

Kinder online begleiten

Was Altersgrenzen wirklich bedeuten, wie man Konten gemeinsam einrichtet, woran man Mobbing und Grooming erkennt — und was zu tun ist, wenn etwas passiert ist.

THEMEN IM ÜBERBLICK

Begleiten statt verbieten

Altersgrenzen verstehen

Gemeinsam einrichten

Regeln vereinbaren

Cybermobbing

Grooming erkennen

Erpressung mit Bildern

Anlaufstellen

Diese Broschüre richtet sich an Erwachsene, die Kinder und Jugendliche begleiten. Die Sicht der Nutzenden selbst behandelt „**Social Media Sicherheit**“; technische Grundlagen stehen in „**Cybersecurity im Alltag**“.

01	Begleiten statt verbieten	3
02	Altersgrenzen und was sie bedeuten	4
03	Konten gemeinsam einrichten	5
04	Regeln, die halten	6
05	Cybermobbing erkennen und reagieren	7
06	Grooming erkennen	8
07	Erpressung mit Bildern	9
08	Kostenfallen und Käufe im Spiel	10
09	Was Erwachsene selbst posten	11
10	Wenn etwas passiert ist: Anlaufstellen	12
11	Spickzettel zum Ausdrucken	13
12	Quellen und weiterführende Hinweise	14
13	Impressum und Weitergabe	15

Kein Erziehungsratgeber

Diese Broschüre beschreibt Risiken und praktische Schritte. Wie viel Freiheit ein bestimmtes Kind verträgt, weiß niemand besser als die Menschen, die es kennen — sie ersetzt keine pädagogische Beratung.

Begleiten statt verbieten

Verbote wirken kurzfristig und erzeugen langfristig Heimlichkeit. Wer nicht erzählen darf, dass er ein Spiel spielt, erzählt auch nicht, dass ihn dort jemand belästigt. Das ist der eigentliche Grund, warum Begleitung besser schützt als Kontrolle.

Reden ohne Konsequenz

Kinder melden Probleme, wenn sie keine Strafe fürchten. „Du kannst mir alles sagen, ohne dass das Handy weg ist“ ist eine Schutzmaßnahme.

Interesse zeigen

Sich erklären lassen, was gerade gespielt oder geschaut wird. Wer die Welt kennt, erkennt Veränderungen darin.

Mitwachsen

Was mit acht gilt, passt mit vierzehn nicht mehr. Regeln gehören regelmäßig neu verhandelt, nicht einmal verkündet.

Selbst Vorbild sein

Am Esstisch, im Auto, beim Posten von Familienfotos. Kinder übernehmen Verhalten, nicht Vorträge.

DER EINE SATZ, DER ZÄHLT

„Wenn dir online etwas komisch vorkommt oder etwas passiert ist, komm zu mir — **ich schimpfe nicht, wir lösen das zusammen.**“ Dieser Satz muss gesagt, wiederholt und im Ernstfall auch eingehalten werden. Er ist wirksamer als jede Kindersicherung.

Altersgrenzen und was sie bedeuten

Auf Plattformen begegnen einem drei verschiedene Angaben, die oft durcheinandergehen. Sie meinen Unterschiedliches und schützen Unterschiedliches.

ANGABE	WOHER	WAS SIE AUSSAGT
Mindestalter der Nutzungsbedingungen	Der Anbieter	Meist 13 Jahre. Eine vertragliche Vorgabe, keine inhaltliche Bewertung – und praktisch kaum kontrolliert.
Altersfreigabe (USK/PEGI)	Prüfstellen	Bewertet die Inhalte eines Spiels. Sagt nichts über Chatfunktionen, Käufe oder andere Spielende aus.
Einwilligung der Sorgeberechtigten	Datenschutzrecht	Für die Verarbeitung von Kinderdaten braucht es je nach Land bis zu einem Alter zwischen 13 und 16 Jahren die Zustimmung der Sorgeberechtigten.

! Die Lücke, die zählt

Eine Freigabe „ab 6“ bedeutet nicht, dass das Umfeld harmlos ist. Ein altersgerechtes Spiel mit offenem Sprachchat bringt ein Kind mit beliebigen Erwachsenen in Kontakt. **Prüfen Sie deshalb nicht die Altersangabe, sondern die Funktionen:** Chat, Direktnachrichten, Freundschaftsanfragen, Livestreams, Käufe.

i Ehrlich bleiben lohnt sich

Viele Kinder geben bei der Anmeldung ein falsches Alter an – oft mit Wissen der Eltern. Die Folge: Das Konto bekommt keine Jugendschutz-Voreinstellungen, weil die Plattform es für ein Erwachsenenkonto hält. Ein korrektes Alter schaltet oft automatisch strengere Grundeinstellungen.

Konten gemeinsam einrichten

Die halbe Stunde beim Einrichten erspart viele Diskussionen später — und sie ist eine Gelegenheit, das Warum zu erklären, statt es nur festzulegen.

- 1 Konto auf privat.** Neue Konten sind meist öffentlich. Follower nur nach Bestätigung.
- 2 Nachrichten von Fremden abschalten.** Die wirksamste einzelne Einstellung gegen unerwünschte Kontaktaufnahme.
- 3 Standort und Live-Funktionen aus.** Kein Standort-Tagging, keine Standortfreigabe an „Freunde“, die niemand kennt.
- 4 Suchbarkeit einschränken** — nicht über Telefonnummer oder E-Mail auffindbar sein.
- 5 Sicherheit einrichten:** eigenes Passwort, 2FA, und eine Wiederherstellungs-Adresse, auf die auch Sie Zugriff haben.
- 6 Gemeinsam durchgehen, wer was sieht.** Das Profil einmal aus fremder Sicht ansehen — viele Kinder unterschätzen, wie viel öffentlich ist.

Family-Funktionen

Beide Handysysteme bieten Familienkonten mit Altersfreigaben, Kaufbestätigung und Zeitkontingenten. Gemeinsam einrichten, nicht heimlich.

Grenzen der Technik

Jede Kindersicherung lässt sich umgehen — spätestens auf dem Gerät einer Freundin. Sie ersetzt kein Gespräch, sie verschafft Zeit.

i Plattform für Plattform

Wo die Einstellungen bei Instagram, Facebook, X, TikTok und WhatsApp liegen, steht in „Social Media Sicherheit“, Kapitel „Sicherheitseinstellungen je Plattform“.

Regeln, die halten

Regeln funktionieren, wenn sie vereinbart statt verordnet sind, wenn sie begründet werden und wenn sie für alle im Haushalt gelten.

Wo

Geräte in Gemeinschaftsräumen laden statt im Kinderzimmer. Nicht als Kontrolle, sondern weil nachts allein die schlechteste Zeit für schwierige Nachrichten ist.

Wann

Feste Zeiten sind leichter einzuhalten als Kontingente. Bildschirmzeit als vereinbarte Grenze, nicht als Strafe.

Was

Welche Apps sind in Ordnung, welche erst nach Rücksprache? Neue Apps gemeinsam ansehen, bevor sie installiert werden.

Mit wem

Freundschaftsanfragen nur von Menschen, die man persönlich kennt. Das ist die Regel, die im Ernstfall am meisten trägt.

Was in eine Vereinbarung gehört

- ✓ Was passiert bei unangenehmen Nachrichten — und dass Bescheidsagen nie bestraft wird.
- ✓ Welche Fotos gepostet werden dürfen, auch von anderen.
- ✓ Dass Passwörter nicht an Freundinnen und Freunde weitergegeben werden, auch nicht „nur kurz“.
- ✓ Wann die Regeln das nächste Mal gemeinsam angeschaut werden. Ein Datum verhindert, dass sie mit dem Kind nicht mitwachsen.

Cybermobbing erkennen und reagieren

Mobbing im Netz hört nicht am Schultor auf, es hat Publikum und es hinterlässt Spuren, die bleiben. Betroffene erzählen selten von sich aus — aus Scham und aus Angst, das Gerät zu verlieren.

Anzeichen

Rückzug, Schlafprobleme, plötzliche Abneigung gegen Schule, heimliches oder gar kein Handy mehr, Stimmungswechsel nach dem Blick aufs Display.

Erste Reaktion

Zuhören, nicht sofort handeln. „Wir überlegen zusammen, was wir tun“ statt „Ich rede morgen mit der Schule“ — sonst folgt beim nächsten Mal kein Gespräch.

Was konkret hilft

- 1 Beweise sichern, bevor blockiert wird.** Screenshots mit Profilname, Datum und Uhrzeit im Bild, dazu die Adresse des Beitrags.
- 2 Blockieren und melden.** Jede Plattform hat Meldewege; sie werden zu selten genutzt.
- 3 Nicht antworten.** Reaktionen sind der Treibstoff. Schweigen und melden wirkt besser als Gegenwehr.
- 4 Schule einbeziehen,** wenn Beteiligte aus dem Umfeld kommen — die meisten Fälle spielen dort weiter.
- 5 Bei Bedrohung, Nötigung oder Verbreitung von Bildern: Anzeige.** Mit den gesicherten Beweisen.

i Ausführlicher

Die Melde- und Beweiswege im Detail stehen in „Social Media Sicherheit“, Kapitel „Belästigung, Mobbing und richtig melden“.

Grooming erkennen

Grooming beschreibt, wie Erwachsene gezielt das Vertrauen von Kindern aufbauen, um sie sexuell auszunutzen. Es passiert dort, wo Kinder ohnehin sind: in Spielen, in Streams, in Chatgruppen – meist über Wochen und mit viel Zuwendung.

AUFMERKSAMKEIT

„Du bist reifer als andere in deinem Alter.“

Ungewöhnlich viel Interesse, Lob und Zeit. Oft von jemandem, der angeblich selbst jung ist.

GESCHENKE

„Ich schenk dir die Spielwährung, ist doch nichts.“

Skins, Guthaben, Gegenstände im Spiel. Sie erzeugen ein Gefühl von Schuld und Verpflichtung.

WECHSEL DES KANALS

„Schreib mir lieber woanders, hier liest jeder mit.“

Weg von der moderierten Plattform hin zu Direktnachrichten. Ein deutliches Warnzeichen.

GEHEIMHALTUNG

„Das bleibt unter uns, sonst verstehen die das falsch.“

Der Kern der Masche. Wer Geheimhaltung verlangt, hat einen Grund dafür.



Was Kinder wissen müssen

Kein Erwachsener, der es gut meint, verlangt Geheimnisse vor den Eltern. Und: **Wer hereingefallen ist, ist nicht schuld.** Genau diese Botschaft entscheidet darüber, ob ein Kind sich meldet, solange noch etwas zu retten ist.

Erpressung mit Bildern

Ein Bild wird erschmeichelt oder erzwungen — danach folgt die Drohung, es zu verbreiten. Inzwischen genügt für die Drohung nicht einmal ein echtes Foto: Bilder lassen sich mit KI aus harmlosen Aufnahmen erzeugen. Für Betroffene ist der Druck derselbe.

DIE DREI SÄTZE FÜR DEN ERNSTFALL

Nicht zahlen. Zahlungen führen zu weiteren Forderungen, nie zum Ende. **Nicht löschen.** Die Nachrichten sind Beweismittel. **Nicht allein bleiben.** Eine erwachsene Vertrauensperson holen — sofort.

- 1 Kontakt abbrechen,** aber den Verlauf sichern: Screenshots, Profilname, Adresse des Profils.
- 2 Konto der anderen Seite melden** und blockieren.
- 3 Anzeige erstatten.** Bei Minderjährigen handelt es sich um schwere Straftaten, die Polizei nimmt sie ernst.
- 4 Meldestelle einschalten,** wenn Material bereits verbreitet wurde — Plattformen und spezialisierte Stellen können Löschungen anstoßen.
- 5 Kind nicht zwingen, alles noch einmal anzusehen.** Erwachsene sichten die Beweise.

! Auch Erwachsene betrifft das

Die gleiche Masche läuft bei Erwachsenen als Massen-E-Mail und ist dort fast immer ein Bluff. Muster und Reaktion stehen in „Cybersecurity im Alltag“, Kapitel „Erpressung, Schockanrufe und falscher Support“.

Kostenfallen und Käufe im Spiel

Spiele für Kinder verdienen selten am Kaufpreis. Sie verdienen an Kleinbeträgen, an Zeitdruck und an Zufallspaketen, deren Inhalt man vorher nicht kennt.

Zufallspakete

Kisten und Pakete mit unbekanntem Inhalt arbeiten mit demselben Reiz wie Glücksspiel — bei Kindern besonders wirksam.

Zeitdruck

„Nur noch 3 Stunden“ ist kein Angebot, sondern eine Technik. Sie funktioniert bei Erwachsenen genauso.

Zweitwährung

Erst Euro in Kristalle tauschen, dann Kristalle ausgeben. Der Umweg verschleiert, was etwas kostet.

Sozialer Druck

Wer nichts kauft, bleibt sichtbar zurück. Darüber zu sprechen hilft mehr als ein Verbot.

- ✓ Keine Zahlungsdaten im Kinderkonto hinterlegen. Guthabekarten statt Kreditkarte.
- ✓ Kaufbestätigung durch die Sorgeberechtigten in den Family-Einstellungen aktivieren.
- ✓ Passwortabfrage bei jedem Kauf einschalten — und das Passwort nicht weitergeben.
- ✓ Abrechnungen gelegentlich durchsehen. Viele Kleinbeträge fallen einzeln nicht auf.
- ✓ Bei ungewollten Käufen durch Minderjährige lohnt der Widerspruch beim Anbieter oder Zahlungsdienst — oft mit Erfolg.

Was Erwachsene selbst posten

Der erste digitale Fußabdruck eines Kindes stammt fast immer von den Eltern. Bilder aus Kindergarten, Urlaub und Krankenbett landen im Netz, lange bevor das Kind gefragt werden kann.

Was bleibt

Was einmal geteilt wurde, lässt sich kaum vollständig zurückholen. In zehn Jahren ist das Kind eine Person mit eigener Meinung dazu.

Was verraten wird

Schulkleidung, Vereinstrikot, Straßenschild im Hintergrund, Name auf der Schultüte: einzeln harmlos, zusammen eine Adresse.

Wer es weiterverwendet

Bilder von Kindern werden aus offenen Profilen abgegriffen und in Zusammenhängen weiterverwendet, die niemand möchte.

Was hilft

Keine Gesichter oder nur an geschlossene Empfängerkreise. Und: Kinder ab dem Grundschulalter fragen — sie verstehen das gut.

DIE FAUSTREGEL

Posten Sie von Ihrem Kind nur, was Sie ihm mit fünfzehn Jahren zeigen würden, ohne dass es Ihnen unangenehm wäre. Bei Krankheit, Wut, Nacktheit und Strafe lautet die Antwort fast immer: nichts.

i Auch der Ort steckt im Bild

Fotos enthalten oft GPS-Koordinaten. Was das bedeutet und wie man sie entfernt, steht in „Social Media Sicherheit“, Kapitel „Was Plattformen über Sie sammeln“.

Wenn etwas passiert ist: Anlaufstellen

ZUERST

Ruhe bewahren und dem Kind sagen, dass es richtig war, sich zu melden. Alles Weitere ist Organisation — diese Reaktion ist das, woran es sich beim nächsten Mal erinnert.

SITUATION

WOHIN

Beratung bei Cybermobbing

klicksafe.de · Nummer gegen Kummer (Kinder- und Jugendtelefon sowie Elterntelefon)

Problematische oder strafbare Inhalte melden

jugendschutz.net · Meldestellen der Plattformen

Straftaten, Bedrohung, Erpressung, Grooming

Polizei — Anzeige mit gesicherten Beweisen; viele Länder bieten eine Online-Wache

Verträge, Abos, ungewollte Käufe

Verbraucherzentrale

Fragen zur Mediennutzung im Alltag

schau-hin.info · Initiative „Gutes Aufwachsen mit Medien“



Beweise zuerst

Vor dem Blockieren, Melden oder Löschen: Screenshots mit Profilname, Datum, Uhrzeit und der Adresse des Beitrags. Ohne sie ist eine Anzeige oft aussichtslos.

Spickzettel zum Ausdrucken

BEIM EINRICHTEN

- ☐ Konto auf privat
- ☐ Nachrichten von Fremden aus
- ☐ Standort und Live aus
- ☐ Korrektes Alter angegeben

VEREINBART

- ☐ Nur bekannte Personen
- ☐ Keine Passwörter weitergeben
- ☐ Bescheidsagen ohne Strafe
- ☐ Nächster Termin zum Nachjustieren

WARNZEICHEN

- ☐ Neue „Freunde“, die niemand kennt
- ☐ Geheimnisse gegenüber Eltern
- ☐ Geschenke im Spiel
- ☐ Rückzug, Stimmungswechsel

IM ERNSTFALL

- ☐ Beweise sichern
- ☐ Blockieren und melden
- ☐ Nicht zahlen, nicht löschen
- ☐ Beratung oder Anzeige

DER SATZ, DER AM MEISTEN SCHÜTZT

„Komm zu mir, wenn etwas komisch ist — ich schimpfe nicht.“

Quellen und weiterführende Hinweise

klicksafe: EU-Initiative für Medienkompetenz
klicksafe.de

jugendschutz.net: Meldestelle für Online-Inhalte
jugendschutz.net

SCHAU HIN!: Medienerziehung im Familienalltag
schau-hin.info

Nummer gegen Kummer: Kinder-, Jugend- und Elterntelefon
nummergegenkummer.de

USK: Alterskennzeichen für Spiele
usk.de

PEGI: Europäische Alterseinstufung
pegi.info

BSI: Kinder und Jugendliche im Netz
bsi.bund.de → Verbraucher

Verbraucherzentrale: In-App-Käufe durch Minderjährige
verbraucherzentrale.de → Digitale Welt

Hinweis

Diese Broschüre ersetzt keine pädagogische, rechtliche oder therapeutische Beratung. Bei Verdacht auf Missbrauch wenden Sie sich an eine Fachberatungsstelle oder an die Polizei.

Weitere Broschüren dieser Reihe

- Cybersecurity im Alltag** — Links, Phishing, Passwörter, 2FA, DNS, öffentliche WLANs und Notfälle.
- Social Media Sicherheit** — Konten, Privatsphäre-Einstellungen, Fake-Profile, Datenweitergabe.
- Smartphone absichern** — Sperre, Berechtigungen, App-Quellen, Verlust, Gerätewechsel, Backups.
- Heimnetz und Smart Home** — Router, WLAN, Gastnetz, vernetzte Geräte, Kameras, Portfreigaben.
- Kinder online begleiten** — diese Broschüre
- Deine Rechte an deinen Daten** — DSGVO praktisch: Auskunft, Löschung, Übertragbarkeit, Musterschreiben.
- Gruppen sicher organisieren** — Rollen, Regeln, Störer, Treffen, Voice, Minderjährige in der Gruppe.
- Allergene und Kennzeichnung** — Die 14 Pflichtangaben, Zutatenlisten lesen, „kann Spuren enthalten“.
- Erste Schritte** — Zweiseitiges Merkblatt zum Einstieg — kein Heft.

Weitergabe und Lizenz

Herausgeber

Plotspace.eu · info@plotspace.eu
Anschrift und Verantwortlicher im Impressum:
plotspace.eu/impressum

Lizenz

CC BY 4.0 — Kopieren, Weitergeben und Bearbeiten ausdrücklich erlaubt. Bitte „Plotspace.eu“ als Quelle nennen und Änderungen kenntlich machen; bearbeitete Fassungen dürfen nicht so wirken, als kämen sie von Plotspace.eu. creativecommons.org/licenses/by/4.0/deed.de
Schriften: Public Sans und IBM Plex Mono, SIL Open Font License 1.1.

Diese Broschüre darf einzeln weitergegeben werden. Sie ist so aufgebaut, dass sie für sich allein verständlich bleibt; Querverweise auf die übrigen Hefte sind Ergänzung, keine Voraussetzung.