



10-Punkte-Kindersicherungs-Checkliste

Für Eltern, Lehrkräfte und Schulen | Stand: März 2026

Kinder und Jugendliche bewegen sich täglich im Internet - und begegnen dabei echten Risiken: Cybermobbing, Grooming, unangemessene Inhalte und Sucht. Laut BSI-Cybersicherheitsmonitor 2025 sind die meisten Kinder diesen Gefahren bereits ausgesetzt, während viele Eltern das Ausmaß unterschätzen. Laut KKH-Studie 2025 waren 21 % der 12- bis 19-Jährigen bereits Opfer von Cybermobbing - das Bündnis gegen Cybermobbing zählt über zwei Millionen betroffene Kinder in Deutschland. Diese Checkliste gibt einen strukturierten Rahmen: technische Maßnahmen und Medienbildung als Team.

1 Früh anfangen, altersgerecht begleiten

Schon Grundschulkinder sind über Spiele, YouTube und Messengerdienste online. Wer wartet bis das Kind „alt genug“ ist, verpasst das Zeitfenster für frühe Begleitung - wenn Gewohnheiten, Vertrauen und Reflexionskompetenz geformt werden. Begleiten Sie Ihr Kind mit klaren, gemeinsam vereinbarten Regeln statt pauschalen Verboten. Gemeinsames Surfen schafft Vertrauen und gibt Ihnen Einblick in die digitale Welt Ihres Kindes.

2 Eigene Kinderkonten auf jedem Gerät einrichten

Kinder sollten niemals über das Erwachsenen-Konto mit vollen Zugriffsrechten surfen. Eigene Konten mit eingeschränkten Rechten sind Grundvoraussetzung für sinnvolle Schutzeinstellungen - ohne Kinderkonto greifen Zeitlimits und Inhaltsfilter nicht zuverlässig. Windows: Familienkonto über account.microsoft.com. Android: Google Family Link. Apple: eigene Apple-ID für Kinder unter 13 erstellen.

3 Technische Kindersicherung konsequent aktivieren

Drei Ebenen kombinieren: DNS-Filter im Router (CleanBrowsing oder Cloudflare 1.1.1.3) schützt alle Geräte im Heimnetz zentral. Betriebssystem-Kindersicherung (Windows Family Safety, Google Family Link, iOS Bildschirmzeit) ermöglicht Zeitlimits und App-Filter je Gerät. Alle Einstellungen mit einem separaten Passwort sichern, das nur Erwachsene kennen.

4 Zeitlimits und bildschirmfreie Zonen vereinbaren

Exzessive Bildschirmzeit verursacht Schlafmangel, soziale Isolation und Suchtentwicklung. Legen Sie gemeinsam Regeln zu Bildschirmzeiten, gerätefreien Schlafenszeiten und Offline-Zonen (Schlafzimmer, Esstisch) fest. Kinder altersgerecht in die Regelgestaltung einbeziehen - selbst vereinbarte Regeln werden besser eingehalten als verordnete Verbote.

5 Medieninhalte regelmäßig gemeinsam besprechen

Nicht nur Risiken thematisieren - auch was das Kind online begeistert, welche Spiele es spielt, welchen Creators es folgt. Das schafft Offenheit und ermöglicht frühe Einordnung problematischer Inhalte. Fragen Sie regelmäßig: Was hast du heute gesehen? Wer hat dir geschrieben? Kinder die wissen dass sie ohne Strafe erzählen können, melden Probleme schneller.

6 Cybermobbing und Grooming klar benennen

Kinder können nur schützend reagieren wenn sie wissen was passiert. Erklären Sie altersgerecht was Cybermobbing (Beleidigungen, Ausgrenzung, Bloßstellen) und Grooming (Erwachsene die sich einschleichen) bedeuten und welche Anzeichen es gibt. Anlaufstellen benennen: Nummer gegen Kummer 116 111 (kostenlos, Mo-Sa 9-17 Uhr), JUUUPORT Online-Beratung. Betonen: Wer betroffen ist, hat nichts falsch gemacht.

7 Schulische Angebote aktiv in den Unterricht integrieren

Medienkompetenz ist Schulaufgabe - nicht nur Elternaufgabe. klicksafe.de bietet für Grundschulen das kostenlose Paket „Durchs Jahr mit klicksafe“ (12 Unterrichtseinheiten). Für weiterführende Schulen gibt es jährlich die Digitale Schulstunde zum Safer Internet Day. Schulleitungen sollten Medienbildung fest in die Jahresplanung integrieren.

8 Datenschutz und Rechte am eigenen Bild vermitteln

Kinder teilen Fotos und persönliche Informationen oft unbedacht. Sprechen Sie konkret: Was passiert wenn man ein Foto ohne Erlaubnis weiterleitet? Was bedeutet Standort-Tracking? Das Recht am eigenen Bild gilt auch im Netz. klicksafe bietet Unterrichtsmaterial zu Datenschutz und Privatsphäre, das auch zu Hause nutzbar ist.

9 Vertrauensvolle Ansprechpersonen und Meldewege etablieren

Der wichtigste Schutzfaktor ist kein technisches Tool - es ist das Vertrauen dass das Kind sich melden darf. Machen Sie explizit klar: Wer berichtet, wird nicht bestraft sondern bekommt Hilfe. In Schulen: Vertrauenslehrkräfte benennen, Schulsozialarbeit einbinden und feste, bekannte Meldewege einrichten.

10 Vorfälle ernst nehmen und schnell handeln

Cybermobbing und sexualisierte Belästigung sind keine Bagatellen - sie verursachen schwere psychische Schäden. Sofortmaßnahmen: Screenshots sichern, Inhalte auf der Plattform melden, Schulleitung informieren, bei schweren Fällen Polizei einschalten. Psychologische Unterstützung organisieren und externe Beratungsstellen einbeziehen. Das Kind in alle Schritte mitnehmen: Wir lösen das gemeinsam.

Notizen / nächste Schritte:

Weiterführende Informationen & Hilfe

<https://sicherheit-im-internet.de/kindersicherung/>

Vollständiger Artikel mit technischen Anleitungen und Einstellungen

<https://www.klicksafe.de>

EU-Initiative: Materialien für Eltern, Lehrkräfte und Schulen

<https://www.internet-abc.de>

Altersgerechter Internet-Einstieg für Kinder

<https://www.bsi.bund.de>

BSI: Empfehlungen zu Kindern und Jugendlichen im Internet

116 111 - Nummer gegen Kummer

Kostenlos, vertraulich, Mo-Sa 9-17 Uhr - für Kinder und Eltern

<https://www.juuuport.de>

JUUUPORT: Online-Beratung von Jugendlichen für Jugendliche

Diese Checkliste kann frei ausgedruckt und weitergegeben werden. Kein Ersatz für professionelle Beratung. Stand: März 2026 | Alle Angaben ohne Gewähr.

www.sicherheit-im-internet.de