Social Media

Privatsphäre & Selbstdatenschutz

Stiftung Medienpädagogik Bayern

Digitale Schule der Zukunft

Übersicht

E Grundlage

E Erweiterung

Stiftung Medienpädagogik Bayern

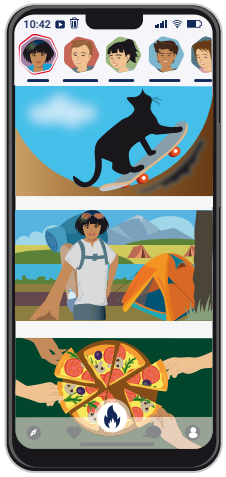
Digitale Schule der Zukunft

E
Grundlage

Was sind persönliche Daten?

Persönliche oder personenbezogene Daten sind sensible Daten, die eine Person erkennbar machen. Zu persönlichen Daten gehören z. B. Angaben auf dem Personalausweis, aber auch Hobbys und Vorlieben. Gerade die Kombination verschiedener persönlicher Daten macht es Außenstehenden und Fremden möglich, etwas über Verhaltensweisen und Vorlieben einer Person herauszufinden. Das bedeutet: Je mehr Daten man über sich selbst preisgibt, desto leichter macht man sich erkennbar und auffindbar. Das gilt vor allem im Internet, z. B. in Social-Media-Angeboten. Beispiele für persönliche Daten sind:

- Name
- Geburtsdatum
- Körpergröße
- KFZ-Kennzeichen
- Alter
- Konto-, Kreditkartennummer
- Geschlecht
- Augenfarbe
- Hobbys und Vorlieben



- Telefonnummer
- Wohnort
- Adresse
- E-Mail-Adresse
- Standort*
- Personalausweisnummer
- Genetische Daten, Krankendaten

* Bestimmte Apps und Social-Media-Angebote greifen z. B. auf GPS-Daten zu. Damit können sie den Aufenthaltsort nachvollziehbar machen und umfangreiche Bewegungsprofile erstellen.

Stiftung Medienpädagogik Bayern
Digitale Schule der Zukunft

Warum ist Selbstdaten-schutz wichtig?

Preisgabe von Daten

Viele Angebote im Internet, z. B. Social-Media-Angebote, ermöglichen es, sich selbst darzustellen, mit anderen auszutauschen und sich zu vernetzen. Wer die Angebote nutzen will, gibt persönliche Daten preis. Schon bei der Anmeldung werden viele Daten abgefragt, wie Name, Geburtsdatum, E-Mail und Telefonnummer. Im eigenen Profil möchte man anderen oft möglichst viele verschiedene Dinge von sich und dem eigenen Leben zeigen, um interessant zu wirken. Daher werden oft persönliche Daten preis-gegeben, die man in einem persönlichen Gespräch oder einer anderen Alltagssituation eher nicht gleich erzählen würde, wie Beziehungsstatus, Geschlechterzuordnung, sexuelle oder politische Orientierung oder Religionszugehörigkeit.

Spannungsfeld: Selbstdarstellung und Datenschutz

Besonders für Kinder und Jugendliche ist es schwierig, ihr Bedürfnis nach Selbstdarstellung und den Schutz der eigenen Privatsphäre unter einen Hut zu bringen.
Problem: Es ist ihnen oft nicht bewusst, welche Nachteile es für sie haben kann, wenn Fremde auf ihre Daten zugreifen.

Persönliche Daten – ein gutes Geschäft

Persönliche Daten sind wie Gold für die Betreiber von Social-Media-Angeboten. Markt-datenhändler, Internet-Tracking-Unternehmen und die Werbewirtschaft freuen sich über wertvolle Daten der einzelnen Nutzerinnen und Nutzer, wie Wohnort, Hobbys, Nutzungsgewohnheiten und vieles mehr. Diese Daten weiter zu verkaufen, ist ein sehr gutes Geschäft. Daher sollte man sich die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen der Angebote genau anschauen. Besonders die Anbieter vieler Apps von Spielen und Social-Media-Angeboten stehen hier in der Kritik. Dort müssen die Nutzerinnen und Nutzer oft in die Weitergabe ihrer Daten einwilligen, sonst können sie das Angebot nicht nutzen.

Spam?

Ihr Briefkasten enthält plötzlich viel mehr Werbesendungen oder Ihr E-Mail-Konto wird von Spam-Mails geflutet? Möglicherweise haben Sie Ihre Daten in einem unseriösen Online-Angebot preisgegeben und Ihre Daten wurden weiterverkauft.

Missbrauch von Daten

Im Internet hinterlässt man – oftmals unbemerkt – viele Spuren, die schwerwiegende Folgen haben können. Daten können durch Fremde missbraucht werden, wenn an einem Profil keine oder zu wenig Privatsphäre-Einstellungen vorgenommen wurden. Persönliche Informationen sind dann öffentlich und können leicht gestohlen und missbraucht werden. Doch auch mit den richtigen Privatsphäre-Einstellungen können Daten gestohlen werden, etwa wenn sich Hacker durch Sicherheitslücken auf der Plattform Zugriff verschaffen.

Identitätsdiebstahl

Eine besondere Form des Datenmissbrauchs ist der Identitätsdiebstahl. Hier gibt sich eine Person als eine andere aus. Dazu wird oft ein gefälschtes Profil (Fake-Profil) erstellt. Das Fake-Profil soll der eigentlichen Person schaden, z. B. wenn rufschädigende Nachrichten oder Bilder veröffentlicht werden. Oft werden mit dem Fake-Profil auch andere Nutzerinnen und Nutzer kontaktiert. Sie erkennen oft nicht, dass es nicht die richtige Person ist und geben ebenfalls persönliche Daten preis, die dann auch missbraucht werden.

Konto gehackt?

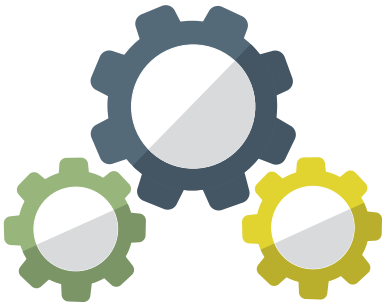
Durch Identitätsdiebstahl kann auch ein finanzieller Schaden entstehen, z. B. wenn Bezahl- oder Kontodaten gestohlen werden und Geld abgebucht wird. Oft reichen schon Name und Adresse eines Opfers aus, um beispielsweise etwas in seinem Namen online zu bestellen. Schauen Sie genau hin, bevor Sie Ihre Konto- oder Kreditkarten-Daten im Internet verwenden und prüfen Sie Ihre Kontoauszüge.

Sind gelöschte Daten wirklich weg?

Digitale Daten lassen sich sehr schnell weiterleiten, vervielfältigen und verbreiten. Sind sie erstmal online, kann man sie nicht mehr zurückholen: Das Internet vergisst nichts. Online gestellte Daten können auch nach Jahren wieder auftauchen, obwohl man sie eigentlich gelöscht hat. So können dann auch zukünftige Arbeitgeber oder neue Partnerinnen und Partner diese Daten abrufen. Auch wenn man den Datenschutz ernst nimmt, kann man nie sicher sein, dass Fotos und Informationen der eigenen Person nicht trotzdem irgendwo im Internet herumgeistern – z. B. eingestellt durch Freundinnen oder Freunde. Zum Schutz der Privatsphäre sollte man also grundsätzlich sparsam mit seinen Daten sein. Man sollte sich in jeder Situation fragen, was man wirklich von sich preisgeben möchte und ob es notwendig ist.

Wie lassen sich eigene Daten am besten schützen?

Der beste Schutz von Daten ist es, sie gar nicht erst zu veröffentlichen. Auf jeden Fall sollte man gerade mit persönlichen Daten wie Name, Adresse, Geburtstag oder Telefonnummer sparsam umgehen und sie nicht einfach so herausgeben. Fragt ein Angebot zu viele dieser Daten ab, sollte man sich überlegen, ob man es wirklich nutzen möchte. Manchmal gibt es auch datensparsame Alternativen. Generell gilt: Weniger ist mehr. Daten, die nicht online stehen, können auch nicht so leicht missbraucht werden.



Tipp

Privatsphäre-Einstellungen sollten unbedingt vorgenommen und regelmäßig überprüft und aktualisiert werden. Eine der wichtigsten Datenschutzfunktionen bei Social-Media-Angeboten ist die Sichtbarkeit. Eigene Daten sollten nicht öffentlich, sondern nur für ausgewählte Kontakte („Freunde“) sichtbar sein. Eine weitere Möglichkeit ist es, Zugriffsrechte von Apps einzuschränken. So kann geprüft werden, auf welche Daten eine App zugreifen kann und ob sie den Zugriff wirklich benötigt.

Weitere Informationen zum Thema Datenschutz sowie konkrete Tipps für technische Einstellungen finden Sie in der Broschüre **„Selbstdatenschutz! Tipps, Tricks und Klicks“** der Bayerischen Landeszentrale für neue Medien (BLM).

Quellenangabe

Der Text ist Bestandteil der bereits bestehenden Unterrichtseinheit „Liken, posten, teilen“ des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Unterrichtseinheit ist verfügbar unter: **www.medienfuehrerschein.bayern.** Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.

Daten verbergen und schützen

Social-Media-Angebote werden häufig genutzt, um sich mit anderen auszutauschen, sich zu informieren, unterhalten zu werden oder sich selbst bzw. die eigenen Hobbys und Interessen zu zeigen. Schon beim Anlegen eines Profils werden viele persönliche Daten abgefragt. Hier sollten nur die nötigsten Angaben gemacht werden. Die Felder, die man ausfüllen muss, sind oft mit einem „*“ gekennzeichnet.

Es ist wichtig, bei dem eigenen Profil auf die Privatsphäre-Einstellungen zu achten und sich vor jedem Post zu überlegen, wer diesen sehen soll. Falls Angaben und Daten voreingestellt öffentlich zu sehen sind, macht es Sinn, diese nur verändert, unvollständig oder gar nicht anzugeben.

Richtiger Name	Nicht den echten Namen nennen → **Nickname verwenden**
Geburtstag	Kein genaues Datum nennen → **z. B. nur den Monat angeben oder die Jahreszahl weglassen**
Adresse oder Wohnort	Niemals die konkrete Adresse nennen → **Nur die Stadt nennen (Stadtteil, Viertel oder Straßennamen weglassen)** → **Nur Bundesland oder Deutschland angeben**
Name und Adresse der Schule oder der Arbeitsstelle	Nicht den konkreten Namen und die Adresse der Schule oder Arbeitsstelle nennen → **Nur Schulart nennen oder Arbeitsfeld beschreiben, z. B. Mittelschule, Gymnasium oder Büro**
E-Mail-Adresse und Telefonnummer	Keine E-Mail-Adresse oder Telefonnummer angeben → **bzw., falls diese angegeben werden müssen, nicht auf öffentlich schalten**

Hobbys und Interessen, z. B. Freizeit-beschäftigungen	Keine konkreten Vereinsnamen, Orts- oder Zeitangaben, wie Wochentage oder Trainings-zeiten nennen → **Nur das Hobby allgemein nennen, z. B. Tanzen, Theaterspielen, Fußball**

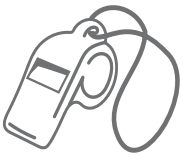
Auch Beschreibungen in Beiträgen oder auf Fotos oder Fotoinhalte lassen Rückschlüsse auf persönliche Daten zu. Daher sollte hier ebenfalls darauf geachtet werden, keine privaten Daten preiszugeben.

Zeit- und Ortsangaben (Aufenthaltsort)	Nicht (aktuell) posten → **Erst zeitverzögert posten, z. B. letzte Woche im Café etc.** → **GPS-Funktion des Smartphones deaktivieren,** wenn man sie nicht braucht. So können die Angebote kein Bewegungsprofil erstellen.
Bilder aus dem Alltag	Nicht posten, wenn durch den Inhalt persönliche Daten zu erschließen sind → **Bilder ohne klar erkennbare Merkmale oder Hinweise zu persönlichen Daten posten** (z. B. keine Informationen, die auf den genauen Aufenthalts- oder Wohnort hindeuten, wie Straßennamen, oder auf das Alter, z. B. Geburtstagskuchen mit Zahl)
Bilder mit anderen Personen	Personen auf dem Bild nicht verlinken oder taggen → **Bilder ohne Angaben zu den erkennbaren Personen posten** (Wichtig: Bild nur mit vorheriger Erlaubnis der erkennbaren Personen posten)

Ein einzelnes Bild, auf dem z. B. ein bekanntes Gebäude einer Stadt zu sehen ist, ist in Bezug auf die Privatsphäre noch kein großes Problem. Kritisch ist die Kombination von mehreren Bildern oder wenn regelmäßig Bilder eines Ortes gepostet werden. Das ermöglicht es anderen, konkrete Rückschlüsse z. B. auf einen beliebten Aufenthaltsort zu ziehen.

Quellenangabe

Medienführerschein Bayern: Liken, posten, teilen. Social-Media-Angebote hinterfragen und sicher nutzen. Internet: **www.medienfuehrerschein.bayern/Angebot/Sonderpaedagogische_Foerderung/5_6_und_7_Jahrgangsstufe/433_Liken_posten_teilen.htm** [Stand: 29.08.2022]



Handlungstipps

Wert von persönlichen und privaten Daten besprechen und klare Regeln vereinbaren

Erklären Sie Ihrem Kind den Wert von privaten Daten. Besprechen Sie gemeinsam, dass Daten auch missbraucht werden können, z. B. für unerwünschte Werbung und Spam, für Belästigung und Mobbing oder sogar Identitätsdiebstahl. Um Missbrauch zu vermeiden, können gemeinsame Regeln helfen, z. B. welche Daten geteilt werden oder welche Personen sie sehen dürfen. Machen Sie Ihrem Kind deutlich, dass es personenbezogene und persönliche Daten nicht ohne Rücksprache mit Ihnen herausgeben sollte.

Über AGB und Altersfreigaben von Social-Media-Angeboten informieren

Beim ersten Anmelden in Social-Media-Angeboten ist es wichtig, sich mit den Allgemeinen Geschäftsbedingungen (AGB) zu beschäftigen. Die wichtigsten Punkte sollten Sie mit Ihrem Kind besprechen. Erkundigen Sie sich z. B. vorab, ab welchem Alter das jeweilige Social-Media-Angebot genutzt werden darf. Viele Angebote geben ein Mindestalter vor. AGB sind jedoch in der Regel nicht sehr nutzerfreundlich aufbereitet – sehr lang, kompliziert geschrieben und schwer verständlich. In der **„Linkliste: Weiterführende Informationsangebote“** finden Sie für verschiedene Social-Media-Angebote die „Nutzungsbedingungen kurzgefasst“ von handysektor. Dort sind die wichtigsten Punkte übersichtlich aufbereitet. Die Betreiber können die AGB auch ändern. Daher kann es helfen, regelmäßig nachzusehen. Besprechen Sie mit Ihrem Kind, dass es Sie informiert, wenn der Anbieter auf AGB-Änderungen hinweist.

Möglichst wenig Daten preisgeben

Wer sich ein Profil in Social-Media-Angeboten anlegt, gibt in der Regel viele persönliche Daten an. Dabei ist es wichtig, nur die nötigsten Angaben zu machen. Angaben, die wirklich notwendig sind, sind mit einem „*“ gekennzeichnet. Vor allem persönliche Daten wie Nachname, Adresse, Geburtsdatum und Telefonnummer sollte man nur angeben, wenn sie für die Nutzung des Profils gebraucht werden. Auch der gewählte Nickname sollte keine Hinweise auf das Alter oder den Nachnamen enthalten.
Tipps, wie sich persönliche Daten verhüllen lassen, finden Sie im Bereich „Privatsphäre und Selbstdatenschutz“ in der **„Checkliste: Daten verbergen und schützen“**.

Alternative Angebote wählen

Fragt ein Angebot zu viele persönliche Daten ab, können Sie gemeinsam mit Ihrem Kind überlegen, ob es das Angebot wirklich nutzen muss. Manchmal finden sich zu bestimmten Angeboten auch datensparsame Alternativen. Ganz allgemein gilt bei der Preisgabe der eigenen Daten die Faustregel: Weniger ist mehr. Daten, die nicht online stehen, können nicht so leicht missbraucht werden.

Zugriffsrechte von Apps beschränken

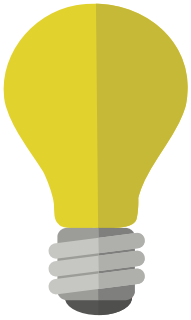
Bei der Installation und, je nach Betriebssystem, auch danach können Sie die Zugriffsrechte von Apps einschränken, z. B. das Taggen von Fotos mit GPS-Daten. Generell ist es sinnvoll, vor der Installation zu prüfen, auf welche Daten eine App zugreift und ob sie diese Zugriffsrechte wirklich benötigt. Falls eine App zu viele Zugriffsrechte fordert, können Sie überlegen, ob die App wirklich genutzt werden soll.

Privatsphäre-Einstellungen von Angeboten nutzen und regelmäßig überprüfen

Die meisten Social-Media-Angebote haben eigene Privatsphäre-Einstellungen. Z. B. kann man seine Daten vor der Öffentlichkeit verbergen und nur für ausgewählte Personen (den „Freunden“) sichtbar machen. Diese Einstellungen können bei der Weiterentwicklung eines Angebotes aber verändert werden, ohne dass die Nutzerinnen bzw. Nutzer informiert oder um ihre Einwilligung gebeten werden. Daher ist es wichtig, die Einstellungen regelmäßig zu überprüfen und bei Bedarf neu anzupassen. Privatsphäre-Einstellungen bieten zwar keinen 100-prozentigen Schutz vor Datenmissbrauch, doch das Risiko wird eingedämmt. Die Privatsphäre-Leitfäden von **saferinternet.at** u. a. für Snapchat, TikTok oder Instagram zeigen in Schritt-für-Schritt-Anleitungen, wie Sie mögliche Sicherheitseinstellungen vornehmen können.

Datenmissbrauch melden

Sind Sie oder Ihr Kind einem Datenmissbrauch zum Opfer gefallen, können Sie das beim jeweiligen Anbieter melden und dagegen vorgehen. Dafür sollten Sie Beweise sichern, z. B. mittels eines Screenshots. Bei Datenmissbrauch können Sie sich z. B. an die **Verbraucherzentrale** wenden. In schweren Fällen wie Identitätsdiebstal sollte Anzeige bei der **Polizei** gestellt werden.



Bereiche von Privatsphäre und Schutzmöglichkeiten

Privatsphäre ist nicht nur offline wichtig, sondern auch online, z. B. im eigenen Social-Media-Profil. Nicht alle Informationen sind im Internet gut aufgehoben und sollten online lieber geheim bleiben. Außerdem macht es einen Unterschied, ob man Daten und Informationen nur mit engen Bezugspersonen, dem engsten Freundeskreis oder mit einer breiten Öffentlichkeit teilt. Es gibt also unterschiedliche Bereiche von Privatsphäre, die jeweils geschützt werden sollten:

„Das können ruhig alle wissen."

z. B. Bilder von öffentlichen Orten oder Sehenswürdigkeiten (ohne Personen), Hobbys und Interessen (außer sie sind sehr privat)

So kann ich meine Daten schützen

z. B. Nutzungsbedingungen der Social-Media-Angebote lesen, nur in Ausnahmen Inhalte öffentlich teilen, sichere Passwörter verwenden, sparsam mit Daten umgehen

„Das erzähle ich Bekannten, aber Fremden nicht!"

z. B. Geburtstag, genaue Adresse, Telefonnummer, Standort/Aufenthaltsort, Schule/Arbeitsplatz, Lebenslauf, religiöse Ansichten, politische Einstellung, Engagement in Vereinen, Ehrenamt

So kann ich meine Daten schützen

z. B. bei Gruppen-Chats vorher prüfen, ob alle Mitglieder bekannt sind und eigene Beiträge sehen sollten, nur Kontakte hinzufügen, die man wirklich kennt oder vorher genau geprüft hat, Privatsphäre-Einstellungen prüfen und Sichtbarkeit der Inhalte einschränken (nur für Kontakte)

„Das erzähle ich nur meinen engsten Bezugspersonen/Freunden bzw. Freundinnen."
z. B. Gesundheitsdaten, familiäre Angelegenheiten, Probleme, Gefühle, Verliebtheit oder Liebeskummer

So kann ich meine Daten schützen
z. B. vertrauliche Informationen nur mit Freunden bzw. Freundinnen und Personen teilen, denen man wirklich vertraut

„Das ist mein Geheimnis. Das geht niemanden etwas an."
z. B. Tagebuch, Beziehungsleben, sexuelle Orientierung, Nacktbilder

So kann ich meine Daten schützen
z. B. Tagebuch abschließen, keine intimen Bilder per Messenger verschicken oder in Clouds speichern

Technischer Schutz von Privatsphäre

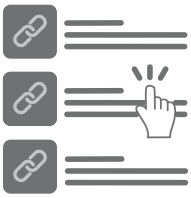
Es gibt verschiedene Möglichkeiten, die eigenen Daten im Internet zu schützen. Am besten ist es, sich vorher zu überlegen, welche Daten man von sich online stellt. Grundsätzlich sollte man sehr sparsam mit persönlichen Angaben umgehen – im Zweifel lieber nicht posten. Es gibt aber auch technische Einstellungen in Social-Media-Angeboten, die die Privatsphäre schützen können:

Mögliche Situation	Privatsphäre-Einstellungen
Ich erstelle ein Profil in einem Social-Media-Angebot.	• Nutzungsbedingungen des Social-Media-Angebots lesen • Das Profil so einstellen, dass es nur für Kontakte/Freundinnen bzw. Freunde sichtbar ist, z. B. ein privates Konto und kein öffentliches • Einen Nickname wählen, der nichts über sich selbst verrät • So wenig Daten wie möglich im Profil angeben, z. B. keine Adresse, Telefonnummer oder Geburtsdaten • Ein sicheres Passwort benutzen, z. B. mit Groß- und Kleinbuchstaben und einer Kombination aus Zahlen und Sonderzeichen

Ich poste etwas in meinem Social-Media-Profil.	● Sichtbarkeit der Inhalte prüfen und einschränken: Wer kann das sehen? Nur bestimmte Freundinnen bzw. Freunde oder alle? ● Eigene Posts und Beiträge regelmäßig prüfen: Möchte ich die Sichtbarkeit so lassen oder doch mehr einschränken? Fühle ich mich noch wohl mit dem Post? Ein Entfernen im eigenen Profil ist möglich
Ich werde in einen Gruppenchat aufgenommen.	● Prüfen: Kenne ich alle Mitglieder im Chat? ● Überlegen: Sollen alle meine Beiträge sehen, obwohl ich sie nicht kenne? ● Wenn man sich unwohl fühlt: aus der Gruppe austreten oder sie sogar melden
Ich verschicke Bilder oder Videos.	● Überlegen: kann man der Person vertrauen? ● Wenn vorhanden, dann die Funktion nutzen, dass Bilder nur einmalig angezeigt werden und danach nicht mehr abrufbar sind ● Vorsichtig sein: Keine intimen Bilder und Videos versenden. Auch bei einmaligem Ansehen kann das Gegenüber einen Screenshot machen ● Keine intimen Bilder oder Videos in Clouds hochladen
Jemand möchte mich verlinken oder jemand hat mich verlinkt und ich möchte das nicht.	● In den Privatsphäre-Einstelllungen der App festlegen, wer den eigenen Account verlinken darf, z. B. nur Freundinnen bzw. Freunde oder gar keiner ● Wenn möglich: Die Verlinkung löschen
Jemand schreibt mir, den ich nicht kenne.	● Vorsichtig sein: Keine Daten an Fremde weitergeben und erst recht keine Bilder oder Videos schicken ● Wenn etwas verdächtig wirkt: Die Person blockieren und melden, ggf. auch zur Polizei gehen

Quellenangabe

Der Text ist Bestandteil der bereits bestehenden Unterrichtseinheit „Liken, posten, teilen“ des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Unterrichtseinheit ist verfügbar unter: **www.medienführerschein.bayern.** Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.



Beratungsstellen und Hilfsangebote

Bayerisches Landeskriminalamt: Zentralstelle Cybercrime

Für die Bearbeitung von Fällen von Cyberkriminalität sind in Bayern die Kommissariate „Cybercrime" der Kriminalpolizei zuständig. Anzeigen nehmen die örtlichen Polizeiinspektionen entgegen. Auf der **Seite des Bayerischen Landeskriminalamtes** finden Betroffene ihre zuständige Polizeidienststelle.

Bundeskonferenz für Erziehungsberatung e. V. – Fachverband für Erziehungs- und Familienberatung

Der Fachverband bietet ein Online-Beratungsangebot für **Jugendliche** und für **Eltern**. Das Angebot ermöglicht z. B. den Austausch mit Gleichaltrigen in Foren oder Gruppen-Chats oder eine professionelle Beratung durch Fachkräfte.

Jugend.support

Jugend.support unterstützt Jugendliche, mit schwierigen Situationen im Internet umzugehen, z. B. Mobbing und Belästigung, Unangenehmes und Extremes oder bei Notfällen.

Juuuport

Juuuport ist eine bundesweite Online-Beratungsstelle von Jugendlichen für Jugendliche. Sie finden dort Hilfe zu verschiedenen Themen und Problemen im Internet. Ehrenamtlich aktive Jugendliche und junge Erwachsene helfen Gleichaltrigen bei Online-Problemen wie Cybermobbing, Stress in sozialen Medien, Datenmissbrauch, exzessiver Mediennutzung oder Fake News.

Medien kindersicher

Das Online-Portal **Medien kindersicher** informiert Eltern über technische Schutzlösungen für unterschiedliche Geräte bzw. Betriebssysteme, Dienste und Apps und bietet Schritt-für-Schritt-Anleitungen für konkrete Sicherheitseinstellungen. Medienkindersicher.de ist ein Angebot der Landesmedienanstalten von Bremen, Baden-Württemberg, Mecklenburg-Vorpommern und Rheinland-Pfalz sowie von klicksafe.

Nummer gegen Kummer

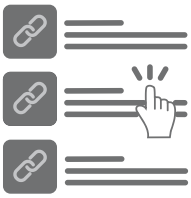
Das Angebot **Nummer gegen Kummer** bietet anonyme Beratung und Hilfe bei unterschiedlichen Problemen – telefonisch und online. Neben Kindern und Jugendlichen können auch Eltern das Angebot nutzen.

Verbraucherzentrale Bayern

Bei Datenmissbrauch können sich Betroffene an die **Verbraucherzentrale** wenden. Die Verbraucherzentrale bietet Beratung telefonisch, online oder vor Ort an.

Weißer Ring

Der **Weiße Ring** bietet Opfern von (Online-)Kriminalität verschiedene Beratungsmöglichkeiten: Anonym per Telefon und E-Mail oder mit Beraterinnen und Beratern vor Ort.



Weiterführende Informationsangebote

Online-Angebote

Internet-ABC: Kinder und Datenschutz

www.internet-abc.de

Die Seite für Eltern zum Thema Kinder und Datenschutz zeigt unter anderem auf, wo Kinder persönliche Daten im Internet hinterlassen, wie sie ihre Daten schützen können und wie Eltern ihrem Kind einen vorsichtigen Umgang mit persönlichen Daten nahebringen können.

klicksafe: Privatsphäre und Big Data. Wie schütze ich meine Daten im Internet?

www.klicksafe.de

Die Seite gibt Tipps zum Schutz von persönlichen Daten z. B. in Bezug auf den Browserverlauf, Cookies und Spyware, Spam und sichere Passwörter.

klicksafe: Welches Mindestalter gilt für WhatsApp, Instagram, TikTok und Co.?

www.klicksafe.de

Übersicht über empfohlene Mindestalter aus den Nutzungsbedingungen verschiedener Social-Media-Angebote.

mobilsicher – Das Infoportal für sichere Handynutzung

https://mobilsicher.de

Das Portal enthält Informationen rund um Privatsphäre, Datenschutz und Sicherheit bei Mobilgeräten. Es gibt eine umfassende Datenbank, die unter anderem aufführt, welche Zugriffsrechte unterschiedliche Apps verlangen.

Saferinternet.at: Privatsphäre-Leitfäden

www.saferinternet.at

Die Privatsphäre-Leitfäden von saferinternet.at für Snapchat, WhatsApp, TikTok oder Instagram zeigen in Schritt-für-Schritt-Anleitungen praktische Tipps zu möglichen Sicherheitseinstellungen der Dienste und Angebote auf.

SCHAU HIN! Was dein Kind mit Medien macht
Persönliche Daten im Netz schützen – das Internet vergisst nichts

www.schau-hin.info

Die Seite zeigt, wo bei der Internetnutzung Datenspuren hinterlassen werden und für welche Zwecke fremde Daten missbräuchlich genutzt werden können.

SCHAU HIN! Was dein Kind mit Medien macht
Daten schützen und sicher surfen: Tipps für Eltern

www.schau-hin.info

Die Seite gibt Tipps, wie Eltern ihr Kind bei einer verantwortungsvollen Mediennutzung in Sachen Datenschutz und Privatsphäre unterstützen und begleiten können.

Verbraucherzentrale:
Datenmissbrauch: Selbsthilfe bei unzureichendem Schutz

www.verbraucherzentrale.de

Die Seite der Verbraucherzentrale informiert darüber, wie Unternehmen an personenbezogene Daten gelangen und sie verarbeiten. Es wird gezeigt, wie Nutzerinnen und Nutzer verhindern können, dass ihre Daten in falsche Hände geraten.

Verbraucherzentrale:
Sicher im Internet – Handy, Tablet und PC schützen

www.verbraucherzentrale.de

Auf der Seite der Verbraucherzentrale wird gezeigt, welche Möglichkeiten es gibt, persönliche Daten zu schützen, z. B. im Bereich von Passwörtern und Accounts, Online-Shopping oder der Datensicherung.

Studien zur Social-Media-Nutzung von Kindern und Jugendlichen

JIM-Studie 2021. Jugend, Information, Medien

www.mpfs.de

Jährlich erscheinende Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger des Medienpädagogischen Forschungsverbands Südwest.

KIM-Studie 2020. Kindheit, Internet, Medien

www.mpfs.de

Zweijährlich erscheinende Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger des Medienpädagogischen Forschungsverbands Südwest.

Broschüren und Informationsmaterial

Instagram-Flyer
Infoflyer von klicksafe
www.klicksafe.de

Mediennutzungsvertrag
Online-Angebot unter **www.mediennutzungsvertrag.de**
sowie Infoflyer von klicksafe
www.klicksafe.de

Dein Vertrag mit Discord – Nutzungsbedingungen kurzgefasst
Infoblatt von handysektor
www.handysektor.de

Dein Vertrag mit Instagram – Nutzungsbedingungen kurzgefasst
Infoblatt von handysektor
www.handysektor.de

Dein Vertrag mit Signal – Nutzungsbedingungen kurzgefasst
Infoblatt von handysektor
www.handysektor.de

Dein Vertrag mit Snapchat – Nutzungsbedingungen kurzgefasst
Infoblatt von handysektor
www.handysektor.de

Dein Vertrag mit TikTok – Nutzungsbedingungen kurzgefasst
Infoblatt von handysektor
www.handysektor.de

Dein Vertrag mit Twitch – Nutzungsbedingungen kurzgefasst

Infoblatt von handysektor

www.handysektor.de

Dein Vertrag mit WhatsApp – Nutzungsbedingungen kurzgefasst

Infoblatt von handysektor

www.handysektor.de

Selbstdatenschutz! Tipps, Tricks und Klicks

Broschüre der Bayerischen Landeszentrale für neue Medien (BLM)

www.blm.de

Selbstdatenschutz: Tipps zum sicheren Passwort

Broschüre der Bayerischen Landeszentrale für neue Medien (BLM)

www.blm.de

Sicherer in Social Media – Tipps für Eltern

Broschüre von klicksafe

www.klicksafe.de

Snapchat-Flyer

Infoflyer von klicksafe

www.klicksafe.de

TikTok-Familien-Checkliste

Checkliste von klicksafe

www.klicksafe.de

TikTok-Flyer

Infoflyer von klicksafe

www.klicksafe.de

Was macht mein Kind eigentlich bei TikTok?

Broschüre von klicksafe

www.klicksafe.de

Was macht mein Kind eigentlich bei YouTube?

Broschüre von klicksafe

www.klicksafe.de

WhatsApp-Flyer

Infoflyer von klicksafe

www.klicksafe.de

YouTube-Familien-Checkliste

Checkliste von klicksafe

www.klicksafe.de

YouTube-Flyer

Infoflyer von klicksafe

www.klicksafe.de

Impressum

Konzeption: Stiftung Medienpädagogik Bayern
Redaktion: Jutta Baumann, Simone Hirschbolz, Verena Radmanic, Julia Vatter (Stiftung Medienpädagogik Bayern)

Satz und Layout: Werbhaus, Georg Lange
Bildnachweise: Peter Weber Grafikdesign

Die entstandenen Materialien basieren zum Teil auf bereits bestehenden Materialien des Medienführerscheins Bayern:

- Bereich der Sonderpädagogischen Förderung: „Gamen, daddeln, zocken – Digitale Spiele hinterfragen und verantwortungsbewusst nutzen“ (Autorin: Annette Pola); „Liken, posten, teilen – Social-Media-Angebote hinterfragen und sicher nutzen“ (Autorin: Selma Brand);
- 5., 6. und 7. Jahrgangsstufe: „Ich im Netz I – Eigene Daten schützen und mit Bildern verantwortungsvoll umgehen“ (Autorin: Dr. Kristina Hopf); „Fakt oder Fake? Glaubwürdigkeit von Online-Quellen prüfen und bewerten“ (Autorin: Stefanie Rack); „Meine Medienstars – Inszenierungsstrategien durchschauen und hinterfragen“ (Autorin: Kim Beck);
- 8. und 9. Jahrgangsstufe: „Im Informationsdschungel – Meinungsbildungsprozesse verstehen und hinterfragen“ (Autoren: Dr. Olaf Selg, Dr. Achim Hackenberg); „Ich als Urheber – Urheberrechte kennen und reflektieren“ (Autorin: Dr. Kristina Hopf)

Digitale Elemente
Konzeption: Stiftung Medienpädagogik Bayern, Fish Blowing Bubbles GmbH
Redaktion: Jutta Baumann, Simone Hirschbolz, Verena Radmanic, Julia Vatter (Stiftung Medienpädagogik Bayern)
Grafische Gestaltung: Fish Blowing Bubbles GmbH

Film-Clips
Konzeption: Stiftung Medienpädagogik Bayern, Enrico Pallazzo – Gesellschaft für gute Unterhaltung GmbH
Redaktion: Jutta Baumann, Simone Hirschbolz, Verena Radmanic, Julia Vatter (Stiftung Medienpädagogik Bayern)

1. Auflage: München, 2022

Stiftung Medienpädagogik Bayern

Entwicklung der Materialien im Rahmen des Pilotversuchs „Digitale Schule der Zukunft“ und gefördert durch das Bayerische Staatsministerium für Unterricht und Kultus.

Bayerisches Staatsministerium für Unterricht und Kultus

Digitale Schule der Zukunft