schön an Handy-Spielen?

Nilays Lieblingsspiel auf ihrem Smartphone ist **Candy Crush.** Immer wenn ihr langweilig ist, z. B. auf der Busfahrt zur Schule, dann schiebt Nilay auf ihrem Handy die Süßigkeiten hin und her. Aber **Candy Crush** ist nur eines von vielen Spielen, die sie auf ihrem Smartphone hat. Je nach Lust, Laune und Zeit spielt sie das eine oder das andere.

Arbeitsaufträge

1. Findet euch zu dritt zusammen, wenn möglich mit verschiedenen Handy-Spielen.

2. Spielt zunächst das eigene Spiel und danach – wenn möglich – reihum die Spiele der anderen.

3. Füllt danach für eines der Spiele diese Tabelle aus:

Dieses Spiel habe ich gespielt:

.....

Das gefiel mir an dem Spiel gut:

Das gefiel mir an dem Spiel nicht so gut:

Ich zeige dieses Spiel:

.....

4. Nun darfst du dieses Spiel einem Erwachsenen zeigen! Lasse ihn unbedingt selbst spielen und frage ihn, was ihm an dem Spiel gefällt und was nicht!

5. Sprecht in der Klasse über eure Erfahrungen mit den Erwachsenen!

Nilays Eltern haben ein wenig Sorge, wenn sie zu viel mit ihrem Handy spielt. Kannst du verstehen warum? Redet in der Klasse darüber, wie Erwachsene Handy-Spiele bei Jugendlichen sehen.

Online-Spiele – was hältst du von diesen Tipps? (1/3)

Der Vater von Anna (14 Jahre) ist schier verzweifelt. Er weiß nicht mehr, was er tun soll, denn Anna sitzt jede freie Minute vor Handy, Computer und Tablet und spielt. Der Vater hat ihr schon das Taschengeld gestrichen, aber Anna spielt immer noch Online-Spiele, die angeblich kostenlos sind. Er hat überhaupt keinen Überblick mehr darüber, was genau Anna spielt und steht kurz davor, ihr die Geräte ganz wegzunehmen.

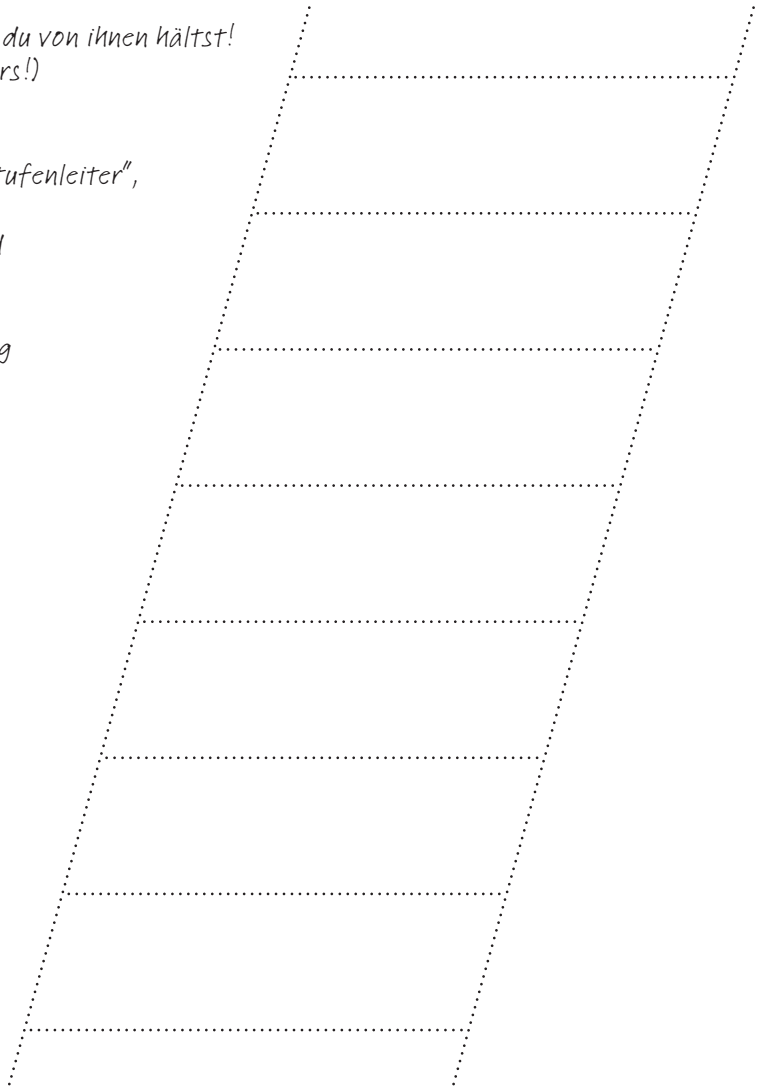
Da stößt Annas Vater auf das Internetangebot von klicksafe.de und liest folgende Tipps:
(siehe nächste Seite)

Arbeitsaufträge

1. Lies die Tipps sorgfältig und notiere kurz, was du von ihnen hältst! (Denke daran, du bist in der Situation des Vaters!)

2. Welche der Tipps hältst du für wichtiger? Sortiere die Tipps nach Wichtigkeit in einer „Stufenleiter", den wichtigsten Tipp nach oben. Tausche dich mit deinen Klassenkameraden darüber aus und zeigt euch gegenseitig eure Einschätzungen.

3. Diskutiert mit der gesamten Klasse eine Lösung für Anna und ihren Vater!



Online-Spiele – was hältst du von diesen Tipps? (2/3)

Tipp	**Erklärung**	**Das halte ich davon:** (in der Rolle des Vaters)
klicksafe.de-Tipp 1: Zeigen Sie Interesse!	Informieren Sie sich über die unterschiedlichen Plattformen, Spielarten (Genres) und die momentan angesagten Spiele. Pädagogische Angebote (z. B. **www.Spieleratgeber-NRW.de, www.spielbar.de, www.usk.de**) bieten weitreichende Informationen zu Inhalten, Altersfreigaben, Chancen und Risiken der gängigen Spiele.	
klicksafe.de-Tipp 2: Beachten Sie Spiele auf mobilen Geräten!	Smartphones und Tablets werden auch als Spielgeräte immer beliebter. Das Angebot ist groß und unübersichtlich. Sie sollten daher gemeinsam geeignete Spiele aussuchen, um z. B. Kostenfallen und problematische Inhalte zu umgehen.	
klicksafe.de-Tipp 3: Sprechen und spielen Sie mit Ihrem Kind!	Interesse, Austausch und gemeinsame Medienerlebnisse ermöglichen eine vertrauensvolle Basis zwischen Ihnen und Ihrem Kind. Suchen Sie daher das offene Gespräch und begegnen Sie dem Freizeitinteresse mit einer grundlegend unvoreingenommenen Haltung. Durch gemeinsame Spielerlebnisse können Sie mitreden, die Faszination nachvollziehen und viel eher erkennen, ob es für Ihr Kind geeignet ist.	
klicksafe.de-Tipp 4: Vereinbaren Sie gemeinsam Regeln!	Erstellen Sie gemeinsam mit Ihrem Kind verbindliche und nachvollziehbare Regelungen zum Medienkonsum. Dazu zählen neben der Nutzung des Computers auch Fernsehen, Smartphones und Spielkonsolen. Achten Sie bei der Vereinbarung auf regelmäßige Bildschirmpausen.	
klicksafe.de-Tipp 5: Orientieren Sie sich an Zeitvorgaben!	Zur Orientierung können folgende Zeitvorgaben hilfreich sein: **4–6 Jahre:** ca. 20 bis 30 Minuten pro Tag in Begleitung der Eltern **7–10 Jahre:** ca. 45 Minuten pro Tag **11–13 Jahre:** ca. 60 Minuten pro Tag (Suchen Sie gezielt nach empfehlenswerten Spielen für Ihr Kind, z. B. auf **www.Spieleratgeber-NRW.de, www.internet-abc.de/eltern**). Für ältere Heranwachsende eignet sich in der Regel ein gemeinsam vereinbartes Medienbudget pro Woche viel eher als eine tägliche Höchstgrenze.	
klicksafe.de-Tipp 6: Achten Sie unbedingt auf die Alterskennzeichnung!	Prüfen Sie unter **www.usk.de**, ob ein Spiel für die Altersgruppe Ihres Kindes freigegeben ist und somit ein entsprechendes Alterskennzeichen der Unterhaltungssoftware Selbstkontrolle (USK) trägt. Diese bieten Ihnen eine wichtige Orientierungshilfe, stellen dabei allerdings keine pädagogische Empfehlung dar. Auch unterliegen viele Spiele im Internet keiner Kennzeichnungspflicht. Nutzen Sie hierzu ergänzende Beratungsangebote (z. B. **www.Spieleratgeber-NRW.de**).	

Online-Spiele – was hältst du von diesen Tipps? (3/3)

Tipp	Erklärung	Das halte ich davon: (in der Rolle des Vaters)
klicksafe.de-Tipp 7: Seien Sie Vorbild!	Erklären Sie lhrem Kind, weshalb es wichtig ist, dass es Gesetze zum Jugendschutz und zum Urheberrecht gibt. Hinterfragen Sie auch lhre eigenen Mediengewohnheiten und gehen Sie mit gutem Beispiel voran.	
klicksafe.de-Tipp 8: Bieten Sie Alternativen!	Viele Kinder sitzen aus reiner Langeweile vor dem Computer oder der Konsole. Bieten Sie lhrem Kind zum Ausgleich gemeinsame Unternehmungen an. Vermeiden Sie es, Computerspiele als „Babysitter" einzusetzen.	
klicksafe.de-Tipp 9: Tauschen Sie sich aus!	Fragen Sie andere Eltern, wie sie mit dem Medienkonsum ihrer Kinder umgehen. lnformieren und unterstützen Sie sich gegenseitig. Das gibt lhnen Sicherheit und fördert die eigene Kompetenz.	
klicksafe.de-Tipp 10: Nutzen Sie Spiele nicht als erzieherisches Druckmittel!	Computerspiele sollten weder zur Belohnung noch als Bestrafung eingesetzt werden. Dadurch erhalten sie einen ungewollt hohen Stellenwert im Alltag lhrer Kinder. Halten Sie lieber an einer verbindlichen Regelung fest: Zuerst die Hausaufgaben, dann eine Pause, dann Computerspielen.	
klicksafe.de-Tipp 11: Handeln Sie, wenn Sie sich um das Spielverhalten lhres Kindes Sorgen machen!	Auskünfte und Hilfsangebote bieten Computerspielsucht-Hotlines und Beratungsstellen, wie bspw. das Berliner Universitätsklinikum Charité, die Uniklinik Mainz sowie die Nummer gegen Kummer. Werden Sie aktiv, wenn lhr Kind (über einen längeren Zeitraum): ■ tägliche Pflichten wie Hausaufgaben vernachlässigt. ■ alle Zeitabsprachen ignoriert. ■ seine Kontakte zu Gleichaltrigen verliert. ■ das lnteresse an anderen Aktivitäten stark zurückgeht.	
klicksafe.de-Tipp 12: Sensibilisieren Sie Ihr Kind bzgl. der Weitergabe persönlicher Daten bei der Nutzung von Online-Spielen.	**Geben Sie folgende Tipps weiter:** ■ Lege Dir eine E-Mail Adresse an, die Du nur für die Anmeldung bei unbekannten Anbietern benutzt! ■ Nutze einen Nickname (Spitznamen) und eine E-Mail-Adresse, die keine Rückschlüsse auf Dich zulassen! ■ Gib Deinen Nickname (Spitzname) und persönliche Daten nur an Bekannte weiter! ■ Nutze als Avatar (virtuelle Spielfigur) kein Foto von Dir! ■ Lies in den AGBs bzw. der Datenschutzerklärung nach, was der Anbieter mit Deinen Daten macht!	

Quelle: www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Flyer_ComSpiel_Eltern_klicksafe.pdf

Methodisch-didaktische Hinweise zu Projekt: Bedrohliche Drohnen?

(ab 10 Jahren, Autorin: Stefanie Rack)

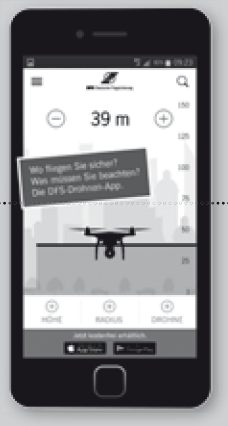
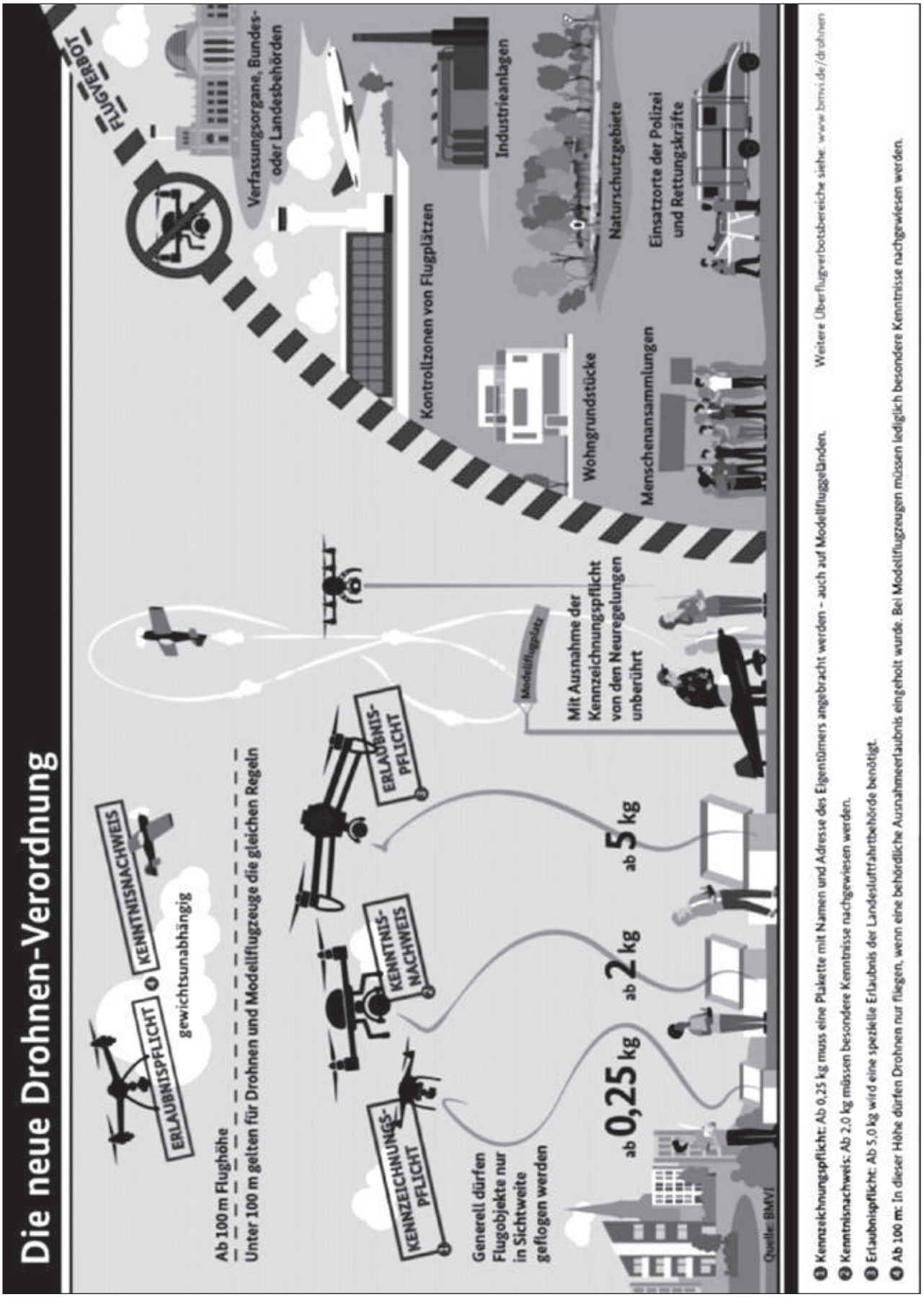
Titel	**Bedrohliche Drohnen?**
Ziele	**Die SuS lernen rechtliche Anforderungen beim Einsatz von Drohnen kennen.**
Unterrichtsstunden à 45 min.	1
Methoden und Material	Vorstellung Plakat, Diskussion zu Drohnenethik Plakat, App
Zugang Internet/PC	Nein (App herunterladen)
Einstieg	Die SuS lesen den Einstiegstext auf dem Arbeitsblatt. Frage an die SuS: In welchen Bereichen werden Drohnen bereits eingesetzt? Wo ist es nützlich? Landschaftsaufnahmen, Kontrolle und Untersuchungen z.B. Überprüfungen von Hochspannungsleitungen, Hochhäusern, Katastrophenhilfe z.B. schwierige Transporte, Medizin und Versorgung in Überschwemmungsgebiete, Postzustellungen, Überwachung von Großveranstaltungen durch die Polizei. Wo haben Drohnen nichts zu suchen? **Was ist eine „Drohne“?** Unter einer „Drohne“ versteht man ein unbemanntes Fluggerät. Das Luftrecht unterscheidet zwischen unbemannten Luftfahrtsystemen und Flugmodellen. Gemäß § 1 Luftverkehrsgesetz handelt es sich bei unbemannten Luftfahrtsystemen um ausschließlich gewerblich genutzte Geräte. Flugmodelle sind hingegen privat, also zum Zwecke des Sports oder der Freizeitgestaltung genutzte Geräte. *Quelle: https://www.bmvi.de/, Abruf: 17.10.2018*
Erarbeitung	Die SuS schauen sich das Schaubild auf dem Arbeitsblatt in Partnerarbeit an und stellen mündlich vor, wo Drohnen verboten sind. **Zum Nachlesen: https://www.bmvi.de/drohnen**, evtl. per Beamer Schaubild größer zeigen. Betonen Sie die Verletzung der Privatsphäre (Höchstpersönlicher Lebensbereich, Recht am eigenen Bild) und den nun gegebenen Schutz durch die Drohnenverordnung.  *Abbildung: Drohnen-App der DFS*
Sicherung	Am Ende der Stunde können sich die SuS die Drohnen-App der deutschen Flugsicherung (DFS) anschauen, downloadbar über itunes oder Google play Store. Sie können die App auch frontal am Beamer zeigen. Die App informiert die Nutzer über geltende Regeln und Vorschriften für die Verwendung von Drohnen in Deutschland. Die App zeigt dem Nutzer in Abhängigkeit von der konkret genutzten Drohne (Modell, Gewicht), welche Regeln/Vorgaben am gewählten Standort gelten. Als Zusatzaufgabe/Hausaufgabe diskutieren die SuS zum Einsatz von Drohnen in Kriegsszenarien. **Praxistest Drohnenflug** Falls SchülerInnen in der Klasse bereits im Besitz einer Drohne sind, kann diese in den Unterricht mitgebracht und ausprobiert werden. Nutzen Sie die App, um einen geeigneten Ort für die Demonstration zu finden.

Schaubild Drohnenverordnung



Quelle: https://www.bmvi.de/drohnen, Abruf: 17.10.2018

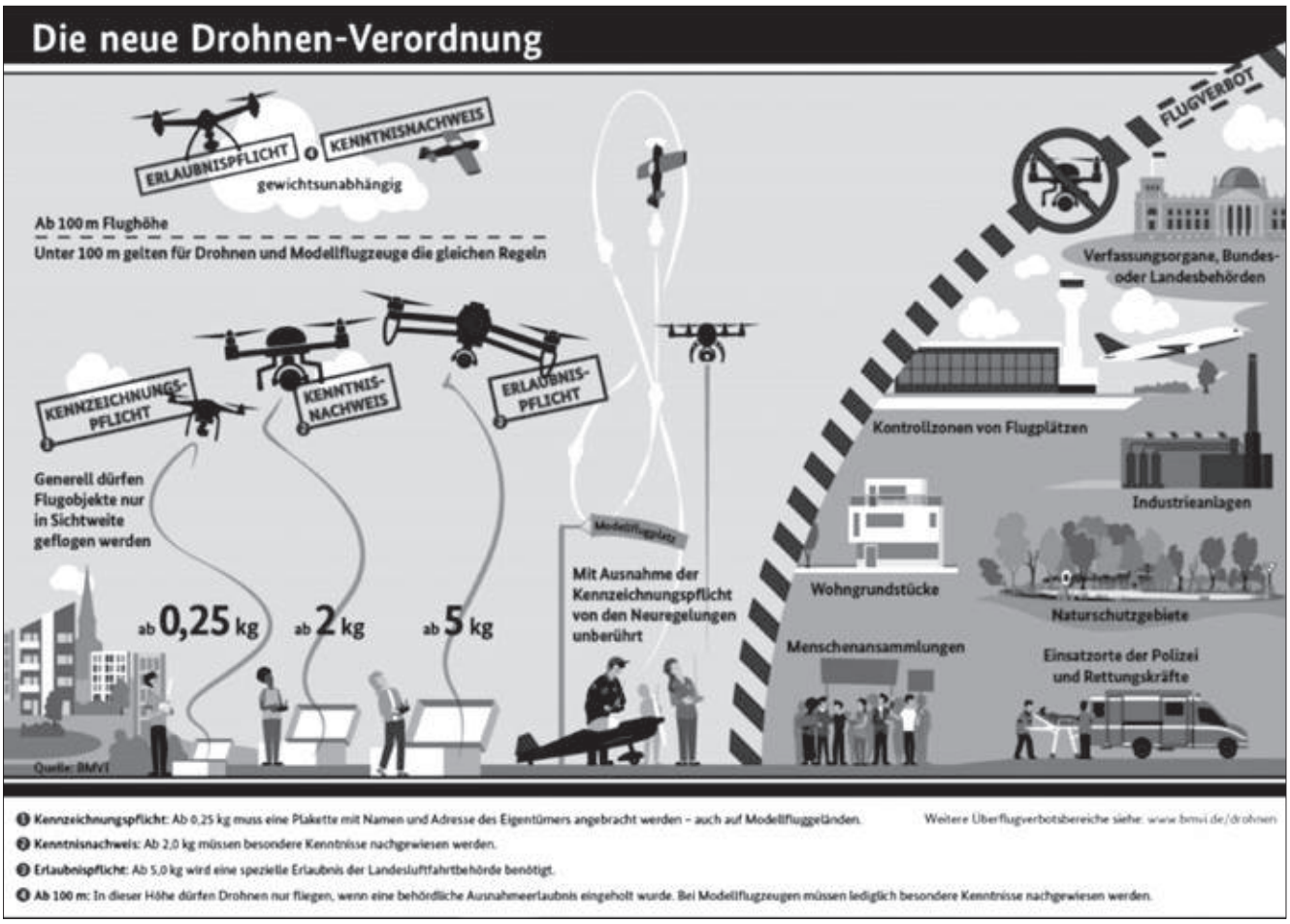
Arbeitsblatt: Bedrohliche Drohnen?

Stell dir vor, du stehst nackt in deinem Badezimmer. Plötzlich erscheint eine Drohne vor deinem Fenster, die dich filmt. Oder eine andere Situation:
Beim Start eines Flugzeuges gerät eine Drohne in das Triebwerk. Ist das eigentlich alles erlaubt?

Information:
Der Verkauf von Drohnen für die private Nutzung hat in den letzten Jahren stark zugenommen. Laut Deutscher Flugsicherung werden im Jahr 2018 in etwa 600.000 Drohnen in Deutschland verkauft.

Aufgabe 1:

Informiere dich in Partnerarbeit auf der Grafik des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) was bei Drohnenbenutzung erlaubt ist und was nicht?



Quelle: https://www.bmvi.de/SharedDocs/DE/Artikel/LF/151108-drohnen.html, Abruf: 17.10.2018

Zusatzaufgabe/Hausaufgabe:

Führt eine Diskussion zum Thema Drohnenethik: Erhöht der Besitz von Drohnen die Bereitschaft, Krieg zu führen? Hier könnt ihr euch informieren:

https://www.zeit.de/politik/ausland/2018-04/kampfdrohnen-luftwaffe-spd-union-debatte

8|1 Lehrer und Datenschutz

8|2 Materialsammlung klicksafe

8

Lehrer und Datenschutz



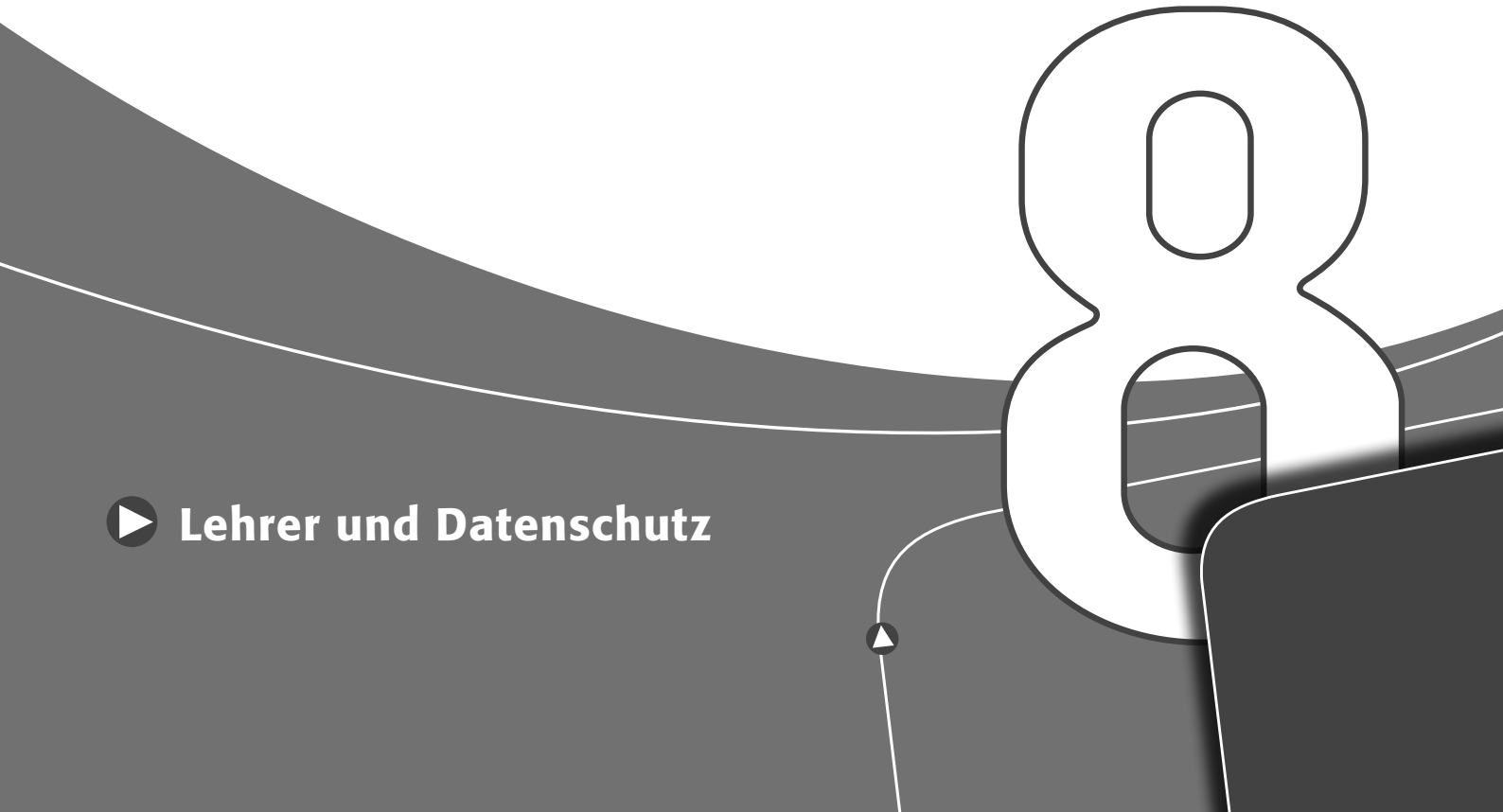
Übersicht der Bausteine:

- **Lehrer und Datenschutz**
- **Materialsammlung klicksafe**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:



Das klicksafe-Lehrerhandbuch
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



Lehrer und Datenschutz

Spezielle Bestimmungen für die Schule

Bei der Vewendung von sozialen Netzwerken durch die Schule außerhalb der Behandlung des Themas im Unterricht für die Kommunikation sind besondere Anforderungen zu beachten. Zu prüfen ist insbesondere dabei, ob dies für alle Schülerinnen und Schüler bzw. Erziehungsberechtigten möglich ist,

- ohne dass das soziale Netzwerk Erkenntnisse aus dieser Kommunikation für eigene Zwecke verwendet,
- die Nutzung dieser Netzwerke für alle Teilnehmer mit keinen Kosten verbunden ist
- und die jeweilige Schulaufsicht dieses Netzwerk dafür freigegeben hat.

Zu bedenken ist auch, dass die Schule als hoheitliche Verwaltungseinrichtung auch an Recht und Gesetz gebunden ist und sich Lehrkräfte, die die Amtsträgereigenschaft aus § 11 Abs. 1 Nur. 2 StGB erfüllen, auch nach § 203 Abs. 2 StGB strafbar machen können, wenn sie unbefugt ein fremdes Geheimnis offenbaren, das ihnen im Rahmen ihrer Tätigkeit anvertraut worden oder sonst bekanntgeworden ist.

Daneben ist zu prüfen, ob beim Einsatz von sozialen Netzwerken als Kommunikationsmittel die datenschutzrechtlichen Anforderungen, wie die Vereinbarung einer Verarbeitung im Auftrag, bzw. die gesetzlichen Vorgaben zu einer gemeinsamen Verantwortlichkeit beachtet werden. Da eine detaillierte Auseinandersetzung mit dabei möglichen Konstellationen hier den Raum sprengen würde, empfiehlt sich in Zweifelsfällen eine Anfrage bei der jeweiligen Schulaufsichtsbehörde unter Einbeziehung des zuständigen Datenschutzbeauftragten. Dabei kann dann auch die jeweils aktuelle Rechtslage berücksichtigt werden, die u.a. durch Rechtsprechung und Aussagen der Datenschutzaufsichtsbehörden gebildet wird.

Kommunikation über Soziale Netzwerke
Die Innenministerkonferenz (IMK) der Bundesländer hat sich in einem Bericht vom April 2012 mit dem Datenschutz in Sozialen Netzwerken beschäftigt und darin rechtliche Bede nken an der Nutzung von Facebook durch öffentliche Stellen und damit auch der Schule angemeldet.[1] Neben den dort aufgeführten, eher allgemein gehaltenen Vorschlägen, existieren noch konkretere Bestimmungen, die den Umgang mit Facebook im schulischen Kontext regeln. In folgenden Bundesländern haben die jeweiligen Schulministerien strikte Verbote erlassen:

- **Baden-Württemberg**
  Das Kultusministerium Baden-Württemberg stellt klar: „Aufgrund datenschutzrechtlicher Bestimmungen ist die Verwendung von Sozialen Netzwerken für die dienstliche Verarbeitung personenbezogener Daten generell verboten“[2]. Damit ist sowohl die Kommunikation (z. B. Termine vereinbaren, Lerngruppen einrichten) zwischen Lehrern und Schülern als auch die Kommunikation zwischen Lehrern über Schüler via Facebook verboten. Soziale Netzwerke dürfen aber im Unterricht genutzt werden, um Vorteile und Risiken pädagogisch zu bearbeiten.

- **Bayern**
  Das Bayerische Kultusministerium formuliert: „Die Kontaktaufnahme als „Follower“ dürfte in beide Richtungen grundsätzlich unzulässig sein. Lehrkräfte sollten selbstverständlich nicht „Anhänger“ ihrer Schülerinnen und Schüler sein, die sie zu erziehen und zu bewerten haben. Entsprechende „Freundschaftsanfragen“ könnten Schülerinnen und Schüler praktisch nicht ablehnen. Und auch die Freundschaftsanfrage durch Schülerinnen und Schüler sollten Lehrkräfte zurückweisen.“[3]

- **Rheinland Pfalz**
  Das Bildungsministerium Rheinland-Pfalz verbietet Facebook-Freundschaften zwischen Lehrern und Schülern, da so das Distanz-Verhältnis zwischen Lehrern und Schülern aufgehoben würde. Zudem

dürfen weder Noten, Hausaufgaben etc. über das Soziale Netzwerk mitgeteilt werden, noch dürfen Klassenausflüge darüber geplant werden. Die Begründung: Der Bildungs- und Erziehungs-Auftrag der Schule und die Datenpolitik von Facebook passen nicht zusammen.[4]

- **Schleswig-Holstein**
  Das Ministerium für Bildung und Wissenschaft des Landes Schleswig-Holstein verbietet die Kommunikation zwischen Lehrern und Schülern über schulische Belange via Facebook. Außerdem ist es Schulen nicht erlaubt, eigene Facebook-Seiten, sogenannte Fanpages einzurichten.[5]

In den übrigen Bundesländern ist die Kommunikation zwischen Lehrern und Schülern derzeit (Stand: 2015) nicht generell verboten:

- **Berlin**
  Zur Nutzung von Sozialen Netzwerken wie Facebook gibt es derzeit keine einheitliche Vorgabe, jedoch forderte der Berliner Datenschutzbeauftragte bereits in seinem Bericht für das Jahr 2013 ein generelles Facebook-Verbot zwischen Lehrern und Schülern.[6]

- **Brandenburg**
  Ein komplettes Verbot wird als unnötig angesehen. Vielmehr wird an das Verantwortungsbewusstsein der Lehrer appelliert, mit persönlichen Daten in allen Nutzungskontexten umsichtig umzugehen.[7]

- **Bremen**
  Auch in Bremen wird die Nutzung von Facebook und ähnlichen Netzwerken nicht grundsätzlich verboten. In einer ausführlichen Handreichung des Landesinstituts für Schule Bremen[8], werden jedoch ausführlich verschiedene Vor- und Nachteile aufgezeigt. Die Art der Nutzung kann somit jeder selbst entscheiden. Es wird jedoch empfohlen, stets eine angemessene bzw. professionelle Distanz einzuhalten.

- **Hamburg**
  Lehrern steht es frei, Soziale Netzwerke im schulischen Kontext zu nutzen. Das Thema Soziale Netzwerke erhält in Hamburg zudem besondere Relevanz, da es ein Teil des für allgemeinbildende Schulen verbindlich zu behandelten Medienpasses ist.[9]

- **Hessen**
  In einer Handreichung zum Umgang mit Sozialen Netzwerken in hessischen Schulen, empfiehlt das hessische Kultusministerium, dass die Nutzung Sozialer Netzwerke im Bereich der schulischen und unterrichtsrelevanten Kommunikation nur sehr eingeschränkt und nur unter bestimmten Voraussetzungen erfolgen sollte. Alternativ sollten vielmehr schulinterne Lernplattformen wie bspw. Moodle genutzt werden, um eine rechtlich unangreifbare Kommunikation und Datenverarbeitung zu gewährleisten. Messenger-Dienste wie bspw. WhatsApp sollten aus datenschutzrechtlichen Gründen in der schulischen Kommunikation nicht eingesetzt werden.[10]

- **Mecklenburg-Vorpommern**
  Es gibt keine expliziten Vorgaben für den Umgang mit Sozialen Netzwerken.

- **Niedersachsen**
  Auch in Niedersachsen werden keine verbindlichen Vorgaben an Lehrkräfte gerichtet.

- **Nordrhein-Westfalen:**
  Es gibt kein explizites Verbot der Facebook-Nutzung im schulischen Kontext. In einer Handreichung der Bezirksregierung Münster wird aber darauf hingewiesen, dass auch innerhalb Sozialer Netzwerke zwischen Lehrern und Schülern stets ein dienstliches Verhältnis herrschen muss.[11]

- **Saarland**
  Aus einem Rundschreiben an alle Schulen des Saarlandes geht hervor, dass die Nutzung von Facebook & Co. im schulischen Kontext generell erlaubt ist. Dabei ist jedoch wichtig, dass Schüler und Eltern, die Facebook nicht nutzen, nicht benachteiligt werden dürfen. Das Soziale Netzwerk

darf also nicht der einzige Kommunikationsweg bleiben und auch innerhalb des Netzwerkes muss eine professionelle Distanz zwischen Lehrern und Schülern gewahrt werden.[12]

- **Sachsen-Anhalt**
  In einem Hinweisblatt des Landes heißt es hierzu: „Soziale Netzwerke dürfen nicht dazu genutzt werden, um dienstliche oder personenbezogene Informationen über ein solches Netzwerk zu verbreiten. Insbesondere wird von der Nutzung i. S. einer Lernplattform abgeraten." [13]

- **Sachsen**
  Das Sächsische Staatsministerium für Kultus verweist bezüglich der dienstlichen Nutzung von Sozialen Netzwerken an Schulen insbesondere auf die Datenschutzproblematik. Das Einstellen personenbezogener wie schulbezogener Daten in Soziale Netz werke durch die Lehrperson wird als datenschutzrechtlich unzulässig bewertet.[14]

- **Thüringen**
  Es herrscht kein explizites Verbot Sozialer Netzwerke, jedoch weist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit in einer Pressemitteilung darauf hin, dass eine dienstliche Nutzung von Facebook den Datenschutzbestimmungen des Landes Thüringen widerspricht und somit unterlassen werden sollte.[15]

Aus der Praxis
Die dienstliche Kommunikation zwischen Lehrern und Schülern via Facebook und Co. ist nicht nur negativ. Für eine Klassenfahrt lässt sich bspw. mittels eines Messenger-Dienstes für einen bestimmten Zeitraum eine Gruppe erstellen, über die die Schüler dann über kurzfristige Programmänderungen informiert werden können. Vorausgesetzt es werden vorher klare Regeln vereinbart, alle SchülerInnen verfügen über den Messenger-Dienst und es ist im jeweiligen Bundesland erlaubt.
***Wichtig dabei vorher abzuklären:** Datenschutzrechtliche Unbedenklichkeit und zwangloses Einverständnis aller Beteiligten!*

Links und weiterführende Informationen:

https://www.kmk.org/dokumentation-statistik/rechtsvorschriften-lehrplaene/uebersicht-schulgesetze.html
Die Seite der Kultusministerkonferenz bietet eine Übersicht über die Schulgesetze aller Bundesländer.

http://li.hamburg.de/medienpass/
Übersichtsseite zum Hamburger Medienpass

www.lis.bremen.de/sixcms/media.php/13/Handreichung_Soziale_Netzwerke_Schule.pdf
Ausführliche Handreichung „Soziale Netzwerke in der Schule" des Landesinstituts für Schule Bremen mit Anwendungsbeispielen.

http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/
Eine umfassende Informationsseite über datenschutzrechtliche Aspekte in der Schule in Baden-Württemberg.

https://www.datenschutzzentrum.de/bildung/schulen/
https://www.datenschutzzentrum.de/bildung/schulen/faq/
Informationen zum Schuldatenschutz in Schleswig-Holstein.

https://www.km.bayern.de/ministerium/recht/datenschutz.html
Webseite des Bayerischen Staatsministeriums für Unterricht und Kultus mit Antworten auf häufige Fragen zum Datenschutz sowie Handreichungen und Arbeitshilfen

https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf
Broschüre des Bayerischen Landesbeauftragten für den Datenschutz zum Thema Schule.

Endnoten

[1] INNENMINISTERKONFERENZ (IKM). (2012, 4. April). *Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012* (Absatz 2). Aufgerufen am 02.08.2015 unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf

[2] IT.KULTUS-BW. (2015, 29. April). *Der Einsatz von „Sozialen Netzwerken" an Schulen.* Aufgerufen am 02.08.2015 unter http://www.kultusportal-bw.de/IT,Lde/Startseite/IT-Sicherheit/soziale+Netzwerke

[3] IT-BEAUFTRAGTER der Bayerischen Staatsregierung. (2012, September). *Der rechtliche Rahmen für den Umgang der Beschäftigten der Bayerischen Staatsverwaltung mit Sozialen Medien* (S. 21). Aufgerufen am 02.08.2015 unter http://www.uni-wuerzburg.de/fileadmin/32040000/_temp_/Weitergabe_Leitfaden_SozialeMedien_-_Rechtlicher_Rahmen_zum_Leitfaden.pdf

[4] DATENSCHUTZ RLP. (2013). *Merkblatt: Lehrkräfte und Soziale Netzwerke (z. B. facebook).* Aufgerufen am 14.07.2015 unter http://www.datenschutz.rlp.de/de/aktuell/2013/images/SMR-Merkblatt-soziale_Netze.pdf

[5] MINISTERIUM für Bildung und Wissenschaft Schleswig-Holstein. (2012, 02. November). *Betrieb von Fanpages auf Facebook und dienstliche Kommunikation über Facebook an Schulen.* Aufgerufen am 14.11.2014 unter http://www.schleswig-holstein.de/DE/Fachinhalte/S/schulrecht/Downloads/Erlasse/Downloads/Facebook.pdf?__blob=publicationFile&v=1

[6] NEWS4TEACHERS.DE. (2014, 2. April). *Berliner Datenschützer will Facebook-Verbot zwischen Lehrern und Schülern auch in der Hauptstadt.* Aufgerufen am 02.08.2015 unter http://www.news4teachers.de/2014/04/berliner-datenschuetzer-will-facebook-verbot-zwischen-lehrern-und-schuelern-auch-in-der-hauptstadt/

[7] KAUFMANN, M. (2013, 24. Juli). *Kein Facebook-Tabu.* maz-online.de. Aufgerufen am 02.08.2015 unter http://www.maz-online.de/Brandenburg/Kein-Facebook-Tabu

[8] LANDESINSTITUT für Schule Bremen. (2013, August). *Soziale Netzwerke in der Schule. Handreichung zur Medienkompetenz.* Aufgerufen am 02.08.2015 unter http://www.lis.bremen.de/sixcms/media.php/13/Handreichung_Soziale_Netzwerke_Schule.pdf

[9] BEHÖRDE für Schule und Berufsbildung. (2013, 8. November). *Digitale Medien. Schulen führen Hamburger Medienpass ein.* Aufgerufen am 02.08.2015 unter http://www.hamburg.de/bsb/pressemitteilungen/4133750/2013-11-08-bsb-digitale-medien/

[10] https://kultusministerium.hessen.de/sites/default/files/media/hkm/handreichung_soziale_netzwerke_-_stand_februar_2015.pdf

[11] SCHEPPING, P., Sieberg, H. & Weichselgärtner, R. (2013, Juni). *„Privat trifft Dienst". Facebook und Co. im schulischen Raum.* Bezirksregierung Münster, Dezernat 46.01 – Lehrerausbildung. Aufgerufen am 02.08.2015 unter http://www.brd.nrw.de/schule/personalangelegenheiten/pdf/2013_10_06_Handreichung_zu_Risiken_und_Grenzen_der_Nutzung_sozialer_Netzwerke_BR_Muenster.pdf

[12] SAARLAND Ministerium für Bildung und Kultur. (2014, 12. Februar). *Rundschreiben an alle Schulen. Umgang mit sozialen Netzwerken.* Aufgerufen am 02.08.2015 unter http://www.saarland.de/dokumente/thema_bildung/Rundschreiben_Soziale_Netzwerke.pdf

[13] KULTUSMINISTERIUM Sachsen-Anhalt. (2014, 19. November). *Hinweise zum Umgang mit sozialen Netzwerken (zum Beispiel Facebook) in den Schulen Sachsen-Anhalts.* Bek. des MK vom 19.11.2014 – 25-5885 (Absatz 5). Aufgerufen am 02.08.2015 unter http://www.mk.bildung-lsa.de/bildung/be-umgang_soziale_netzwerke.pdf

[14] http://www.schule.sachsen.de/download/download_bildung/14_07_verhaltenshinweise_smk.pdf

[15] HASSE, Dr. L. (2013, 29. Juli). *Pressemitteilung. Lehrer in facebook & Co.? NEIN!* Aufgerufen am 02.08.2015 unter https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_lehrer_in_facebook___co.pdf



Datenschutzbestimmungen für Lehrer

Datenschutz im Schulalltag

Die gängige Praxis im Umgang mit Daten im Schulalltag ist nicht immer optimal: Oft gibt es keine persönlichen Büros, die abgeschlossen werden können. Teilweise gibt es keine Dienst-Computer, die ausschließlich zu schulischen Zwecken genutzt werden und zentral von Experten eingerichtet und gewartet werden etc. Häufig bringen Lehrkräfte ihre eigenen ungesicherten Geräte, wie Laptops oder USB-Sticks mit. Auf diesen werden dann zu Hause und unterwegs Klassenlisten, Fotos, Noten etc. verwaltet und gespeichert – schlimmstenfalls in einer ungesicherten Cloud. So kann es leicht vorkommen, dass ein USB-Stick in der Schule vergessen und dann von Schülern gefunden wird. Viele sind sich dieser Gefahren nicht immer bewusst.

Immer daran denken, was schlimmstenfalls passieren kann, wenn Daten (Klassenlisten, Noten, etc.) wirklich einmal in falsche Hände geraten sollten und Risiken minimieren.

Verwaltung von Daten: Was ist erlaubt?

Jedes Bundesland hat seine eigenen Bestimmungen bezüglich der Verarbeitung personenbezogener Daten in der Schule. Allen gemein sind jedoch die folgenden Punkte:

- Private Geräte dürfen nur in Ausnahmefällen zu dienstlichen Zwecken eingesetzt werden.
- Wenn Lehrer personenbezogene Daten von SchülerInnen verarbeiten, ist dies automatisch eine dienstliche Tätigkeit, d. h. es gelten die Landesbestimmungen für den Datenschutz in diesem Falle auch zu Hause und auf privaten Geräten.
- Die Schulleitung muss diese Nutzung (schriftlich) genehmigen, diese Genehmigung kann für maximal fünf Jahre erteilt werden.
- Schülerdaten dürfen nur von den Lehrern verarbeitet werden, die als Klassenlehrer oder Fachlehrer diese Schüler auch unterrichten.
- Es dürfen nur benötigte Daten verarbeitet werden, max. die folgenden:
  - Namen,
  - Geschlecht,
  - Geburtsdatum, Geburtsort,
  - Zugehörigkeit zu einer Religionsgemeinschaft,
  - Klasse, Gruppe oder Kurs,
  - Ausbildungsrichtung bzw. Ausbildungsberuf,
  - Fächer,
  - Art, Datum und Ergebnisse von Leistungskontrollen,
  - Zeugnisnoten und andere Zeugniseintragungen.
- Das Gerät muss so behandelt werden, dass niemand sonst Zugriff auf die Daten haben kann, z. B. durch Passwortschutz und andere Sicherungen.
- Diese Daten dürfen nur verschlüsselt übertragen werden (d. h. bspw. kein unverschlüsselter Versand der Klassenliste per E-Mail).

Die Datenschutzbestimmungen der Länder beziehen nicht immer zu allen Verwendungszusammenhängen Neuer Medien klar Stellung, was durch die fortschreitenden Neuentwicklungen in diesem Feld nicht verwunderlich ist. Bei Unklarheiten ist es aber sicherlich sinnvoll, auf die Nutzung eines bestimmten Dienstes zu verzichten.

Die genauen Datenschutzbestimmungen der einzelnen Bundesländer finden sich hier:

Baden-Württemberg	http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=SchulG+BW&psml=bsbawueprod.psml&max=true (Schulgesetz für Baden-Württemberg – SchulG) http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=PrSchulG+BW&psml=bsbawueprod.psml&max=true (Privatschulgesetz – PSchG)
Bayern	http://www.gesetze-bayern.de/Content/Document/BayEUG (Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen – BAYEUG) http://www.gesetze-bayern.de/Content/Document/BaySchO2016 (Bayerische Schulordnung)
Berlin	http://gesetze.berlin.de/jportal/?quelle=jlink&query=SchulG+BE&psml=bsbeprod.psml&max=true&aiz=true (Schulgesetz für Berlin)
Brandenburg	http://bravors.brandenburg.de/gesetze/bbgschulg (Brandenburgisches Schulgesetz - BbgSchulG)
Bremen	http://transparenz.bremen.de/sixcms/detail.php?gsid=bremen2014_tp.c.69600.de&asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d (Bremisches Schulgesetz - BremSchulG) http://transparenz.bremen.de/sixcms/detail.php?gsid=bremen2014_tp.c.69634.de&asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d (Bremisches Schulverwaltungsgesetz - BremSchVwG)
Hamburg	http://www.landesrecht.hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-SchulGHArahmen&st=lr (Hamburgisches Schulgesetz – HmbSG)) http://www.landesrecht.hamburg.de/jportal/portal/page/bshaprod.psml?doc.id=jlr-FrTrSchulGHA2004rahmen&st=lr&showdoccase=1&paramfromHL=true#focuspoint (Hamburgisches Gesetz über Schule in freier Trägerschaft - HmbSfTG)
Hessen	http://www.rv.hessenrecht.hessen.de/jportal/portal/t/uom/page/bshesprod.psml?doc.hl=1&doc.id=jlr-SchulGHE2005rahmen%3Ajuris-lr00&documentnumber=1&numberofresults=270&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint (Hessisches Schulgesetz – Schulgesetz HSchG)
Mecklenburg-Vorpommern	http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&doc.id=jlr-SchulGMV2010rahmen&doc.part=X&doc.origin=bs&st=lr (Schulgesetz für das Land Mecklenburg-Vorpommern)
Niedersachsen	http://www.schure.de/2241001/nschg.htm (Niedersächsisches Schulgesetz (NSchG)
Nordrhein-Westfalen	http://www.schulministerium.nrw.de/docs/Recht/Schulrecht/Schulgesetz/index.html (Schulgesetz für das Land Nordrhein-Westfalen)

Rheinland-Pfalz	http://landesrecht.rlp.de/jportal/portal/t/n9a/page/bsrlpprod.psml?doc.hl=1&doc.id=jlr-SchulGRP2004rahmen%3Ajuris-lr00&documentnumber=1&numberofresults=146&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint (Schulgesetz Rheinland-Pfalz – SchulG) http://landesrecht.rlp.de/jportal/portal/t/no3/page/bsrlpprod.psml?doc.hl=1&doc.id=jlr-PrivSchulGRPrahmen%3Ajuris-lr00&documentnumber=1&numberofresults=53&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint (Privatschulgesetz Rheinland-Pfalz)
Saarland	http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/SchulOG_SL.htm#SchulOG_SL_rahmen (Schulordnungsgesetz - SchoG) http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/SchulPflG_SL.htm#SchulPflG_SL_rahmen (Schulpflichtgesetz) http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/SchulMG_SL.htm#SchulMG_SL_rahmen (Schulmitbestimmungsgesetz - SchumG) http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/PrSchulG_SL.htm#PrSchulG_SL_rahmen (Privatschulgesetz - PrivSchG) http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/SchulO_SL.htm#SchulO_SL_rahmen (Allgemeine Schulordnung – AschO)
Sachsen	https://www.recht.sachsen.de/vorschrift/4192 (Recht und Vorschriftenverwaltung Sachsen – GVBl. Sachsen 2018,7, S. 198 ff.) https://www.recht.sachsen.de/vorschrift/16220 (Recht und Vorschriftenverwaltung Sachsen – GVBl. Sachsen 2018,12, S. 547 f.)
Sachsen-Anhalt	https://www.bildung-lsa.de/schule/schulrecht/ausgewaehlte_gesetze__verordnungen_und_erlasse/schulgesetz.html (Schulgesetz des Landes Sachsen-Anhalt – SchulG LSA)
Schleswig-Holstein	http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=SchulG+SH&psml=bsshoprod.psml&max=true (Schleswig-Hilsteinisches Schulgesetz - SchulG)
Thüringen	http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=SchulG+TH&psml=bsthueprod.psml&max=true&aiz=true (Thüringer Schulgesetz - ThürSchulG) http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=F%C3%B6rdSchulG+TH&psml=bsthueprod.psml&max=true&aiz=true (Thüringer Förderschulgesetz) http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=FrTrSchulG+TH&psml=bsthueprod.psml&max=true&aiz=true (Thüringer Gesetz über Schulen in freier Trägerschaft - ThürSchfTG)
BfDI	https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html (Anschriften, Telefonnummern, URLs aller Landesbeauftragten für den Datenschutz)

Checkliste
Folgende Checkliste kann helfen, Daten dienstrechtlich korrekt zu verwalten:

- ☐ *Die Schulvorschriften zur Verarbeitung von Schülerdaten auf privaten Geräten wird beachtet*
- ☐ *Es sind ausschließlich Schülerdaten gespeichert, die wirklich benötigt werden (z. B. Namen, Geschlecht, Noten etc.)*
- ☐ *Das Gerät (vor allem auch der USB-Stick) ist mit einem starken Passwort geschützt (d. h. mind. 12 Zeichen, darunter Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen etc.)*
- ☐ *Der unberechtigte Zugriff auf die Daten und Geräte durch Dritte ist ausgeschlossen – auch zu Hause*

Links und weiterführende Informationen

Webseiten

https://www.kmk.org/dokumentation-statistik/rechtsvorschriften-lehrplaene/uebersicht-schulgesetze.html
Übersichtsseite der Kultusministerkonferenz zu den einzelnen Schulgesetzen der Bundesländer. Hier finden sich auch die speziellen Bestimmungen für Privatschulen.

https://www.lehrer-online.de/unterricht/sekundarstufen/geisteswissenschaften/deutsch/unterrichtseinheit/ue/persoenliche-daten-im-internet/
Übersichtsseite von Lehrer-Online zu persönliche Daten und Datenschutz.

www.content-zwh.de/FAH/datenschutznav/default.htm
Lernprogramm für Beschäftigte im öffentlichen Dienst. Erstellt von der Fortbildungsakademie des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen in Zusammenarbeit mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

www.ldi.nrw.de/mainmenu_Datenschutz/index.php
Einführung in grundlegende Fragen des Datenschutzes.

Mediennutzung und Aufsichtspflicht

Aufsichtspflicht auch bei der Mediennutzung
Jeder Minderjährige fällt unter die Aufsichtspflicht. In der Schule übernimmt der Lehrer anstelle der Eltern diese Aufsichtsplicht. Ziel ist immer, Schüler vor Schaden jeglicher Art zu bewahren und das muss überall und zu jeder Zeit gewährleistet sein. Deshalb müssen Lehrer in den Pausen Schulhof und Flure beaufsichtigen und dürfen auch die Klassenräume nicht unbeaufsichtigt lassen. Für volljährige SchülerInnen gilt die sogenannte **Fürsorgepflicht**. Die jeweiligen Bestimmungen sind in den Schulgesetzen der Länder geregelt.

Auch in Bezug auf die Mediennutzung in der Schule gelten diese Pflichten. In vorangegangenen Kapiteln wurde aufgeführt, welche Inhalte für die Entwicklung von Kindern und Jugendlichen problematisch oder gar gefährlich sein können. Auch für den Schulalltag gilt es sicherzustellen, dass besonders gefährdende Inhalte für Kinder und Jugendliche nicht zugänglich sind. Ist das dennoch der Fall, kann dies als Form der Unterlassung geahndet werden.

Da es nur schwer möglich ist, die Aufsicht bzw. die sichere Mediennutzung eines jeden Schülers zu gewährleisten, hat sich im Schulalltag bewährt, dass sich die Schüler beaufsichtigt „fühlen" müssen.[1] Diese gefühlte Aufsicht wäre bswp. nicht gegeben, wenn die zuständige Lehrkraft bei Unterrichtseinheiten im Computerraum grundsätzlich in andere Tätigkeiten vertieft ist und so den Schülern das Gefühl gibt, sich frei und ohne Beachtung der Arbeitsaufträge im Internet bewegen zu können.

Für die korrekte Beaufsichtigung der SchülerInnen können die drei folgenden Grundsätze berücksichtigt werden: [2]

- **Vorausschauende Umsichtigkeit**
  Lehrer müssen Gefahren identifizieren und mit den SchülerInnen klare Regeln vereinbaren, um diese zu vermeiden.
- **Ununterbrochene Beständigkeit**
  SchülerInnen müssen sich darauf verlassen können, dass Lehrer ihre Aufsicht grundsätzlich immer ausführen und wahrnehmen.
- **Kontrollierende Nachdrücklichkeit**
  Regeln werden den SchülerInnen immer wieder ins Gedächtnis gerufen, deren Einhaltung wird kontrolliert und Regelverstöße werden angemessen geahndet.

Verletzung der Aufsichtspflicht
LehrerInnen handeln im Schulalltag nicht als Privatpersonen, sondern als Beamte und damit Angestellte des Staates. Bei einer Verletzung der Amtspflicht (also der durch das ausgeführte Amt eines Beamten begründeten Dienstpflicht), haftet daher auch der Dienstherr.[3] Bei Vorsatz oder grober Fahrlässigkeit kann dieser seine Beamten allerdings zur Verantwortung ziehen.

Doch was genau ist unter Vorsatz und Fahrlässigkeit zu verstehen? Das Bürgerliche Gesetzbuch legt in § 823 grundsätzlich fest, dass jeder, der einem anderen schuldhaft Schaden zufügt, diesen auch ersetzen muss. Einen Schaden zu „verschulden", ist jedoch nicht gleichbedeutend damit, ihn zu „verursachen".[4] Um einen Schaden zu verursachen, muss ein Vorsatz, also die Intention vorliegen, jemanden einen Schaden zuzufügen bzw. muss dieser Schaden billigend in Kauf genommen werden (§ 15 StGB)[5].

Wird ein Schaden „verursacht" kann Fahrlässigkeit vorliegen. Fahrlässig handelt, „wer die erforderliche Sorgfalt außer Acht lässt"[6]. Hier wird in grobe (d. h. Sorgfalt wird bewusst und in schwerem Maße vernachlässigt) oder leichte (d. h. unbewusste) Fährlässigkeit unterschieden.

Die Frage nach grober oder leichter Fahrlässigkeit ist für die Rechtsfolgen einer Aufsichtspflichtverletzung relevant. Folgende Rechtsfolgen können unterschieden werden[7]:

- Bei einem zivilgerichtlichen Verfahren können Schadensersatzforderungen geltend gemacht werden, bspw. wenn im Sportunterricht grundlegende Vorsichtsmaßnahmen wissend außer Acht gelassen wurden.

- Bei einem dienstgerichtlichen Verfahren kann es zu einer Disziplinarstrafe kommen, bspw. nach bewusstem, unerlaubtem Verlassen des zu beaufsichtigenden Bereiches.

- Strafrechtliche Folgen im Sinne einer Verurteilung sind in schwerwiegenden Fällen der Aufsichtspflichtverletzung zu erwarten, bspw. bei einem Badeunfall mit fahrlässiger Tötung.

Internetnutzung sicher gestalten
Es gibt verschiedene Möglichkeiten die Mediennutzung in der Schule für alle Beteiligten sicher zu gestalten:

- **Medienkompetenz**
  Schüler, Lehrer und Eltern sollten um die Chancen und Risiken der Internetnutzung wissen und eigenständig sicher damit umgehen können.

- **Nutzerordnung**
  Mittels einer Nutzerordnung sollten klare Regeln darüber aufgestellt werden, was erlaubt ist und was nicht. Die Ordnung sollte folgende Aspekte umfassen, von allen Beteiligten (Schüler, Eltern) schriftlich bestätigt und ausführlich besprochen werden:

  - Regelung über die Geheimhaltung von Passwörtern
  - Auflistung der verbotenen Nutzungsformen und -inhalte
  - Einhaltung von Datenschutz und Datensicherheit
  - Integrität der Techniken, d. h. kein Eingriff in Soft- und Hardware
  - Umsichtiger Umgang mit den Geräten bis hin zum Ess- und Trinkverbot am PC
  - Klare Regelungen über den Abruf von Informationen / Daten / Programmen aus dem Internet und das Versenden von Informationen über das Internet
  - Wahrung von Urheberrecht und Persönlichkeitsrechten
  - Evtl. Abschnitt zur Aufsicht und außerunterrichtlichen Nutzung

- **Sanktionen bei Missbrauch**
  Verstöße müssen sanktioniert werden. Zur Verfügung stehen im Regelfall die schulischen Disziplinarmaßnahmen bis hin zur strafrechtlichen Ahndung schwerer Verstöße.

- **Technische Kontrolle**
  Der Einsatz von Filtersoftware sowie Servern, die die Zugriffe protokollieren und eindeutige Nutzerkennungen zuweisen, ermöglicht die Kontrolle der Internetaktivitäten.



Aus der Praxis
Um eine sichere Internetnutzung während des Unterrichts zu gewährleisten, hat es sich bewährt, neben technischem Schutz, klaren Regeln etc. den Schülern auch immer mal wieder über die Schulter zu schauen. So sehen sie, dass dem Lehrer nicht vollkommen entgeht, was sie tun (Stichwort: gefühlte Aufsicht).

Exkurs: WLAN in der Schule

Viele Schulen ermöglichen mittlerweile ihren SchülerInnen einen kostenlosen Internetzugang über WLAN – auch außerhalb des Unterrichts, in Pausen und Freistunden. Voraussetzung dafür sind allerdings klare und eindeutige Nutzungsregeln, die als Teil der Schulordnung von der Schulkonferenz beschlossen werden. Diese sollten in schriftlicher Form vorliegen und von Schülern und Eltern unterzeichnet werden.

In den Nutzungsregeln sollte enthalten sein,

- dass der Internet-Zugang nur zu schulischen Zwecken genutzt wird,
- dass alle gesetzlichen Bestimmungen zum Urheberrecht, Jugendschutz, Strafrecht etc. zu beachten sind,
- dass die Schule Nutzungseinschränkungen wie technische Filtersperren, zeitliche Beschränkungen und definierte Zugänge vornehmen darf,
- dass die Schule keine Haftung für die Datensicherheit und -integrität der Geräte der SchülerInnen übernimmt,
- welche Sanktionen bei Missbrauch erfolgen,
- dass die Schule jede Aktivität personenbezogen protokollieren, speichern und verarbeiten darf.

Für den Einsatz von WLAN im Schulgebäude ist es wichtig dafür Sorge zu tragen, dass der Internetzugang nur seitens berechtigter Personen, also SchülerInnen und LehrerInnen, möglich ist. Gewährleistet werden kann dies in technischer Hinsicht bspw. über eine Anmeldung mit Nutzername und Passwort.

Links und weiterführende Informationen

Webseiten

www.schulministerium.nrw.de/docs/Recht/
https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/index.html

Unter Regelungen > Muster-Nutzerordnung der Computereinrichtung an Schulen findet sich hier ein Musterbeispiel einer Nutzerordnung für den schulischen Einsatz

www.schleswig-holstein.de/DE/Fachinhalte/L/lehrer_innen/Downloads/Muster_Internetnutzung.pdf?__blob=publicationFile&v=1

Musterbeispiel einer WLAN-Nutzungsregelung für Schulen

www.schulrecht-sh.de/texte/i/internetnutzung.htm

Schulrecht von Schleswig-Holstein zur Internetnutzung an Schulen

www.nibis.ni.schule.de/~as-ver/fach/paedagogik/material/aufsichtspflicht.pdf

Ein detailliertes Skript zu Fragen rund um die schulische Aufsichtspflicht

www.schulrecht-rw.de/2_Aufsichtspflicht.pdf

Ein Skript zum Thema Aufsichtspflicht, zusammengestellt für angehende und bereits tätige Lehrende an Grund- und Hauptschulen in Baden-Württemberg

Endnoten

[1] STAATLICHES Seminar für Didaktik und Lehrerbildung Rottweil. (o. A.). *Aufsichtspflicht*. Aufgerufen am 02.08.2015 unter http://www.schulrecht-rw.de/2_Aufsichtspflicht.pdf

[2] Ebd.

[3] GRUNDGESETZ für die Bundesrepublik Deutschland. *Artikel 34*. Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/gg/art_34.html

[4] BÜRGERLICHES Gesetzbuch. *§ 823 Schadensersatzpflicht.* Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/bgb/__823.html

[5] STRAFGESETZBUCH. *§ 15 Vorsätzliches und fahrlässiges Handeln.* Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/stgb/__15.html

[6] BÜRGERLICHES Gesetzbuch. *§ 276 Verantwortlichkeit des Schuldners* (2. Satz). Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/bgb/__276.html

[7] STAATLICHES Seminar für Didaktik und Lehrerbildung Rottweil. (o. A.). *Aufsichtspflicht*. Aufgerufen am 02.08.2015 unter http://www.schulrecht-rw.de/2_Aufsichtspflicht.pdf

Materialsammlung Klicksafe



Ethik macht klick –
Werte-Navi fürs digitale Leben

Mit den zunehmenden technischen Möglichkeiten, die die digitalen Medien bieten, steigt auch der Bedarf an Orientierung. Wer sagt einem, was geht und was besser nicht im Internet veröffentlicht bzw. angeklickt werden sollte? Welche Handlungshilfen und Vereinbarungen braucht es für Kinder, Jugendliche und erwachsene Internetnutzer? Und auf welche Werte genau sollten sich diese Vereinbarungen stützen, um auf den „guten Seiten" des Internets zu bleiben?

Zahlreiche Informationen, Anregungen und praktische Übungen zu diesem Thema bietet das neue klicksafe-Unterrichtmodul „Ethik macht klick – Werte-Navi fürs digitale Leben".

klicksafe hat sich auf drei Themenfelder konzentriert, bei denen Orientierungsbedarf besteht: der Schutz der Privatsphäre, Cyber-mobbing bzw. Online-Gewalt und Gender-Sensitivität. Durch den Einsatz des neuen Unterrichtmoduls wird die Persönlichkeit der Jugendlichen gestärkt und ihnen eine wertebezogene Haltung vermittelt. Auf diese Weise finden sie ihren eigenen Weg, sich in der digitalen Gesellschaft zurechtzufinden.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf



Wikipedia –
Gemeinsam Wissen gestalten

Schnell etwas in der Online-Enzyklopädie nachzuschauen, gehört für viele inzwischen zur alltäglichen Online-Nutzungsrealität. Ob für die Hausaufgaben, die Fragen, die im Alltag auftauchen, oder aber für Lehrer bei der Vorbereitung des Unterrichts – auf Wikipedia wird besonders gerne für die schnelle Recherche über ein Thema zurückgegriffen.

Doch noch zu wenige Nutzer wissen über die Prinzipien der Wikipedia Bescheid. Wie entstehen die Inhalte? Kontrolliert jemand, was geschrieben wird? Das Unterrichtsmaterial erlaubt Einblicke hinter die Kulissen der Wikipedia und soll Schülern Informationskompetenz, Quellenkritik und die Freude am kollaborativen Mitarbeiten an der Wissengemeinschaft vermitteln.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Wikipedia/LH_Zusatzmodul_Wikipedia_klicksafe.pdf



Wie finde ich, was ich suche?
Suchmaschinen kompetent nutzen

In der heutigen Informationsgesellschaft hat jeder Einzelne die Möglichkeit, an Informationen zu kommen, die ihm noch vor wenigen Jahren nicht so ohne weiteres zugänglich gewesen wären. Andererseits müssen wir uns aber auch einer immer größer werdenden Informationsflut stellen. Der kompetente, effiziente und verantwortungsbewusste Umgang mit Informationen gewinnt daher zunehmend an Bedeutung Informations- und Medienkompetenz ist eine Basisqualifikation, die bereits im frühen Schulalter erworben werden sollte.

Das klicksafe-Zusatzmodul „Suchmaschinen" ist für die Arbeit mit Kindern und Jugendlichen der Sekundarstufen I und II gedacht. Ziel aller Partner dieser Broschüre ist es, Lehrer und Schüler über die Funktionsweise von Suchmaschinen zu informieren. Nur wer zumindest in Grundzügen verstanden hat, wie Suchmaschinen arbeiten und wie man sie im eigenen Sinne einsetzt, wird in der Lage sein, die aufgefundenen Inhalte zu bewerten und verantwortungsvoll mit dem Medium Internet umzugehen.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmaschine/LH_Zusatzmodul_Suchmaschinen_klicksafe.pdf



Rechtsextremismus hat viele Gesichter
Wie man Rechtsextreme im Netz erkennt – und was man tun kann

Rechtsextremismus tritt in vielerlei Gestalt auf – als Partei oder als rechtsautonome Gruppe, im Internet oder als nächtlicher Fackellauf, im Sportverein oder bei Auftritten von rechtsextremen Musikgruppen. Oft geschickt getarnt streuen Rechtsextreme ihr menschenverachtendes Weltbild, werben junge Menschen an und agieren gegen unsere freiheitlich-demokratische Grundordnung.

Um gegen rechtsextreme Agitation vorzugehen, sind neben Engagement auch Informationen und pädagogisch aufbereitetes Material nötig. Die vorliegende Broschüre verbindet das spezifische Know-how verschiedener kompetenter Organisationen. Das Themenspektrum erstreckt sich vom Vermitteln von Grundwerten menschlichen Zusammenlebens über die Sensibilisierung für das Erkennen rechtsextremer Meinungsmache bis hin zu Gegenstrategien und dem Kennenlernen von Aussteigerprogrammen.

Link zum Download:
http://hthhhklicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Rechtsextremismus_klicksafe.pdf



Nicht alles, was geht, ist auch erlaubt! Downloaden, tauschen, online stellen – Urheberrecht im Alltag

Fast alle Jugendlichen und immer mehr Kinder nutzen heute das Internet: zum Spielen, Musik Hören,Recherchieren für die Schule und um miteinander zu kommunizieren. Dieses neue Kommunikationsverhalten birgt großartige Möglichkeiten. Man kann sich darstellen, über Musik, Filme, Fotos etwas über sich und seine Vorlieben mitteilen und mit anderen in einem nie dage-wesenen Maß vernetzen und austauschen. Dies birgt aber auch rechtliche Fallstricke. Denn es ist rechtlich betrachtet ein grundlegender Unterschied, ob man jemandem etwas ins Gesicht sagt oder das Gleiche bei Facebook postet, wo es viele andere lesen können.

Ebenfalls völlig unterschiedlich ist es, ob man zu Hause eine Musik-CD brennt und sie einer Freundin gibt oder man dieselben Musikstücke bei RapidShare hochlädt oder in einem Shared Folder auf dem PC speichert, auf den alle anderen Nutzer einer Tauschbörse zugreifen und die Dateien herunterladen können. Nicht alles, was geht im Internet, ist auch erlaubt!

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Urheberrecht_klicksafe.pdf



Let's talk about Porno! Jugendsexualität, Internet und Pornographie

Nacktfotos und Pornos sind heute über das Internet für Jugendliche quasi frei verfügbar. Doch viele dieser sexualisierten Medieninhalte können sie verunsichern und überfordern, warnen Jugendschützer.
Das klicksafe-Zusatzmodul, welches in Zusammenarbeit mit pro familia Bayern und dem Landesmedienzentrum Baden-Württemberg entwickelt wurde, liefert zum Thema „Pubertät 2.0: Aufwachsen in sexualisierten Lebenswelten" sowohl Hintergrundinformationen für Lehr- und Fachkräfte als auch konkrete Module für Unterricht und Jugendarbeit.
Das Heft gliedert sich in die vier Bausteine:
1. Leben in der Pubertät,
2. Schönheitsideale in unserer Gesellschaft,
3. Pornografie im Netz und
4. Sexualisierte Kommunikation.

Zum Angebot zählen auch Praxismaterialien und methodische Vorschläge, zum Beispiel zur Frage, wie Jugendliche mit dem medial aufgebauten Druck, vermeintlich körperlich attraktiv und „sexy" sein zu müssen, umgehen lernen.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Porno/LH_Zusatzmodul_Porno_klicksafe_gesamt.pdf



Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web

Das Thema Datenschutz ist in aller Munde. Nach den großen Datenskandalen in letzter Zeit ist das Thema anscheinend über Nacht populär geworden. Gleichzeitig lässt sich aber beobachten, wie sich ein beachtlicher Teil, auch der erwachsenen Bevölkerung, im World Wide Web zur Schau stellt, wie leichtfertig heute Vieles preisgegeben wird, was früher ganz selbstverständlich in den schützenswerten Bereich der Privatsphäre gefallen wäre. klicksafe stellt deshalb mit dem Zusatzmodul „Datenschutz und Persönlichkeitsrechte im Web" Informationen und Arbeitsmaterialien für Lehrerinnen und Lehrer zur Verfügung, mit denen das Thema im Unterricht erarbeitet werden kann.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Datenschutz_klicksafe.pdf



Social Communities – Ein Leben im Verzeichnis

Social Networks, wie z. B. schülerVZ, wer-kennt-wen oder Lokalisten boomen. Sie treffen mitten in die Bedürfnisse junger Menschen nach Kommunikation, nach Selbstfindung, nach Darstellung, nach Peer-Group-Erlebnissen, nach Freiräumen, nach Grenzteststungen und -überschreitungen, um nur einige zu nennen. Sie bieten damit einen chancenreichen Bewegungsraum, der jedoch nicht ohne Risiken ist. klicksafe stellt deshalb mit dem Zusatzmodul „Social Communities – Ein Leben im Verzeichnis" Informationen und Arbeitsmaterialien für Lehrerinnen und Lehrer zur Verfügung, mit denen das Thema im Unterricht erarbeitet werden kann.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Social_Communities.pdf



Was tun bei Cyber-Mobbing?

Unter Cyber-Mobbing versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mit Hilfe moderner Kommunikationsmittel. Das Zusatzmodul bietet zahlreiche Hilfestellungen und Materialien, mit denen zentrale Fragen rund um das Thema „Cyber-Mobbing" im Unterricht bearbeitet werden können: Was versteht man eigentlich unter Cyber-Mobbing? Wer ist von Cyber-Mobbing betroffen und was kann man eigentlich dagegen tun?

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Cyber-Mobbing.pdf



Das klicksafe-Lehrerhandbuch

Das **klicksafe-Handbuch „Knowhow für junge User"** ist eine praxisnahe Einführung in die weiten Felder der Online- und Netzkommunikationen.

Aufbauend auf dem Konzept und den Erfahrungen der klicksafe-Lehrerfortbildungen bietet es für Lehrer und Multiplikatoren eine Fülle von sinnvollen Hilfestellungen und praxisbezogenen Tipps für den Unterricht. Entscheidend ist, dass die Einheiten leicht verständlich sind und eine vorherige Schulung oder Fortbildung nicht notwendig ist. Zu jedem Jugendmedienschutz-Thema bietet das Handbuch Unterrichtseinheiten (d. h. Arbeitsblätter zum Kopieren) in verschiedenen Schwierigkeitsgraden an.

Link zum Download:
http://www.klicksafe.de/service/fuer-lehrende/lehrerhandbuch/



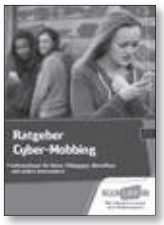
Handreichung zur Durchführung von Elternabenden: Computerspiele

Die **Handreichung „Elternabende Computerspiele"** bietet **Referentinnen und Referenten** das nötige Rüstzeug, um medienpädagogische Elternabende in den Bereichen Computer-, Online- und Konsolenspiele sowie Mobile Gaming anzubieten.

Sie ist eine direkte Erweiterung der klicksafe-Handreichung „Elternabende Internet + Handy", die seit 2009 bundesweit erfolgreich genutzt wird. Ende August 2015 ist die Handreichung in vollständig aktualisierter 2. Auflage erschienen.

Für die vorliegende Handreichung hat der **Spieleratgeber-NRW** – ein Angebot der Fachstelle für Jugendmedienkultur NRW – seine Expertise und seine Erfahrung eingebracht. Darüber hinaus wurden erneut die praktisch erprobten Konzepte der **Initiative Eltern+Medien** aufgegriffen, welche seit Jahren Elternabende zum Thema „Computerspiele" anbietet.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_HR_Computer/HR_Computerspiele_klicksafe.pdf



Ratgeber Cyber-Mobbing
Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte

Durch Soziale Netzwerke, Video-Portale, Messenger-Apps und andere Online-Angebote, die Austausch, Kommunikation und Vernetzung zum Ziel haben, ist das Internet in vielerlei Hinsicht zum Abbild der Gesellschaft geworden. Und so findet man online bei allen Vorteilen auch problematische Aspekte wieder, die aus dem realen Leben bekannt sind – zum Beispiel Mobbing. Da dieses Phänomen vergleichsweise neu ist und sich laufend weiterentwickelt, gibt es hier noch viele Unsicherheiten.

Dieser Ratgeber stellt Besonderheiten, Funktionen, Auslöser und die Verbreitung von Cyber-Mobbing vor und behandelt das Thema Cyber-Mobbing in den Medien. Darüber hinaus wird erläutert, ob Cyber-Mobbing strafbar ist und wie man Cyber-Mobbing im schulischen und familiären Umfeld vorbeugen oder anhand bestimmter Warnzeichen so früh wie möglich erkennen kann. Im Kapitel „Was tun bei Cyber-Mobbing?" werden Möglichkeiten vorgestellt, gegen Cyber-Mobbing vorzugehen. Die bei Cyber-Mobbing über Smartphones und Apps geltenden Besonderheiten werden hier ebenfalls vorgestellt. Drei Experteninterviews beleuchten die rechtlichen Möglichkeiten sowie die psychologischen Aspekte und Folgen von Cyber-Mobbing und geben Ratschläge für Betroffene und Angehörige. Die Linktipps am Ende der Broschüre bieten weiterführende Informationen zum Themenfeld.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Elternratgeber_Cybermobbing.pdf



Datenschutz-Tipps für Jugendliche – So sind Deine Daten im Internet sicher

Der Flyer „Datenschutz-Tipps für Jugendliche – So sind Deine Daten im Internet sicher" klärt Jugendliche darüber auf, welche Folgen die unbedachte Weitergabe und Verbreitung persönlicher Daten im Internet haben kann. Neben grundlegenden rechtlichen Rahmenbedingungen werden Sicherheits-Tipps vorgestellt. Außerdem zeigt der Flyer auf, wie man sich als „Datenprofi" in Sozialen Netzwerken verhält. Auch der faire Umgang mit den Daten anderer wird behandelt. Konkrete Tipps, wie man bei Datenschutzverletzungen reagieren sollte einschließlich der Nennung kompetenter Ansprechpartner für alle Fragen zum Thema Datenschutz runden den Flyer ab.

Link zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Jugendliche/klicksafe_Flyer_Datenschutztipps_Jugend_2013.pdf



klicksafe to go
Datensatz – Datenschatz: Warum Datenschutz und Sicherheit wichtig sind.

klicksafe to go ist ein neues Format, in dem aktuelle medienpädagogisch relevante Themen aufgegriffen und für Schule und Unterricht kompakt aufbereitet werden. Nur zum Download und als PDF erhältlich. Die zweite Ausgabe der Reihe „klicksafe to go" unterstützt Pädagogen dabei, Jugendliche für einen bewussten und sicheren Umgang mit ihren Daten im Netz zu sensibilisieren und Maßnahmen zum Selbstdatenschutz zu ergreifen.

Link zum Download:
http://www.klicksafe.de/klicksafe-to-go



Mobile Medien – Neue Herausforderungen

Die Unterrichtsreihe „Mobile Medien – Neue Herausforderungen" von klicksafe und Handysektor bietet kurze Unterrichtseinheiten zu den Themen Handynutzung und Herausforderungen bei der Nutzung mobiler Medien vor dem Hintergrund der Omnipräsenz von Smartphones und Internetzugang. Aufbauend auf dem Konzept und den Erfahrungen der klicksafe-Unterrichtsmaterialien bietet die Reihe für Lehrer und Multiplikatoren eine Fülle von sinnvollen Hilfestellungen und praxisbezogenen Tipps für den Unterricht. Entscheidend ist, dass die Einheiten leicht verständlich sind und eine vorherige Schulung oder Fortbildung nicht notwendig ist. Jedes Material dieser Reihe bietet drei Stundenentwürfe (d. h. Arbeitsblätter zum Kopieren), die auf den Erklärvideos von Handysektor basieren und sich einem ausgesuchten Thema widmen.

Link zum Download:
https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/Selfies_Sexting_Selbstdarstellung_Mobile_Medien_3.pdf

Ausgezeichnet als „Ausgewählter Ort 2011" für Aufklärungsarbeit an Schulen

Die Initiative „Datenschutz geht zur Schule" (DSgzS) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. hat die Sensibilisierung von Schülerinnen und Schülern der Klasse 5 bis zu Berufsschülern im Umgang mit dem Internet und modernen Kommunikationsmedien zum Ziel. Die Initiative ist seit Anfang 2010 mit verschiedenen Unterrichtskonzepten für Schülerinnen und Schüler der verschiedenen Altersklassen bundesweit unterwegs, um ihnen einfache Verhaltensregeln für den sensiblen Umgang mit ihren persönlichen Daten im Netz näher zu bringen.

In Vorträgen, die sich über zwei Schulstunden erstrecken, werden Schülerinnen und Schüler der Sekundarstufe I und II anhand von praxisnahen Beispielen und unter Einsatz von Filmbeiträgen zu einem verantwortungsvollen und bewussten Umgang mit personenbezogenen Daten angehalten. Für die Schulen fallen für diesen ehrenamtlichen Einsatz keine Kosten an (außer Übernahme der Fahrtkosten).

Das Modell der externen Experten für dieses Themengebiet hat sich bewährt und wird durch andere Organisationen erfolgreich übernommen. Gleichwohl ist der Bedarf an der Vermittlung dieser Kernkompetenz ungebrochen und die Nachfrage an Dozenteneinsätzen besteht nach wie vor. Wir kommen diesen Anfragen gerne nach.

Dies geschieht mit großem Erfolg: Es wurden bereits mehr als 80.000 Schülerinnen und Schüler im Umgang mit ihren persönlichen Daten sensibilisiert. Rund 50 ausgebildete Dozenten übernehmen ehrenamtlich die Aufklärungsarbeit an den Schulen.

Die Initiative „Datenschutz geht zur Schule"

- deutschlandweit aktiv
- Sensibilisierungsveranstaltungen im Umgang mit persönlichen Daten
- abgestimmte Sensibilisierungskonzepte für Schülerinnen und Schüler der Sekundarstufen I und II sowie für Berufsschüler, Eltern und Lehrer
- fachkundige, geprüfte, ehrenamtlich tätige Dozenten
- keine Kosten für Schulen oder Schüler (ggf. Fahrt- und Reisekosten)
- Preisträger des Wettbewerbs „365 Orte im Land der Ideen"
- regelmäßiges Durchführen von Aktionstagen, seit 2012 Teilnahme am Safer Internet Day

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

DSgzS – Die Initiative „Datenschutz geht zur Schule“ des BvD e. V.

DATEV-Stiftung Zukunft –
Gemeinnützige Stiftung zur Förderung und Fortentwicklung
von Maßnahmen in den Bereichen IT und Datenschutz,
Finanz-, Steuer- und Rechtswesen sowie
Genossenschaftswesen

klicksafe wird kofinanziert
von der Europäischen Union

Kontakt zur Initiative DSgzS

Initiative „Datenschutz geht zur Schule“, BvD e. V.
Rudi Kramer, Sprecher
Frank Spaeing und Riko Pieper, stellv. Sprecher

Budapester Straße 31
10787 Berlin
Tel.: (030) 26 36 77 62
E-Mail: dsgzs@bvdnet.de
Web: www.bvdnet.de/dsgzs