Glossar

Auf den nächsten Seiten finden Sie Begriffe und Erklärungen zum Thema **Jugendschutz und Sicherheitseinstellungen.**

Diese Begriffe finden Sie im Glossar:

Altersverifikationssystem

Ein Altersverifikationssystem (Abkürzung: AVS) ist ein **technisches Mittel für den Jugendschutz**, mit dem geprüft wird, ob **eine Person das geforderte richtige Alter** hat. Altersverifikationssysteme sind eine **Vorsperre** für Angebote, zu denen nur Erwachsene Zugang haben dürfen. Damit wird beispielsweise auf einer Internetseite überprüft, ob eine Nutzerin oder ein Nutzer schon 18 Jahre alt ist. Dazu muss sich diese bzw. dieser im Vorfeld persönlich identifizieren, z. B. über eine Aufnahme/Foto des Ausweises. Erst dann kann der Inhalt eingesehen werden.

Cybermobbing

Cybermobbing bedeutet, dass jemand **über einen längeren Zeitraum über das Internet fertiggemacht** wird, z. B. **wenn eine oder mehrere Personen jemanden belästigen oder beschimpfen, sich lustig machen, ausgrenzen oder sogar bedrohen.** Cybermobbing passiert immer online, z. B. über Instagram, WhatsApp oder Snapchat. Daher hört es auch nach der Schule nicht auf und geht zu Hause weiter. Opfer werden Tag und Nacht beschimpft – über Social Media oft auch für alle sichtbar.

Fake-Profil

Ein Fake-Profil ist ein **gefälschtes Social-Media-Profil.** Es gibt verschiedene Arten von Fake-Profilen. Entweder die Person, der das Profil gehört, **gibt es gar nicht** und die Informationen auf dem Profil sind frei erfunden (z. B. Name, Alter und auch das Profilbild). Oder jemand erstellt ein Profil und benutzt **den Namen und das Bild einer echten Person,** z. B. eines Stars oder den Namen einer Person, die er

Stiftung Medienpädagogik Bayern
Digitale Schule der Zukunft

oder sie kennt. Dann gibt es die Person auf dem Profil zwar wirklich, aber das Profil gehört jemand anderem.

Manche erstellen ein Fake-Profil von einer bestimmten Person, **um diese zu mobben.** Auf dem Profil werden dann gemeine Dinge veröffentlicht oder Lügen verbreitet. Für die Opfer ist es sehr schwer, das Fake-Profil zu löschen. Ein Fake-Profil anzulegen, ist verboten und strafbar.

Grooming

Grooming kommt vom englischen Wort „to groom" und bedeutet „anbahnen" bzw. „vorbereiten". Es bezeichnet den Versuch von Erwachsenen, **einen jungen Menschen zu verführen,** v. a. minderjährige Kinder und Jugendliche. Erwachsene sprechen dabei Minderjährige über das Internet gezielt an und versuchen, sie dazu zu bewegen, z. B. Nacktfotos von sich zu verschicken oder sich vor der Webcam auszuziehen. Grooming hat dabei zum Ziel, die Kinder und Jugendlichen auch im echten Leben zu treffen, um sie sexuell zu missbrauchen.

Beim Grooming werden **oft Fake-Profile genutzt.** Dort geben die Täterinnen oder Täter z. B. ein falsches Alter an und hinterlegen ein falsches Profilbild. Deshalb ist oft schwer zu erkennen, wer wirklich hinter dem Profil steckt. Grooming ist **als Vorbereitung zum sexuellen Missbrauch strafbar.**

Gruppe

In vielen Apps kann man Gruppen anlegen, in denen mehrere Nutzerinnen und Nutzer **miteinander gleichzeitig kommunizieren** können – in sog. Gruppen-Chats. Neben Nachrichten können dort auch Bilder oder andere Dateien verschickt werden. In **offene Gruppen** kann man selbst beitreten und jeder kann mitmachen. In **geschlossene Gruppen** muss man erst von einem Administrator eingeladen werden. Generell ist die Gruppengröße in den meisten Angeboten unbegrenzt. Es können also auch sehr viele Personen in einer Gruppe sein, die dann sehr viele Nachrichten schreiben. Um v. a. bei großen Gruppen nicht den Überblick zu verlieren, sind gute Gruppenregeln wichtig, z. B. welche Beiträge gewünscht sind und welche nicht oder die Umgangsformen unter den Mitgliedern.

Hacking

Hacking kommt vom englischen Wort „to hack" und bedeutet **„in etwas eindringen".** Hacking wird oft in der Computersprache verwendet und bedeutet, in einen **Computer** oder auch in ein **Social-Media-Profil** einzudringen. Dabei kann sich eine fremde Person ohne Erlaubnis Zugang zu den persönlichen Daten anderer verschaffen und so deren Privatsphäre verletzen. Hacking ohne Erlaubnis ist **illegal.**

Indizierung

Indizierung bedeutet, etwas **auf den Index** zu **setzen.** Der Index ist eine **Sammlung jugendgefährdender Medien** wie Schriften, Filme, DVDs, Video- und Computerspiele oder Internetseiten (Telemedien). Jugendgefährdend bedeutet u. a., dass die Medien oder Inhalte unsittlich sind, verrohend wirkend oder zu Gewalttätigkeit,

Verbrechen oder Rassenhass anstacheln. Wenn diese Inhalte auf dem Index stehen, dürfen sie nicht mehr vertrieben und beworben werden. Zuständig für die Indizierung ist in Deutschland die Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ).

Jugendschutz

Der Jugendschutz soll Kinder und Jugendliche vor schädlichen Einflüssen schützen, z. B. vor Gefahren im Internet oder in digitalen Spielen. Jugendschutzrelevante Inhalte sind u. a. Gewalt, Pornografie oder Extremismus, aber auch Kostenfallen und Gewinnspiele.

Die gesetzliche Grundlage ist das **Jugendschutzgesetz (JuschG).** Es enthält bestimmte Regelungen, die junge Menschen schützen sollen. Viele digitale Spiele oder Filme sind mit einer Alterskennzeichnung versehen und erst ab einem bestimmten Alter erlaubt. Zusätzlich müssen bei den gekennzeichneten Filmen mögliche Risiken für die Entwicklung von Kindern und Jugendlichen vorher angezeigt werden, dafür gibt es sog. **Warnhinweise (= Gefährdungshinweise).**

Jugendschutz-programm

Jugendschutz- bzw. Filterprogramme sind Computerprogramme, die Kinder und Jugendliche vor gefährlichen Inhalten schützen sollen. Sie filtern im Vorfeld die Angebote und legen fest, welche Inhalte Kindern und Jugendlichen angezeigt werden. Dabei arbeiten sie mit **Positiv- und Negativ-Listen.** Das bedeutet: Entweder sind nur kinderfreundliche Seiten erreichbar oder problematische Angebote werden ausgeblendet. Viele Programme können auch die Gerätenutzung insgesamt beschränken. Es können beispielsweise Benutzerkonten angelegt und Zeitbegrenzungen festgelegt werden. Jugendschutzprogramme müssen aktiv installiert werden.
Ein gesetzlich anerkanntes Jugendschutzprogramm ist z. B. **JusProg.**

PIN

Die Abkürzung PIN steht für **Personal Identification Number** und meint einen Code, der nur einer Person bekannt ist. Die PIN wird z. B. zur Sicherung von Diensten oder Geräten eingesetzt, damit nur die Person darauf zugreifen kann, die die Erlaubnis dazu hat. Das soll **Missbrauch oder Diebstahl von Daten verhindern.**

Eine PIN wird auch bei Bankkarten oder Smartphones genutzt, manchmal nennt man sie auch Geheimzahl. Eine andere Art von PIN ist die **Jugendschutz-PIN.** Sie verhindert, dass Kinder und Jugendliche Zugriff auf Inhalte haben, die sie nicht sehen sollen. Etwa brutale Filme, Serien oder Spiele ab 18 Jahren. Daher ist es sinnvoll, dass Eltern eine Jugendschutz-PIN einrichten, um ihr Kind vor problematischen Inhalten zu schützen. In den meisten Angeboten oder Geräten kann eine Jugendschutz-PIN vergeben werden, z. B. auf Video- und Streaming-Plattformen oder am WLAN-Router.

Post

Ein Post ist ein Beitrag in Social-Media-Angeboten. Posts sehen je nach Social-Media-Angebot **sehr unterschiedlich** aus. Ein Post kann ein Text, ein Bild oder ein Video sein. Mehrere Posts kann man auch **zu einer Story verbinden.** Die Posts haben dann einen Zusammenhang.

Prank

Prank bedeutet **„Streich".** Im Internet und auf Social-Media-Angeboten sind mit Pranks Videos gemeint, in denen **Personen anderen einen Streich spielen,** z. B. Freundinnen bzw. Freunden oder Familienmitgliedern, aber auch unbekannten Personen. Oft sind Pranks lustig und deshalb sehr beliebt. Sie können aber auch gemein und gefährlich sein, z. B. wenn Menschen dabei verletzt werden.

Privatsphäre

Der Begriff Privatsphäre umschreibt den **persönlichen Lebensbereich** einer Person. Jeder Mensch hat ein Recht auf diesen persönlichen Lebensbereich. Das ist im Grundgesetz verankert. Die Privatsphäre umfasst Bilder von einer Person oder persönliche Informationen über eine Person. Aber auch private Nachrichten in einem Chat werden durch die Privatsphäre geschützt. Deshalb darf man im Internet keine Bilder oder private Nachrichten von anderen teilen oder persönliche Informationen über andere Personen ohne deren Einverständnis veröffentlichen. Außerdem ist es wichtig, die **eigene Privatsphäre zu schützen.** Deshalb sollte man immer gut überlegen, welche persönlichen Informationen man im Internet von sich preisgibt oder welche Bilder man von sich zeigt.

Selbstdatenschutz

Selbstdatenschutz bedeutet, die **eigenen Daten zu schützen** und zu entscheiden, welche Daten veröffentlicht werden können und welche lieber privat bleiben sollten. Dabei sollte man sich im Klaren darüber sein, was passieren kann, wenn man seine Daten weitergibt. Das ist v. a. bei **sensiblen Daten** wie Adresse, Kontodaten oder auch Fotos und Videos wichtig, die besonders schützenswert sind.

Social Media

Social Media bedeutet Soziale Medien. Das sind Angebote oder Plattformen im Internet, auf denen sich Nutzerinnen und Nutzer **miteinander austauschen und sich selbst darstellen können.** Der Austausch kann ganz unterschiedlich sein, z. B. indem man Medien wie Fotos oder Videos veröffentlicht, also etwas **postet** oder **teilt.** Man kann auch mit anderen Nutzerinnen und Nutzern Nachrichten schreiben oder ihre Posts kommentieren.

Um in Sozialen Medien aktiv sein zu können, muss man sich erst anmelden. Man erstellt dann ein **Profil bzw. einen Account** mit seinem Namen und einem Profilbild. Anschließend kann man sich **mit anderen Nutzerinnen und Nutzern vernetzen,** wie dem eigenen Freundeskreis oder der Familie, aber auch mit anderen Menschen auf der ganzen Welt. Man kann sein **Profil privat** stellen. Dann können nur diejenigen, mit denen man befreundet ist, sehen, was man teilt. Macht man sein **Profil öffentlich,** können alle die Inhalte darauf sehen.

Social-Media-App

Man kann **Social-Media-Angebote** auf verschiedenen Geräten nutzen, z. B. über einen Browser am Computer. Wenn man Social Media auf den Smartphone oder Tablet nutzt, **kann man dafür eine eigene App verwenden.** Manche Social-Media-Apps sind schon automatisch auf dem Smartphone oder Tablet vorinstalliert, andere muss man erst im App Store herunterladen.

Story und Status

Social-Media-Angebote wie Instagram oder WhatsApp haben verschiedene Funktionen. Eine davon ist die Story oder der Status. Man postet dabei etwas auf seinem Profil, das nur für eine bestimmte Zeit zu sehen ist. Meistens gilt das für **24 Stunden.** Dabei kann man auswählen, ob sie alle oder nur bestimmte Nutzerinnen und Nutzer sehen können. Eine Story oder ein Status kann ein **Bild** oder ein **Video,** ein **Link zu einer Seite** oder ein **kurzer Text** sein. Oft werden dabei die verschiedenen Medien bzw. Formate auch **miteinander kombiniert,** um mehr Aufmerksamkeit zu bekommen.

Quellenangabe

Das Glossar basiert auf den bereits bestehenden Unterrichtseinheiten „Liken, teilen, posten" sowie „Gamen, daddeln, zocken" des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Materialien sind abrufbar unter: **www.medienfuehrerschein.bayern.** Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.