SICHER IM DIGITALEN
STARKE MÄDCHEN. STARKE ZUKUNFT.

gefördert von
Bundesministerium
Frauen, Wissenschaft
und Forschung

JOHANNES KEPLER
UNIVERSITÄT LINZ

MEINE DATEN IM NETZ:
NUTZUNGSBEDINGUNGEN & KONSEQUENZEN

Welche Daten teile ich online, was regeln die Nutzungsbedingungen und welche Folgen hat das Weiterleiten fremder Inhalte?

LEHRER*INNEN-HANDREICHUNG

Tags: #Datenschutz, #Nutzungsbedingungen, #Rechtliches, #Medienkompetenz

Materialien:	Schulstufe:	Dauer:
Interaktive Tools (Mentimeter), Videos, Arbeitsblätter, Beamer, Smartphones	4. bis 7. Schulstufe	3 bis 4 Unterrichtseinheiten

Ziele:

EH	Ziele der Unterrichtseinheit
1	➔ Schüler*innen verstehen, welche personenbezogenen Daten Plattformen erfassen. ➔ Sensibilisierung für Datenweitergabe und Datenschutz im Alltag. ➔ Reflexion: Unterschiede zwischen den Daten, die man Freunden preisgibt, und denen, die Plattformen erhalten. ➔ Einführung in Nutzungsbedingungen und erste kritische Auseinandersetzung damit.
2	➔ Kenntnis der Grundprinzipien der DSGVO und deren Schutzfunktion. ➔ Verständnis des Geschäftsmodells sozialer Medien: „Wenn es gratis ist, bist du das Produkt“. ➔ Reflexion über die Risiken personenbezogener Daten, z. B. personalisierte Werbung, Weitergabe an Dritte.
3	➔ Anwendung des Gelernten auf konkrete rechtliche und moralische Fallbeispiele. ➔ Verständnis des Rechts am eigenen Bild und der Konsequenzen von Datenweitergabe. ➔ Reflexion über Cybermobbing, Manipulation und altersgerechte Nutzung von Social Media. ➔ Sicherung des Gelernten durch Diskussion und Zusammenfassung.

Ablauf:

1.EH	Privatsphäre und Nutzungsbedingungen (50 min)
1.1	<u>Einstieg / Awareness</u> ➔ Leitfrage: Wie peinlich wäre es mir, wenn eine fremde Person meine Verläufe sehen könnte? ➔ Mentimeter-Umfrage: Abfrage der persönlichen Datenabgabe (Name, Geburtsdatum, unbewusste Daten wie Spotify-Profil). => Vergleich mit aktuellen Studien zur Nutzung. (saferinternet) => Warum haben sich die Schüler*innen so entschieden?
1.2	<u>Einführung: Personenbezogene Daten</u> ➔ Kurzes Video: Privatsphäre (2 min) Fokus auf den Begriff personenbezogene Daten. ➔ Vorstellung des Spotify-Steckbriefs durch LP: ➔ Welche Daten geben wir ungewollt preis ➔ (z.B. Musikpräferenz, Podcasts)?
1.3	<u>Gruppenarbeitsphase: Nutzungsbedingungen</u> ➔ Gruppeneinteilung nach genutzten Plattformen (max. 4 Pers.): ◆ *Snapchat, TikTok, Instagram, Google/YouTube, WhatsApp, Discord, Roblox.* ➔ Analyse der Nutzungsbedingungen in Gruppen (mind. 1 Nutzer*in pro Gruppe sinnvoll). (Arbeitsblätter); Steckbrief ausfüllen; Vorstellung des Steckbriefs vorbereiten

2.EH	Datenschutz (DSGVO & Geschäftsmodelle) (50 min)
2.1	<u>Einstieg & Ergebnissicherung</u> ➔ LP wiederholt Aufgabe ➔ Vorstellung der Gruppenergebnisse im Plenum: Informationen aus den Nutzungsbedingungen der Plattformen anhand des ausgefüllten Steckbriefs.
2.2	<u>Reflexion und Überleitung</u> ➔ Diskussion: Mindestalter (Datenschutz, aber auch Manipulation/Cybermobbing). ➔ Überleitung zur DSGVO: So viele gespeicherte Daten → Schutzbedarf → EU führt DSGVO (2018) ein.
2.3	<u>Geschäftsmodell Social Media</u> ➔ Einführung: Geschäftsmodell Social Media ("Wenn es gratis ist, bist du das Produkt"). ➔ Artikel: Das Geschäftsmodell von Social-Media-Unternehmen: https://www.bpb.de/themen/medien-journalismus/soziale-medien/545978/das-geschaeftsmodell-von-social-media-unternehmen/ ➔ Beispiele: Personalisierte Werbung, Verkauf an Dritte. ➔ Wichtiger Hinweis: Daten sind auch nach Löschung der Profile oft noch gespeichert.
2.4	<u>Arbeitsphase - DSGVO</u> ➔ Bearbeitung des Arbeitsblattes zum Erklärvideo über die DSGVO: https://youtube.com/watch?v=DIjTZ5DqGmY

3.EH	Fallbeispiele & Recht am eigenen Bild (50 - 100 min)
3.1	<u>Einstieg / Vorbereitung</u> ➔ Triggerwarnung erklären (Hinweis auf heikle Inhalte in Fall 1-2). ➔ Verweis auf Hilfestellungen in Österreich ➔ Arbeitsblätter austeilen.
3.2	<u>Lesen, Gruppen/Einzelarbeit & Plenumsdiskussion</u> ➔ Lesen des/der ausgewählten Fallbeispiele(s) (Fall 1 und/oder Fall 2). ➔ Moderierte Diskussion im Plenum anhand der Fragen ➔ Fokus auf Konsequenzen und moralische/rechtliche Aspekte
3.3	<u>Fazit & Sicherung</u> ➔ Zusammenfassung und Schlusswort: Klärung der wichtigsten rechtlichen Grundlagen und Konsequenzen (z. B. Recht am eigenen Bild, Weiterleitung ist strafbar). ➔ Klärung offener Fragen.

1. Privatsphäre und Nutzungsbedingungen (50 Minuten)

1.1 Einstieg / Awareness

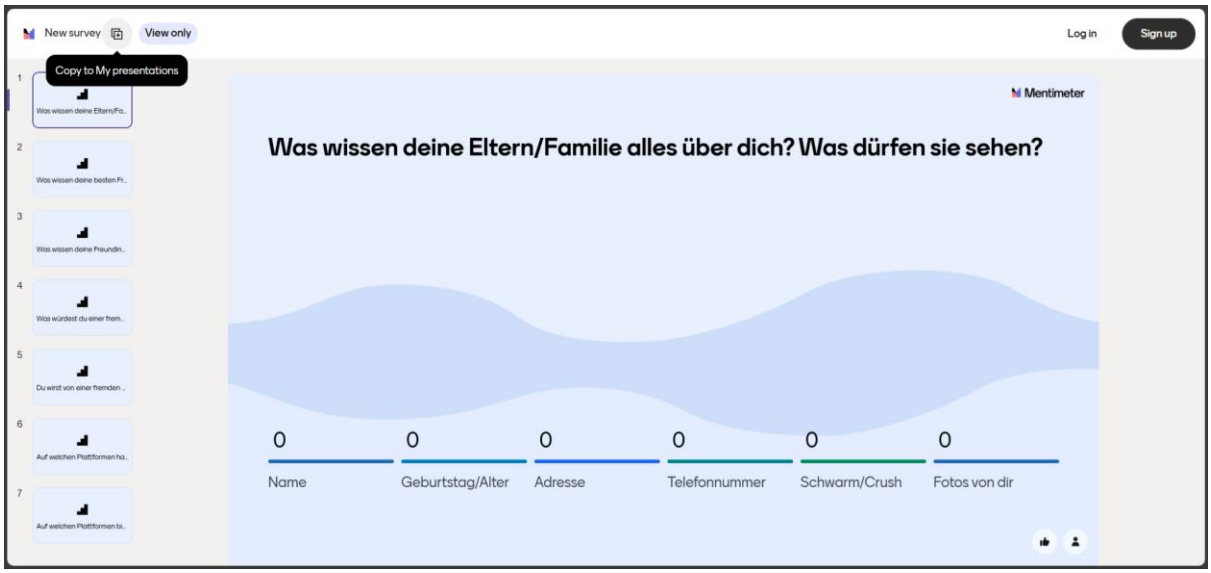
Dieser Abschnitt der Handreichung zeigt Ihnen, wie Sie die interaktive Präsentationssoftware wie beispielsweise Mentimeter oder Pingo in Ihrem Unterricht nutzen können. Sie erfahren, wie Sie auf eine vorbereitete Mentimeter-Vorlage zugreifen und diese an Ihre eigenen Bedürfnisse anpassen können. Folgen Sie einfach den untenstehenden Schritten.

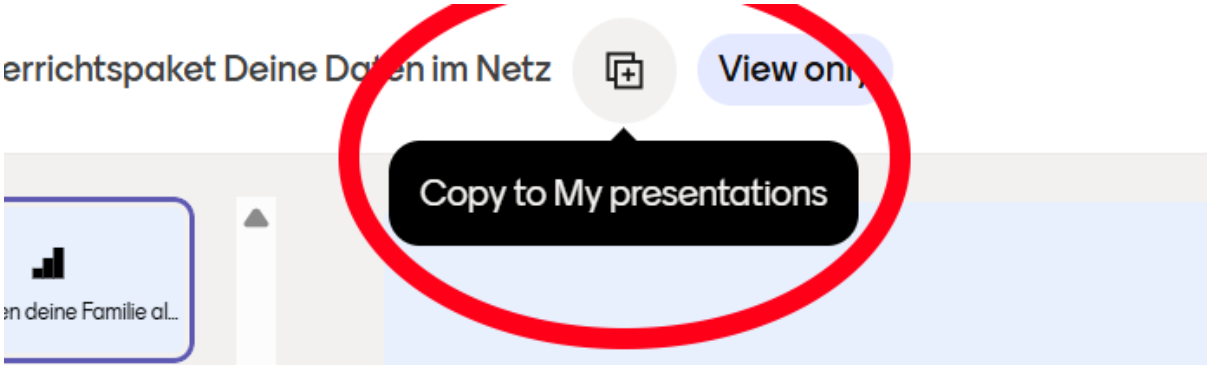
Präsentationsmöglichkeiten im Klassenzimmer:

Mentimeter

Sie rufen folgenden Link auf:
https://www.mentimeter.com/app/presentation/al3pkj29k9ji6cgcw57xxowxu8s54i85

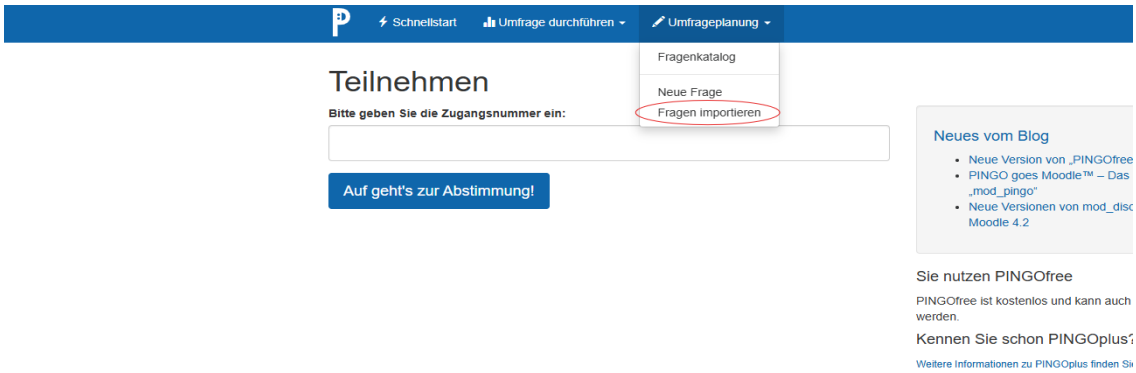
Sie sehen das Mentimeter und müssen es nur mehr zu Ihren eigenen Präsentationen hinzufügen. Dafür muss nur der Button neben dem Namen der Mentimeter-Umfrage geklickt werden. (Siehe Screenshot) Wenn die Lehrkraft die Umfrage zu ihren Präsentationen hinzugefügt hat, kann sie sie nach Belieben verändern. Der Link ist eine *View Only* Berechtigung, das heißt, es kann nichts an der Vorlage bearbeitet werden.



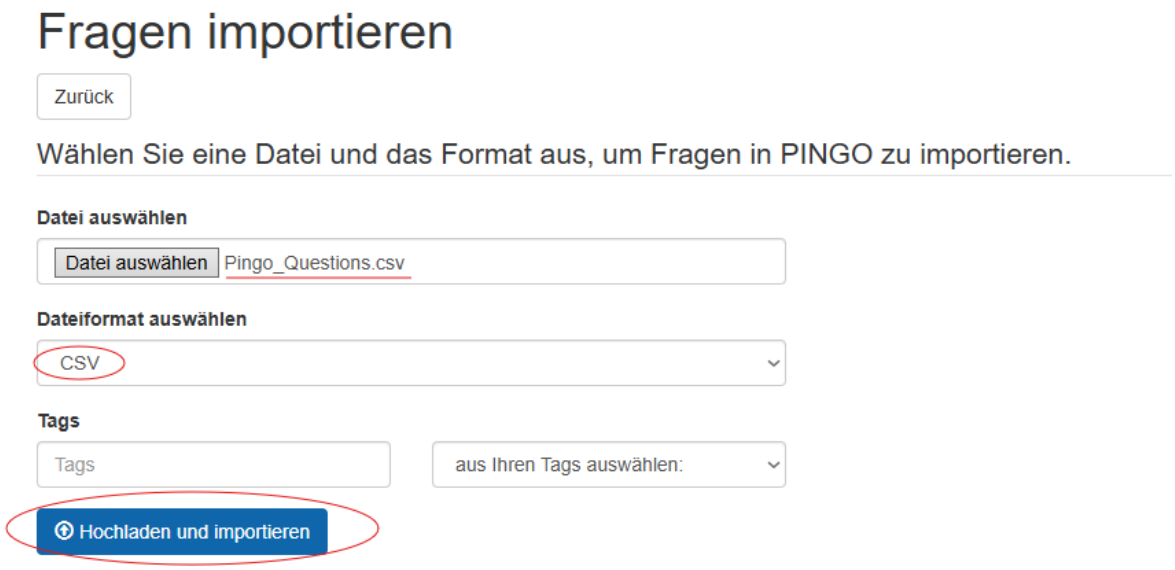


Pingo

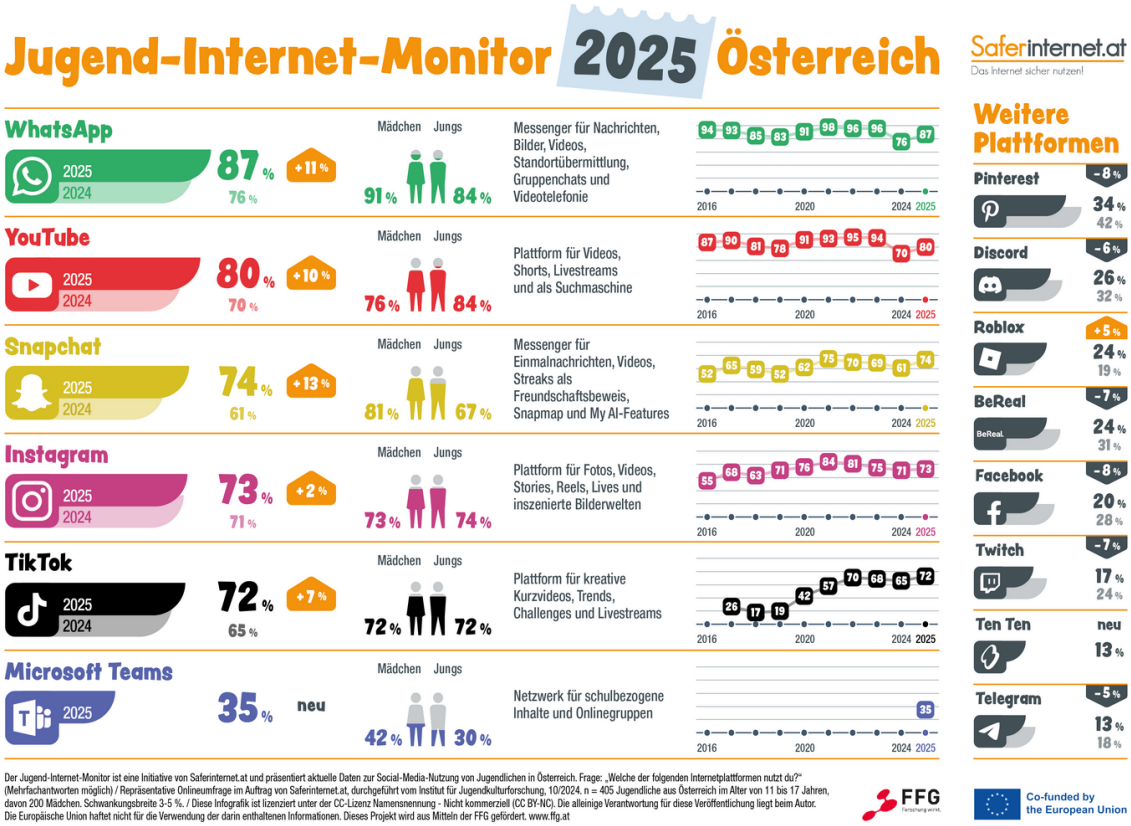
Alternative zu Mentimeter:
https://pingo.coactum.de
Anleitung für die Fragen:
Besuchen Sie https://pingo.coactum.de und loggen Sie sich ein (registrieren, falls noch kein Account besteht). Anschließend oben unter “Umfrageplanung” auf “Fragen importieren” klicken.



Anschließend ist diese Seite sichtbar. Laden Sie auf der Seite die Datei “pingo_questions.csv” (zu finden in der **COOL Lab Materialbörse**) hoch, wählen Sie “CSV” als Dateiformat aus und klicken Sie anschließend auf “hochladen und importieren”. Sie können vor dem Hochladen optional auch die Fragen einem Tag zuweisen.



Anschließend müssen Sie nur noch eine Session starten. Die Schüler*innen können der Session über einen Session-Code beitreten. Es ist möglich, die Fragen live in die Session zu integrieren (jede Frage einzeln).



https://www.saferinternet.at/services/jugend-internet-monitor

1.2 Einführung: Personenbezogene Daten

Kurzes Video über Datenschutz (1.2) (ca. 2 min) https://youtu.be/Uziy7ghMeJE

(Alles safe? Datenschutz einstellen in Apps - App+on | ZDFtivi)

Das Video zeigt, wie voreingestellte App-Berechtigungen unnötig viele Daten sammeln können und erinnert daran, Privatsphäre-Einstellungen regelmäßig zu prüfen und zu deaktivieren, was man nicht teilen möchte.

Stellen Sie nun den ausgefüllten Steckbrief Spotify vor.

Welche Daten könnten wir unbewusst ungewollt preisgeben? (z.B. Musikpräferenz über öffentliches Spotify Profil) Welche Daten darf Spotify verwenden?

Vorbereitung auf Arbeitsblätter zu Nutzungsbedingungen (Kleingruppen)

Anschließend Ergebnissicherung im Plenum

1.3 Gruppenarbeitsphase: Nutzungsbedingungen

Arbeitsblätter zu den Nutzungsbedingungen.

Die Nutzungsbedingungen legen die Regeln und Richtlinien fest, die bei der Nutzung der jeweiligen Plattformen gelten. Sie enthalten wichtige Informationen zu den Rechten und Pflichten der Nutzer*innen sowie zu den Einschränkungen und Verantwortlichkeiten. Ziel ist es, die Nutzer*innen/Schüler*innen und Lehrpersonen über die Bedingungen der Nutzung zu informieren und sicherzustellen, dass sie diese verstehen und einhalten.

Snapchat: https://www.snap.com/terms

TikTok: https://www.tiktok.com/legal/page/eea/terms-of-service/de

Instagram: https://www.tiktok.com/legal/page/eea/terms-of-service/de

YouTube: https://www.youtube.com/t/terms

WhatsApp: https://www.whatsapp.com/legal/terms-of-service-eea?lang=de

Roblox: https://en.help.roblox.com/hc/de/articles/115004647846-Nutzungsbedingungen-von-Roblox#user-terms

Sonstige nützliche Links:

- https://justdeleteme.xyz/ (eine Sammlung an Direktlinks, um Accounts zu löschen)
- https://tosdr.org/de (Terms of services didn't read)

2. **Datenschutz** - **DSGVO & Geschäftsmodelle** (50 Minuten)

2.1 Einstieg & Ergebnissicherung

Vorstellung der Gruppenergebnisse im Plenum.

Die Datenschutzbestimmungen beschreiben, wie die jeweiligen Plattformen persönliche Daten der Nutzer erheben, speichern, verwenden und schützen. Ziel ist es, Transparenz über den Umgang mit personenbezogenen Daten zu schaffen und die Nutzer*innen, v.a. Minderjährige und deren Erziehungsberechtigte über ihre Rechte in Bezug auf Datenschutz informieren.

Snapchat: https://values.snap.com/privacy/privacy-policy?lang=de-DE

TikTok: https://www.tiktok.com/legal/page/eea/privacy-policy/de

Instagram: https://privacycenter.instagram.com/policy/

YouTube: https://policies.google.com/privacy?hl=de

WhatsApp: https://www.whatsapp.com/legal/privacy-policy-eea#privacy-policy-information-we-collect

Roblox: https://en.help.roblox.com/hc/de/articles/115004630823-Roblox-Datenschutz-und-Cookie-Richtlinie

2.2 Reflexion und Überleitung

Überleitung zur Datenschutzgrundverordnung (nächste Stunde):

- Die LP geht auf die Problematik ein, dass sehr viele Daten gespeichert werden → daher hat die EU die DSGVO 2018 ins Leben gerufen, um Personen besser zu schützen

2.3 Geschäftsmodell Social Media

https://www.bpb.de/themen/medien-journalismus/soziale-medien/545978/das-geschaeftsmodell-von-social-media-unternehmen/ (*Das Geschäftsmodell von Social-Media-Unternehmen | Soziale Medien – wie sie wurden, was sie sind | bpb.de*)

Der Artikel erklärt, wie Sozial-Media-Plattformen ihr Geld verdienen: Sie bieten Infrastruktur für Kommunikation und Inhalt und wandeln die Aufmerksamkeit und Daten der Nutzer*innen in Wert um. Dabei basiert ihr Geschäftsmodell vor allem auf personalisierter Werbung, dem Handel bzw. der Analyse von Nutzerdaten und zunehmend auf Zusatzangeboten wie Premium-Abos, In-App-Käufen oder Kooperation mit Influencer*innen.

2.4 Arbeitsphase - DSGVO

Video DSGVO: (ca. 8 min) https://www.youtube.com/watch?v=DIjTZ5DqGmY

(*EU-Datenschutz-Grundverordnung (DSGVO): Was erwartet dich? | Rechtsanwalt Christian Solmecke*)

Die DSGVO vereinheitlicht ab 2018 das europäische Datenschutzrecht und ersetzt in Deutschland u. a. das BDSG und datenschutzrelevante TMG-Regeln, wodurch Unternehmen umfassende neue Pflichten treffen. Besonders betroffen sind Cookie-Einwilligungen (klares Opt-in), interne Datenschutzprozesse wie Folgenabschätzungen sowie die weiterhin strengen Anforderungen an Datenschutzbeauftragte.

3. Fallbeispiele & Recht am eigenen Bild (50 - 100 min)

3.1 Einstieg / Vorbereitung

Triggerwarnung erklären (Hinweis auf heikle Inhalte in Fall 1-2).

Verweis auf Hilfestellungen in Österreich.

3.2 Gruppen/Einzelarbeit & Plenumsdiskussion

Arbeitsblatt austeilen und lesen. Anschließend Fragen im Plenum beantworten.

Sie haben als Lehrperson nun die Auswahl von 2 Arbeitsblätter zu zwei echten Fallbeispielen. Diese Fälle stammen direkt aus der Gerichtspraxis (Landesgericht Steyr, Österreich und einem deutschen Verwaltungsgericht) und wurden für diese Unterrichtseinheit didaktisch aufbereitet.

Ziel dieser Leseaufgaben und der anschließenden Gruppen - und Plenumsdiskussion ist es, den Schüler*innen die praktische Bedeutung von Gesetzen wie dem Recht am eigenen Bild und den Strafen bei Cyber-Mobbing oder Sexting zu vermitteln. Die Einheit soll nicht nur aufklären, sondern die Jugendlichen auch dazu befähigen, digitale Verantwortung zu übernehmen und in kritischen Situationen (z. B. bei Fake-Profilen oder der Weiterleitung von Stickern) die richtigen Entscheidungen zu treffen.

Hinweise für die Durchführung:

Triggerwarnung vorlesen. Einzel- oder freiwillige Partnerarbeit ermöglichen; keine persönlichen Erfahrungen einfordern. Klare Meldewege benennen (Lehrkraft, Schulsozialarbeit, Eltern) und lokale Beratungsstellen bereithalten.

Fokus: Rechtslage (Recht am eigenen Bild), Selbstschutz und Hilfewege. Plenum sensibel moderieren (respektvolle Sprache, keine Schuldzuweisungen), Time-out ermöglichen. Optional: anonyme Fragenbox und ggf. Nachgespräch anbieten.

Fallbeispiele

Arbeitsblatt	Schlagworte	Beschreibung
„Meine Rechte und Grenzen im Internet“	Intimsphäre „Sexting“ und falsche Freunde	In diesem Teil geht es um den Schutz der persönlichsten Daten: Nacktbilder und die eigene Privatsphäre.
„Der Lehrer als WhatsApp-Sticker“	Schule, Respekt - Recht am eigenen Bild	In diesem Teil geht es um Konflikte im Schulalltag und die Frage, ob private Chats wirklich rechtsfreie Räume sind.

3.3 Fazit & Sicherung

Egal ob es um intime Fotos oder lustige Sticker geht – für beides gelten im Internet die gleichen Grundregeln:

1. Das Internet vergisst nichts: Screenshots und Weiterleitungen machen Inhalte unkontrollierbar.
2. Weiterleiten ist Täter-Sein: Wer illegale oder verletzende Inhalte teilt, macht sich strafbar und verletzt Rechte.
3. Unwissenheit schützt nicht: „Das war nur Spaß“ oder „Ich wusste das nicht“ verhindert keine Strafe.

Schwierige Begriffe im Unterricht – Social Media und digitale Themen

Diese Handreichung bietet Lehrpersonen eine Übersicht über häufig verwendete, aber oft schwer verständliche Begriffe aus der digitalen Welt und sozialen Medien. Ziel ist es, Lehrkräfte dabei zu unterstützen, diese Begriffe im Unterricht verständlich zu erklären und so die Medienkompetenz der Schüler*innen zu fördern.

Die Handreichung enthält Definitionen und Beispiele zu Begriffen, die in sozialen Medien wie Snapchat, TikTok, YouTube und WhatsApp häufig vorkommen. Sie soll dazu beitragen, Missverständnisse zu vermeiden und den Schüler*innen ein besseres Verständnis für die digitale Welt zu vermitteln.

Im Folgenden finden Sie eine Sammlung von Begriffen, die in sozialen Medien und im digitalen Kontext eine wichtige Rolle spielen, sowie einfache Erklärungen und Beispiele, die Sie direkt in Ihrem Unterricht verwenden können.

- Community:
  Eine Community ist eine Gemeinschaft von Menschen, die sich in sozialen Medien zu einem bestimmten Thema, Interesse oder Ziel zusammenschließen.

  In Snapchat bezeichnet die Community die Gemeinschaft aller Nutzer*innen, die über die App miteinander in Kontakt stehen.

  Diese kann aus Freund*innen, Followern oder auch regionalen Gruppen bestehen, die gemeinsame Interessen teilen (z. B. durch öffentliche Storys oder Themenfilter).

  Beispiel: Jugendliche aus einer Schule, die sich gegenseitig ihre Snaps schicken oder eine „Campus Story“ teilen, bilden eine Snapchat-Community.

- Hosten:
  „Hosten“ bedeutet, Inhalte oder Daten auf einem Server bereitzustellen, damit sie im Internet zugänglich sind.

Wenn jemand einen Snap (Foto oder Video) hochlädt, wird dieser auf den Servern von Snapchat gespeichert – also gehostet.

Snapchat sorgt dafür, dass die Inhalte an Freund*innen ausgeliefert werden und nach einer bestimmten Zeit automatisch verschwinden.

Beispiel: Ein Snap, der an eine Gruppe geschickt wird, wird kurzzeitig auf Snapchats Servern gespeichert, bevor er gelöscht wird.

- Lizenz:

Eine Lizenz ist die Erlaubnis, etwas zu nutzen – z. B. ein Bild, Musikstück oder Software.

In sozialen Medien regelt die Lizenz, wer welche Inhalte verwenden oder weiterverbreiten darf.

Beispiel: Ein Foto unter der „Creative Commons"-Lizenz darf unter bestimmten Bedingungen geteilt werden.

Durch die Nutzung von Snapchat stimmen Nutzer*innen zu, dass das Unternehmen eine Lizenz erhält, ihre Inhalte zu verwenden (z. B. für technische Zwecke, Speicherung oder Analyse).

Das heißt: Wer einen Snap erstellt, bleibt Eigentümer*in, aber Snapchat darf den Inhalt im Rahmen seiner Dienste nutzen.

Beispiel: Wenn jemand eine öffentliche Story postet, darf Snapchat diese anzeigen, verbreiten oder archivieren – innerhalb der Plattformregeln.

- Serviceanbieter:

Ein Serviceanbieter (oder Dienstanbieter) ist ein Unternehmen, das Dienstleistungen erbringt oder Produkte verkauft. Meistens sind die digitalen Dienste oder die Bereitstellung von Plattformen.

Snap Inc., das Unternehmen hinter Snapchat, ist der Serviceanbieter.

Es stellt den Dienst, die App und die Infrastruktur zur Verfügung, die Nutzer*innen verwenden.

Beispiel: Wenn Lehrkräfte Snapchat für Medienbildung thematisieren, ist Snap Inc. der Dienstanbietende, der auch für Datenschutz, Nutzungsbedingungen und Sicherheit verantwortlich ist.

- Drittanbietende:

Ein/Eine Drittanbietende/r ist ein/eine externe/r Anbietende/Anbietender, der zusätzlich zu einem Hauptdienst Funktionen oder Inhalte bereitstellt.

Ein/Eine Drittanbietende*r ist ein externer Dienst, der in Snapchat integriert ist oder mit Snapchat-Daten arbeitet.

Snapchat nutzt z. B. Drittanbietende für Filter, Spiele, Werbung oder Analysefunktionen.

Beispiel: Wenn ein Linsen-Filter von einem externen Entwickler*innen stammen oder Werbeanzeigen über ein anderes Unternehmen eingeblendet werden, sind das die Drittanbietenden.

- Unterlizenzierbar:

Wenn eine Lizenz unterlizenzierbar ist, bedeutet das:

Das Unternehmen oder die Person, die eine Lizenz erhalten hat, darf die Nutzungsrechte weitergeben – also anderen ebenfalls erlauben, das Werk zu nutzen.

Beispiel: Eine Schule lizenziert eine Software, die sie auch Schüler*innen oder Partnern weitergeben darf.

- ## Feed:
  Ein Feed ist der persönliche Nachrichtenstrom oder die Startseite in einer Social-Media-App.

  Dort werden Beiträge, Fotos, Videos oder Storys angezeigt, die von anderen Nutzer*innen oder Seiten stammen, denen man folgt — oder die die Plattform als interessant vorschlägt.

  Beispiel: TikTok zeigt in der „Für dich"-Seite (Feed) Videos, die auf das eigene Nutzungsverhalten abgestimmt sind.

- ## Botnets:
  Ein Botnet (Kurzform von Robot Network) ist ein Netzwerk aus vielen Computern, Smartphones oder anderen Geräten, die heimlich miteinander verbunden sind – oft ohne, dass die Besitzer*innen es wissen.

  Diese Geräte werden durch Schadsoftware (Bots) ferngesteuert und führen Befehle eines Angreifers oder einer Angreiferin aus.

- ## Scraper:
  Ein Scraper ist ein Computerprogramm oder eine Software, die automatisch Daten aus Webseiten oder Apps ausliest und sammelt.

  Das Wort stammt vom englischen „to scrape" = abschaben oder herauskratzen – also: Informationen automatisch „herausholen".

  Unterschied zu Crawler: ein Crawler indexiert einfach Seiten, er "crawlt" durch das ganze Internet, sammelt irgendwelche Daten und indexiert die Webseiten. Ein Scraper "crawlt" auch durch das Internet, jedoch sucht er auf jeder Website spezielle Informationen, welche er extrahiert und sammelt.

- ## Malware:
  Malware ist die Abkürzung für „malicious software" – also schädliche Software.

  Darunter versteht man Programme oder Dateien, die absichtlich entwickelt wurden, um Computern, Smartphones oder Netzwerken zu schaden oder sie zu manipulieren.

- ## Tantieme:
  Eine Tantieme ist eine Geldzahlung, die Urheber*innen (also z. B. Künstler*innen, Musiker*innen, Autor*innen oder Fotograf*innen) erhalten, wenn ihre Werke genutzt oder weiterverwendet werden.

  Das Wort stammt aus dem Französischen tant pour cent („so viel Prozent") – es geht also meist um eine prozentuale Beteiligung am Gewinn oder an den Einnahmen.

- ## Reverse Engineering:
  Reverse Engineering bedeutet, ein fertiges Produkt — z. B. eine Software, eine Datei oder ein Protokoll — rückwärtszuanalysieren, um zu verstehen, wie es funktioniert, wie es aufgebaut ist oder welche Daten es verarbeitet. Statt von Quellcode aus einem Programm zu bauen, nimmt man das fertige Produkt auseinander (gedanklich oder technisch), um seine Strukturen, Formate oder Algorithmen nachzuvollziehen.

Überblick Platformen

Plattform	Hauptsitz (Land)	Zuständige Einheit (EU/EEA)	Gerichtsbarkeit / Nutzungsbedingungen	Datenschutz & Datenübertragung	Ende-zu-Ende-Verschlüsselung	Schutzmaßnahmen (intern & empfohlen)	Altersschutz-Regelungen
Snapchat (Snap Inc.)	USA (Santa Monica, CA)	Snap Group Ltd (UK/EU)	Regionale TOS, Streitigkeiten nach Land; Snap Inc. US-Recht für viele Märkte	Datentransfer in/aus USA, Standardklauseln für EU; US CLOUD Act (USA darf auf Daten, welche in der EU gespeichert sind, zugreifen, solange die Firma ihren Hauptsitz in den USA hat, auch wenn Tochterfirmen den Sitz wo anders haben) möglich	Keine durchgängige E2E	Zwei-Faktor-Authentifizierung, Screenshot-Benachrichtigung, Privatsphäre-Optionen für Stories; empfohlen: „Nur Freunde"-Modus aktivieren	
TikTok (ByteDance)	China (Beijing) / globaler Sitz: Singapur	TikTok Ireland (EU), TikTok UK (GB)	TOS je nach Land; Irische Einheit für EU maßgeblich	EU-Daten oft in Irland/UK gespeichert, Übertragung nach China in der Kritik; DSGVO-Verstöße → Strafen (2025)	Keine E2E	Family Pairing (Eltern-Kontrolle), Bildschirmzeit-Limits, Inhaltsfilter; empfohlen: Privates Konto & „Nur Freunde"-Kommentare	Mindestalter 13; unter 16 eingeschränkte Funktionen (z. B. keine DMs), unter 18 keine Livestreams oder virtuelle Geschenke
Instagram (Meta)	USA (Menlo Park, CA)	Meta Platforms Ireland Ltd	EU-Vertrag über irische Einheit; US-/EU-Regelungen	Datentransfer in Meta-Konzern (USA ↔ EU); Meta subject to GDPR-Strafen	Teilweise E2E für DMs (in Rollout)	Privatsphäre-Kontrolle pro Beitrag, Blockieren/Einschränken, Filter für beleidigende Kommentare; empfohlen: „Privates Konto" & Sensitivity-Filter aktivieren	Mindestalter 13; unter 18 eingeschränkte Werbe-Targeting-Daten; Altersprüfung via KI-Foto oder Ausweis
YouTube (Google)	USA (Mountain View, CA)	Google Ireland Ltd (EU)	Regionale AGBs; Irische Einheit für EEA-Nutzer	Datenübertragung in Konzern; Nutzung zu Werbezwecken; Regulierung nach DSA/GDPR	Keine E2E	„Sicherer Modus", Eltern-App „YouTube Kids", Inhaltsbewertungssystem; empfohlen: Kinderkonto über „Family Link"	Mindestalter 13 (YouTube Main); YouTube Kids für <13, automatische Altersverifikation (z. B. via Geburtsdatum oder Ausweis)
WhatsApp (Meta)	USA (Menlo Park, CA)	WhatsApp Ireland Ltd (EU)	EU-spezifische AGB; EU-Gerichtsstand Irland	E2E-Verschlüsselung standardmäßig für Chats, Datenteilung mit Meta eingeschränkt; DSGVO-relevant	Ja – vollständig für Nachrichten & Anrufe	Zwei-Faktor-Authentifizierung, Fingerprint-Sperre, Selbstlöschende Nachrichten; empfohlen: Backup-Verschlüsselung aktivieren	Mindestalter 16 in EU (Meta passt an EU-DSGVO an); unter 18 keine Business- oder Werbefunktionen

Kompetenzen DigComp 2.3 AT

0 Grundlagen, Zugang und digitales Verständnis	**1 Umgang mit Informationen und Daten**	**2 Kommunikation, Interaktion und Zusammen-arbeit**	**3 Kreation, Produktion und Publikation**	**4 Sicherheit und nachhaltige Ressourcen-nutzung**	**5 Problemlösung, Innovation und Weiterlernen**
0.1 Konzepte der Digitalisierung verstehen	1.1 Daten, Informationen und digitale Inhalte recherchieren, suchen und filtern	2.1 Mithilfe digitaler Technologien kommunizieren	3.1 Inhalte und Objekte digital entwickeln	4.1 Geräte schützen	5.1 Technische Probleme lösen
0.2 Digitale Geräte und Technologien bedienen	1.2 Daten, Informationen und digitale Inhalte kritisch bewerten und interpretieren	2.2 Mithilfe digitaler Technologien Daten und Informationen teilen und zusammen-arbeiten	3.2 Inhalte und Objekte digital integrieren und neu erarbeiten	4.2 Personen-bezogene oder vertrauliche Daten sowie Privatsphäre schützen	5.2 Bedürfnisse und technologische Antworten darauf erkennen
0.3 Inklusive Formen des Zugangs zu digitalen Angeboten kennen, nutzen bzw. bereitstellen	1.3 Daten, Informationen und digitale Inhalte verwalten	2.3 Digitale Technologien für die gesellschaftliche Teilhabe verwenden	3.3 Werknutzungs-recht und Lizenzen beachten	4.3 Gesundheit und Wohlbefinden schützen	5.3 Kreativ und innovativ mit digitalen Technologien umgehen
0.4 Auseinander-setzung mit der Digitalität suchen und entsprechende Urteilsfähigkeit entwickeln		2.4 Ein- und Verkäufe durchführen	3.4 Programmieren und Abläufe automatisieren	4.4 Sich vor Betrug und Konsumenten-rechts-missbrauch schützen	5.4 Digitale Kompetenz-lücken erkennen und schließen
		2.5 Angemessene Ausdrucks-formen verwenden	3.5 Inhalte und Objekte digital in verschiedenen Öffentlichkeiten rechtskonform produzieren und publizieren	4.5 Umwelt schützen und IT nachhaltig betreiben	
		2.6 Die digitale Identität verstehen und gestalten			