„Meine Daten gehören mir“

Eine Unterrichtseinheit zum Thema Datenschutz

Zielgruppe: Schüler/innen der 4. - 6. Klasse

Zeitlicher Rahmen: mind. 2 Schulstunden, 90 Min.

Inhalt

Die SuS befassen sich mit dem Thema Datenschutz im Netz. Ausgehend von ihren eigenen Nutzungsgewohnheiten und -erfahrungen werden sie für die Schutzwürdigkeit ihrer Daten im Internet sensibilisiert. Sie erfahren, welche Bedeutung persönliche Daten für die Nutzung von Onlineplattformen oder auch Apps spielen und welche Folgen ein unvorsichtiger Umgang mit persönlichen Daten nach sich ziehen kann. Dabei wird insbesondere auch das Recht am eigenen Bild beleuchtet. Außerdem lernen die SuS, wie sie sich vor der ungewollten Weitergabe oder gar dem Missbrauch ihrer persönlichen Daten im Netz schützen können, z.B. durch sichere Passwörter.

Lernziele

didaktische Analyse, Kompetenzen, die erlernt werden sollen:

- Verstehen, welche Daten schützenswert sind und wie man seine Daten im Netz schützen kann
- Kennenlernen von Folgen des Datenmissbrauchs
- Wissen, verstehen und anwenden, was man beim Teilen von Fotos im Netz beachten muss (Recht am eigenen Bild)
- Erkennen, warum Passwörter sicher sein müssen und wissen, wie man sich ein sicheres Passwort erstellt

Verlaufsplan

Phase/ Thema	Inhalt	Sozial-/Arbeitsform	Medien/ Material	Zeit
Einstieg	Was macht ihr im Internet am liebsten? Wie geht ihr ins Internet? (Smartphone, Tablet, Computer/Laptop, Spielekonsole etc.)	Offene, kurze Fragerunde	PPT Folien 1-2	5 Min.

	Warm-up: Was wisst ihr über Apps?	Zuordnungsspiel Kurze Beratung in 2er-Teams, Ergebnisse sammeln im Plenum	Fakten (s. **Anlage 1_ Zuordnungsspiel**) Pin-/ Magnetwand/ Tafel, Pinnadeln oder Magnete	10 Min.
Thema 1 Datenschutz und Privatsphäre	Einführung: Datenschutz	Input/ Präsentation	PPT Folien 3-4	5 Min.
	Was ist öffentlich? Was ist privat?	Kurze Beratung in 2er-Teams, Ergebnisse sammeln im Plenum	Pinnwand/Magnet-wand/Tafel Kärtchen „privat“, „öffentlich“, „nicht eindeutig“ Pinnadeln oder Magnete Je nach Anzahl der 2er-Teams Kärtchen mit Beispielen personenbezogener Daten (s. **Anlage 2_Privat vs. Öffentlich**)	15 Min.
	Video „Charlie und das Geheimnis der Daten“ Was kann passieren, wenn man zu viele Daten von sich im Internet preisgibt?	Plenum Stopp bei 1:05 – Frage an die SuS: Was glaubt ihr – woher weiß er das alles? Stopp bei 2:05 – Frage an die SuS: Was glaubt ihr – was könnte passieren?	PPT Folie 5 Link zum Video: https://www.kindersache.de/bereiche/juki/charlie-und-das-geheimnis-der-daten	5 Min.
	Zusammenfassung der Folgen	Input/ Präsentation	PPT Folie 6-9	5 Min.
Thema 2 Fotos im Netz – Das Recht am eigenen	Einführung: Das Recht am eigenen Bild	Input/ Präsentation	PPT Folie 10	5 Min.
	Beispielhafte	Plenum	PPT Folien 11-13	5 Min.

Bild	Situationen bewerten 3 Bilder – „Darf ich das posten?“ – Begründung und Erfahrungsaustausch			
	Wissen anwenden und vertiefen: Darf ich das im Netz veröffentlichen?	Einzelarbeit, anschließend gemeinsame Auswertung im Plenum	Anlage 3_Arbeitsblatt Fotos im Netz Anlage 4_Lösung_Arbeitsblatt Fotos im Netz	15 Min.
Thema 3 Passwörter	Einstieg: Die beliebtesten Passwörter	Frage ans Plenum: Was glaubt ihr, sind die beliebtesten Passwörter?	PPT Folie 14	2 Min.
	Warum sind Passwörter wichtig?	Input/ Präsentation	PPT-Folie 15	3 Min.
	Optional: Wenn Computer oder Tablets zur Verfügung stehen. Wissen anwenden: Ein gutes und ein schlechtes Passwort ausdenken und online prüfen	2er-Teams	PPT-Folie 16 (mit Link zu www.checkdeinpasswort.de) Laptops (je 1 Gerät für 2 SuS) oder Smartphones der SuS	10 Min.
Abschluss	Was packt ihr in euren Datenschutzkoffer ein?	Offene Frage	PPT-Folie 17	5 Min.

Einstieg

Kurze offene Fragerunde mit allen SuS:

→ *Was macht ihr im Internet am liebsten?* **[FOLIE 2]**
→ optional: *Wie geht ihr ins Internet?*
(Smartphone, Tablet, Computer/Laptop, Spielekonsole etc.)

Zuordnungsspiel: Was wisst ihr über Apps?

Mit dem Spiel können die SuS bereits vorhandenes Wissen aktivieren und sich darüber austauschen. An die Tafel oder auf Moderationskarten werden die Namen folgender Apps geschrieben und angepinnt:

- YouTube
- WhatsApp
- Instagram
- TikTok

Die SuS werden in 2er-Teams (jeweils mit Banknachbar/in) eingeteilt und erhalten jeweils einen Fakt zum Thema Apps (siehe **Anlage 1_Zurodnungsspiel**). In den Kleingruppen beratschlagen sich die SuS kurz, auf welche der vier Apps dieser Fakt zutrifft. Anschließend werden die Fakten nach und nach von jeder Gruppe im Plenum vorgestellt und entsprechend der vorgenommenen Zuordnung zu einer der Apps an der Tafel, Magnet- oder Pinnwand angebracht.

Thema 1: Datenschutz und Privatsphäre

Datenschutz – was ist das? [FOLIE 3]

- Datenschutz heißt, Daten sollen geschützt werden.

- (optionale) Frage an die SuS → *Was glaubt ihr, warum sollten Daten im Internet geschützt werden?*

- Es gibt Gesetze in Deutschland, die verhindern sollen, dass eure Daten einfach an andere Menschen verteilt werden. Ein Arzt darf z.B. nicht einfach jemandem erzählen, was er sich beim letzten Besuch über euch aufgeschrieben hat. Seit 2018 gibt es auch ein Gesetz dazu, dass besonders die Daten von Kindern im Internet geschützt werden müssen (EU-Datenschutzgrundverordnung). Das besagt Folgendes: Seid ihr jünger als 16 Jahre, so müssen immer erst eure Eltern/ Erziehungsberechtigten ihre Einwilligung geben, bevor eure Daten im Netz weitergegeben werden dürfen.

- Meist geht es beim Datenschutz um persönliche Daten.

- (optional) Frage an die SuS → *Was sind eigentlich "persönliche Daten"?* (2 bis 3 Beispiele sammeln)

- Dies sind alle Informationen, die etwas über eine Person verraten. Es gibt persönliche Daten, die eine Person direkt bestimmbar machen (z.B. Name, Adresse). Und es gibt persönliche Daten, die weitere Informationen über euch verraten, die nicht einzigartig/einmalig sind, wie zum Beispiel euer WhatsApp-Chatname oder auch eure Augenfarbe. Dennoch sind auch dies Informationen über eure Person!

Übung: "Was ist öffentlich? Was ist privat?"

- Einstiegsfragen an die SuS
  → *(Wo) musstet ihr schon einmal im Internet persönliche Daten angeben?*
  → *Was bedeutet für euch „privat", was bedeutet „öffentlich"?*

- Die SuS finden sich in 2er-Teams zusammen und erhalten jeweils ein Beispiel für persönliche Daten (siehe **Anlage 2_Privat vs. Öffentlich**).

- Ziel: Die SuS sollen anhand vorgegebener Beispiele in 2er-Teams über ihre (individuelle) Grenze von privaten und öffentlichen Daten diskutieren. Diese sollen wiederum einem der (an der Tafel/Magnet-/Pinnwand vorbereiteten) Bereiche „Privat", „Öffentlich", „Nicht eindeutig" zugeordnet werden.

- Die Ergebnisse werden im Klassengespräch gesammelt, an der Tafel/Wand angebracht und diskutiert.

- Leitfrage: Welche Daten sollten im Internet (also bspw. auf Plattformen wie Instagram oder YouTube, aber auch über Messenger wie WhatsApp) ganz privat bleiben und nicht geteilt werden? Welche Daten darf man im Netz eventuell weitergeben?

- Wichtig für die Auswertung im Klassenverband: Die Grenze zwischen privaten und öffentlichen Daten kann und darf individuell sein. Bei der Übung geht es in erster Linie um Einschätzungen aufgrund eigener Erfahrungen und Befindlichkeiten. Es gibt hier keine richtigen oder falschen Lösungen. An einigen Stellen wird eine eindeutige Zuordnung schwierig sein. Vielmehr geht es um eine gemeinsame Diskussion der Beispiele, die wiederum zur Sensibilisierung der SuS für die Schutzwürdigkeit persönlicher Daten beitragen soll.

Datenspuren im Netz

- Wie ist das jetzt aber genau mit den Daten im Internet? **[FOLIE 4]**

  Wenn du durch den Schnee stapfst, hinterlässt du Spuren. Auch wenn du im Internet surfst, hinterlässt du Spuren: deine Daten.

- Warum ist das so? Und warum sind eure Datenspuren im Netz so interessant?

  → Unternehmen und Firmen (wie zum Beispiel Google, Facebook oder Amazon) interessieren sich für deine Daten. Überlege mal Folgendes: Du lädst mit deinem Vater eine App auf das Tablet oder das Smartphone. Dabei kommt ein Hinweis: Die App (und damit der Hersteller der App) möchte zum Beispiel wissen, wo du immer gerade bist. Manchmal ist dies für die Funktion der App notwendig. Oft aber auch nicht.

- Was will der Hersteller aber mit deinen Daten?

  → Manche möchten schlicht und einfach wissen, was dich interessiert. Und was dich in Zukunft interessieren könnte. Und so bekommst du Empfehlungen für weitere, ähnliche Apps oder Produkte. Sie zielen genau auf deine Interessen. Und sie beeinflussen dich dann bei der Auswahl neuer Apps oder Produkte. Das nennt man „personalisierte Werbung".

Filmclip: Charlie und das Geheimnis der Daten [FOLIE 5]

Das Kind Charlie begegnet einer unheimlichen Gestalt, die verblüffend viel über es weiß. Schnell wird klar woher: Charlie hat im Internet unbedarft den Namen und die Adresse verraten, Auskunft über Hobbys und Freunde erteilt und noch einiges mehr. Am Ende des Clips ist Charlie schlauer.

- **Stopp bei Minute 1:05**

  → *Frage an die SuS: Was glaubt ihr, woher weiß die unheimliche Gestalt das alles über Charlie?*

- **Stopp bei Minute 2:05**

  → *Frage an die SuS: Was könnte denn passieren, wenn man zu viele Daten über sich im Internet preis gibt?*

Folgen – Was kann passieren, wenn man zu viele Daten über sich preisgibt?

Zusammenfassung der Folgen für Charlie gemeinsam im Plenum [FOLIE 6]

- Partys: Ungewollt öffentlich
- Fotos im Netz: Kann jeder weiterverbreiten
- Ungeschützte Passwörter: Bestellung von Produkten im fremden Namen

Deine Daten sind kostbar [FOLIE 7]

- Ist etwas kostenlos, „bezahlst" du häufig mit den eigenen persönlichen Daten. Besonders wenn du Apps installierst, gibst du viele persönliche Daten an.

  ➔ Beispiel 1: WhatsApp

  Die App ist ein fleißiger Datensammler. Wer WhatsApp installiert, sendet das Telefonbuch mit Namen der Kontakte an das Facebook-Unternehmen. Verschickt man über die App Fotos, dann tritt man die Rechte an das Unternehmen ab. Man stimmt also zu, dass WhatsApp sie verwenden darf. Die App hat auch Zugriff auf die Fotos und Videos. Das sind auch Gründe, weshalb die App erst ab 13 Jahre erlaubt ist – aber nur mit Zustimmung der Eltern. Ohne Einverständnis der Eltern ist WhatsApp erst ab 16 Jahren erlaubt. Kontrolliert wird das Alter allerdings nicht.

  ➔ Beispiel 2: Android Betriebssystem

  Google-Handys senden ständig den Standort, wo man sich aufhält. So könnte sich kinderleicht ein Bewegungsprofil von dir erstellen lassen.

- E-Mail-Adressen werden für Werbung gesammelt – viele unerwünschte Mails, also Spam, können die Folge sein. Die verstopfen das Postfach.

- TIPP: Wenn man eine App installiert, sollte man genau hinschauen, was man anklickt. Was kann man zulassen und was ablehnen? Die Frage sollte man sich immer stellen. Ist der Zugriff dieser App auf die Fotos wichtig? Und auf die Handykamera? Oftmals genügt es, wenn man auf „Ablehnen" klickt.

E-Mails [Folie 8]

Wenn man bedenkenlos überall seine E-Mail-Adresse angibt, dann:

- Kann man viel **Spam** erhalten. Diese unerwünschte Werbung müllt das eigene E-Mail-Postfach zu, was sehr ärgerlich ist.

- **Phishing-Mails**: Das sind Betrugmails, bei denen Vorsicht geboten ist. Es gibt sie in verschiedenen Arten, die mitunter nicht leicht zu erkennen sind. Oftmals soll man einen Anhang öffnen oder einen Link anklicken. Dahinter kann sich ein Virus verstecken, der das Handy oder den Computer ausspioniert oder schädigt. Phishing-Mails können täuschend echt sein – meist geben sich die Absender für eine bekannte Firma aus, manchmal wird ein Gewinn versprochen.

- **Konto hacken**: Wer ein einfaches Passwort für den Login in sein E-Mail-Postfach verwendet, braucht sich nicht zu wundern, wenn Fremde es hacken und sich einloggen können. Ziel ist es oftmals, Spamattacken über das gehackte Mailkonto zu versenden. Das muss man nicht unbedingt mitbekommen. Es kann auch strafbare Taten, wie Phishing, einschließen.

Communitys [Folie 9]

- **Identitätsklau:** Jemand gibt sich als andere (reale) Person im Internet aus. Sie erstellt also im Namen einer anderen Person ein Profil in einer Community. Sie kann über das Profil Lügen verbreiten, Fotos teilen und Dinge liken oder weiterverbreiten (Beispiel TikTok und Instagram).

- Identitätsklau bedeutet auch, wenn jemand unter falschem Namen etwas in Online-Shops bestellt. Das ist eine Straftat.

- **Profilklau:** Leichte Passwörter, die etwas über dich verraten, sind schnell herausgefunden. So kann sich ganz einfach jemand in deinen Account einloggen und sich für dich ausgeben und zum Beispiel Lügen über dich verbreiten oder dumme und schlimme Dinge posten, die du nicht willst.

- **Mobbing über das Internet**: wird auch "Cybermobbing" genannt. Es ist eine schlimme Art von Mobbing, weil die Mobber oft anonym sind und somit die Hemmschwelle niedriger liegt. Für Mobbingopfer ist es besonders schlimm, weil es sie überall hin verfolgt. Oft bekommen es viele der Mitschüler und Mitschülerinnen mit, weil sie in derselben Community sind. Cybermobbing kann jederzeit stattfinden und ist unüberschaubar. Identitätsklau und Profilklau ist eine besonders schwere Art von Cybermobbing.

Thema 2: Das Recht am eigenen Bild

Fotos oder Videos mit Anderen [FOLIE 10]

Jeder Mensch hat das Recht am eigenen Bild. Das bedeutet, dass jede und jeder selbst bestimmen darf, ob ein Foto von ihr oder ihm gemacht wird oder nicht. Das Recht am eigenen Bild besagt außerdem, dass Bilder und Videos nur dann veröffentlicht und verbreitet werden dürfen, wenn die abgebildete Person **eingewilligt** hat. Das heißt, bevor ich ein Foto oder Video über z.B. Instagram, YouTube oder auch WhatsApp teile oder verschicke, muss ich alle Personen, die darauf zu sehen sind, **um Erlaubnis fragen**. Gleichzeitig schützt es aber auch mich, denn es darf niemand ein Bild von mir teilen oder verschicken, ohne dass ich zugestimmt habe.

Es gibt aber auch Ausnahmen. Beispiele:

- Sind Personen Beiwerk auf einem Foto, das heißt nur zufällig und sehr klein z.B. auf einem Bild einer Sehenswürdigkeit oder einer Landschaftsaufnahme, dann kann das Bild in der Regel ohne Erlaubnis veröffentlicht werden.
- Ist der oder die Abgebildete eine Person des öffentlichen Interesses, darf er oder sie in der Öffentlichkeit (nicht in privaten Situationen!) auch fotografiert werden, also beispielsweise Politiker/innen, Sportler/innen, Schauspieler/innen, Musiker/innen usw.

- Ist die auf dem Foto abgebildete Person Teil einer Menschenmenge, zum Beispiel auf Demonstrationen oder Konzerten, dürfen die Fotos auch ohne Einwilligung weiterverbreitet werden.

Ein absolutes **Verbot** ist, jemanden **heimlich** zu filmen oder zu fotografieren. Das verbietet ein Gesetz (§ 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen). Ein Foto oder Video, das jemanden in einer peinlichen Situation zeigt, darf man nicht machen und besitzen. Und erst recht nicht ins Internet stellen oder jemand anderem schicken. Damit verletzt man die Privatsphäre. Jeder Mensch und jedes Kind hat ein **Recht auf Privatsphäre**. Das ist auch in der UN-Kinderrechtskonvention (Artikel 16) festgeschrieben.

Wird gegen diese Rechte verstoßen, macht man sich strafbar – und das kann teuer werden.

3 Beispielbilder – Darf ich das posten?

„Selfies“ (Handy-Selbstporträt) FOLIE 11

Viele finden es witzig, sich selbst zu fotografieren. Das Foto ist dann auch mal schnell auf das Handy vom Freund geschickt. Manche finden es auch cool, sich selbst zu filmen und dabei Dinge zu erzählen. Das kannst du natürlich machen, doch überlege dir gut, ob das auch fremde Menschen sehen sollten. Wenn andere Personen, zum Beispiel dein bester Freund/ deine beste Freundin mit auf dem Foto zu sehen ist, musst du vor dem Posten oder Verschicken um Erlaubnis fragen.

FOLIE 12

Fotos oder Videos **am Strand** in **Badehose** oder **Bikini** sind vielleicht eine schöne Urlaubserinnerung für das Fotoalbum. Doch im Internet haben sie nichts zu suchen.

FOLIE 13

Fotos können per App oder **Bildbearbeitungsprogramm** schnell bearbeitet und verändert werden. Ein Foto, das jemanden lächerlich darstellt, darf keinesfalls im Netz geteilt oder weiter verbreitet werden. Auch nicht, wenn die Person in dem Moment zustimmt. Denn manche Dinge können einem auch erst Jahre später peinlich sein. Das Netz vergisst nämlich nichts.

Übung Arbeitsblatt „Darf ich das Bild im Internet veröffentlichen?“

Die SuS erhalten jede/r das Arbeitsblatt (siehe **Anlage 3_Arbeitsblatt Fotos im Netz**) mit Beispielsituationen unter der Fragestellung, ob in dieser Situation ein Foto veröffentlicht werden darf oder nicht und kreuzen jeweils ihre Antwort an(„Ja“, „Kommt drauf an“ oder „Nein“).

Im Klassenverband werden die Ergebnisse zusammengetragen und begründet.

Auflösung: siehe **Anlage 4_Lösung_Arbeitsblatt Fotos im Netz**

Zusammenfassung:

Überlege dir sehr gut, was du alles von dir im Internet erzählst und zeigst. Manche Dinge können dir im Nachhinein vielleicht peinlich sein oder andere können sie falsch verstehen. Am besten ist es, **möglichst wenig von sich im Netz zu zeigen**. Auch wenn du denkst, dass du ein Bild nur mit einem Freund teilst - das Foto kann schnell weitergeleitet werden. Und so kursiert ein heikles Foto von dir im Internet herum und alle lachen…

Zusatzinfos:

- Ein prima **Videoportal für Kinder** ist www.kindersache.de. Hier prüfen Erwachsene zunächst, ob das Video veröffentlicht werden kann. Sie achten genau darauf, dass die Filme nicht zu viel Privates preisgeben.

- **Checkliste** zum Thema **„Bilder ins Internet stellen“** auf Kindersache: https://www.kindersache.de/bereiche/wissen/medien/check-bilder-ins-internet-stellen

Thema 3: Passwörter - Mach dein Passwort sicher!

Kurze, offene Fragen an die SuS:

→ *Was glaubt ihr, sind die beliebtesten Passwörter?*
→ *Wo werden Passwörter genutzt?*

- Beliebte und gleichzeitig unsichere Passwörter sind [FOLIE 14]:
    - 123456
    - passwort
    - hallo
    - hallo123
    - 111111

Einführung: Warum sind sichere Passwörter wichtig? [FOLIE 15]

Passwörter sind eine Art Geheimsprache, ein Code für deine persönlichen Daten. Sie stellen so etwas wie einen Schlüssel zum Schloss dar. Hinter dem Schloss verbirgt sich dein Schatz. Es ist dein Schatz – deine Daten, die geschützt werden müssen. Gute und sichere Passwörter sind darum sehr wichtig. Man nutzt sie zum Einloggen ins Mailkonto, in Communitys, auf dem Handy. Erwachsene haben noch viel mehr Passwörter, die benötigen sie zum Online-Banking und zum Einkaufen in Online-Shops. Ein Passwort muss immer ein Geheimnis bleiben, du darfst es niemandem verraten.

Wie kann ich ein sicheres Passwort erstellen? [FOLIE 16]

Ein sicheres Passwort:

- hat mindestens 8 Zeichen.
- enthält Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (wie z. B. +, / oder ?!).
- beinhaltet keine persönlichen Daten (wie z.B. dein Name oder dein Geburtsdatum).
- ist streng geheim - du solltest es also niemandem verraten.
- ist nirgendwo aufgeschrieben. Du solltest es dir also gut merken können.

Merkhilfe: Denk dir einen Satz aus und nimm die ersten Buchstaben jeden Wortes, um dein Passwort zu erstellen.

Beispiel: „Um 17 Uhr läuft meine Lieblingssendung."

Passwort: „U17Ulm<3s"

Optional:

Gruppenarbeit + Auswertung [FOLIE 17]

- Wissen anwenden: Die SuS bilden 2er-Teams und denken sich jeweils ein sicheres und ein unsicheres Passwort aus. Diese Passwörter können sie online überprüfen: www.checkdeinpasswort.de

Abschluss und Auswertung [FOLIE 18]

Offene Fragen an die SuS:

→ *Was packt ihr heute in euren Datenschutzkoffer ein?*
→ *Welche Infos/ Hinweise/ Tipps nehmt ihr mit, wenn ihr das nächste Mal im Netz unterwegs seid?*