

# TECHNISCHER KINDERSCHUTZ IM INTERNET



Co-funded by  
the European Union



# INHALTS VERZEICHNIS

---

<b>I. Kinderschutz im Internet .....</b>	<b>4</b>
Digitaler Alltag von Kindern und Kinderschutz .....	5
Was ist technischer Kinderschutz und auf welchen Geräten ist er möglich? .....	5
Eltern sind der effektivste Kinderschutz im Internet .....	7
Technischen Kinderschutz besprechen.....	7
Was ist in welchem Alter sinnvoll? .....	7
Tipps .....	10
<b>II. Überblick – Welche Funktionen gibt es? .....</b>	<b>12</b>
Inhalte steuern: Content-Filter und Sperren .....	13
Zeitbeschränkung setzen.....	16
Sichere Umgebung schaffen (Sandbox).....	17
Blockieren von Anwendungen.....	18
Aufzeichnen der Online-Aktivitäten .....	19
Aufenthaltsorte mitverfolgen/Geofencing (GPS-Tracking) .....	20
Kostenfallen auf mobilen Endgeräten deaktivieren .....	22
Inhalte für bestimmte Altersgruppen .....	24
<b>III. Leitfaden für die Praxis – Wie stellt man Kinderschutzmaßnahmen ein?.....</b>	<b>26</b>
Wie stellt man Kinderschutzmaßnahmen ein? .....	27
Computer, Standgeräte, Laptop und Pc.....	27
Kinderschutz im Browser.....	29
Mobile Geräte: Smartphone und Tablet.....	30
Einstellungen durch Apps von Drittanbietern .....	31
Einstellungen durch die Mobilfunk-/Internetanbieter .....	33
Router mit Kinderschutz/WLAN .....	35
Kinderschutzmaßnahmen der Plattformen .....	36
Spielekonsole .....	37
Smart Toys .....	41
GPS-Kinderuhren .....	42
<b>IV. Linkliste .....</b>	<b>43</b>

# 01

# KINDERSCHUTZ IM INTERNET



# **DIGITALER ALLTAG VON KINDERN UND KINDERSCHUTZ**

Nutzer:innen von digitalen Geräten werden immer jünger. Egal ob PC, Tablet, Spielkonsole, smartes Spielzeug oder Smartphone, die junge Zielgruppe wächst zunehmend. Die Saferinternet.at-Studie, die 2020 präsentiert wurde, belegt, dass sich 72 Prozent der Null- bis Sechsjährigen mit internetfähigen Geräten beschäftigen. Die Studie „Digitale Medien im Volksschulalter“, die im Rahmen des Safer Internet Day 2018 von Saferinternet.at veröffentlicht wurde, zeigt, dass die Kinder mit Tablets bzw. Smartphones von älteren Geschwistern oder den Eltern bereits online sind, bevor sie eigene Geräte haben.

Viele Eltern fühlen sich nicht wohl dabei, wenn ihre Kinder unbeaufsichtigt Zugang zu allen Inhalten im Internet haben, und möchten deshalb auf technischen Kinderschutz zurückgreifen. Das ist verständlich, denn Kinder und Jugendliche sollen in Österreich gemäß den verschiedenen Jugendschutzgesetzen vor potenziell gefährdenden Inhalten wie Gewaltverherrlichung und Pornografie geschützt werden. Die Weitergabe dieser Inhalte an Minderjährige ist daher klar untersagt. Eltern sollen Kinder darüber aufklären, welche Medieninhalte verboten sind, und Unterstützung anbieten, wenn sie dennoch mit derartigen Inhalten (z. B. als Mutprobe durch Gleichaltrige)

konfrontiert werden. Sollten etwa illegale Inhalte auf dem Mobiltelefon Minderjähriger gefunden werden, sind diese zu löschen, wobei rechtlich weder eine Überwachung noch regelmäßige Kontrollen vorgeschrieben sind.

## **WAS IST TECHNISCHER KINDER- SCHUTZ UND AUF WELCHEN GERÄTEN IST ER MÖGLICH?**

---

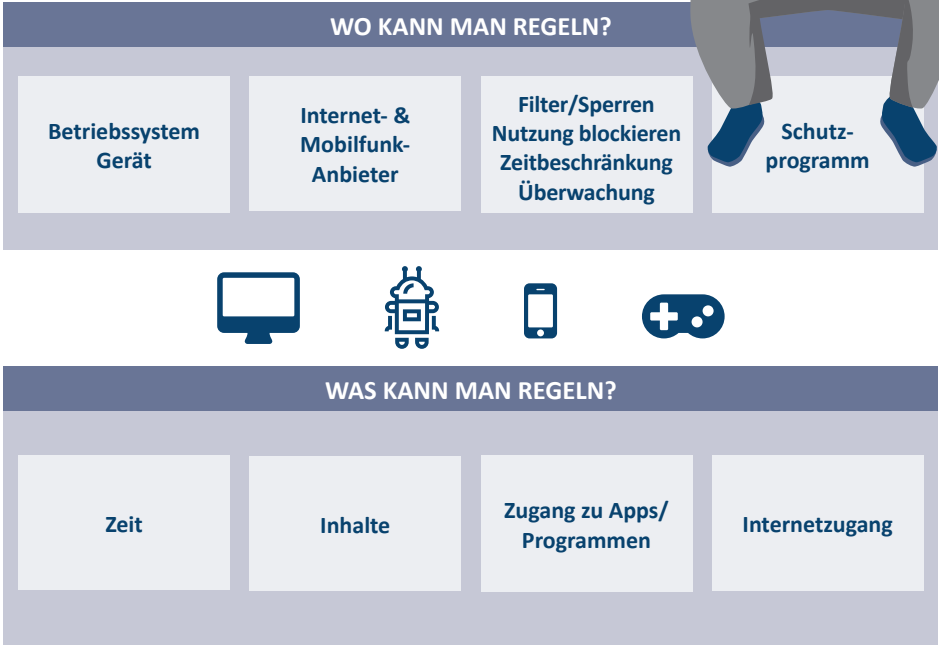
Technische Kinderschutzmaßnahmen gibt es viele. Sie alle kombinieren in der Regel verschiedene Funktionen, um unpassende Inhalte von Heranwachsenden fernzuhalten. Dabei geht es meistens um das Festlegen von Nutzungszeiten, das Filtern von Inhalten und das Blockieren bestimmter Anwendungen. Außerdem können die Tätigkeiten und Aufenthaltsorte der Kinder überwacht und dokumentiert werden.

Kinderschutz ist auf allen Geräten möglich, die von Kindern genutzt werden, also Smartphones, Tablets, Laptops, Stand-PCs, Spielkonsolen und sogar auf sogenanntem smartem Spielzeug und Kinderuhren.

Aber technischer Kinderschutz ist keine absolut sichere Lösung. In sozialen Netzwerken, Tauschbörsen, Foren, Chats, Messengerdiensten sowie bei Cybergrooming und Cybermobbing greifen technische Hilfsmittel nicht. Laut einer EU-Kids-Online-Studie ist Cybermobbing das Problem, das die Kinder am meisten verunsichert, mehr noch als pornografische Bilder

oder Nachrichten. Da keine Filter vor Cybermobbing schützen, ist es auch bei Einsatz von Kinderschutzmaßnahmen wichtig, die Heranwachsenden im Umgang mit dem Internet zu unterstützen und sie über Gefahren zu informieren. Den Zugang zu Inhalten im Internet zu filtern, ist dabei nur ein Teil der Problemlösung. Dennoch können Kinderschutzsoftware und restriktive Einstellungen auf den Geräten vor allem bei jüngeren Kindern eine Hilfe sein. Am wichtigsten ist, dass die Verantwortung für ein sicheres und positives Internet-Umfeld nicht ausschließlich an die Technik delegiert wird. Eltern sollen sich gemeinsam mit ihren Kindern mit den Inhalten auseinandersetzen

und die Medienkompetenz der Kinder fördern. Diese von ISPA in Zusammenarbeit mit Safe-rinternet.at erstellte Broschüre bietet einen Überblick über die Möglichkeiten des technischen Kinderschutzes an unterschiedlichen Geräten und allgemeine Praxistipps, welche Einstellungen sich wo vornehmen lassen.



## ELTERN SIND DER EFFEKTIVSTE KINDERSCHUTZ IM INTERNET

---

Ein wichtiger Punkt ist das gemeinsame Nutzen von digitalen Medien. Am besten lässt man sich von den Kindern zeigen, was sie gerne online machen. Dadurch bekommen die Eltern ein Gefühl dafür, wie sie das Kind beim sicheren Surfen unterstützen können. Aufmerksamkeit und Offenheit sind zentral, damit Kinder sich bei Problemen an die Eltern wenden können. Wenn das Kind im Internet auf eine schwierige oder verstörende Situation stößt, ist es wichtig, Verständnis zu zeigen und das Problem ruhig zu lösen, wenn nötig mithilfe von Expert:innen („147 Rat auf Draht“, Stopleveline.at, Internet Ombudsstelle, Saferinternet.at). Keinesfalls sollten Kinder für den Kontakt mit nicht für sie bestimmten Inhalten bestraft werden oder Internetverbot erhalten, da sie sich sonst beim nächsten Mal mit ihrem Problem womöglich nicht mehr an die Eltern wenden.

Um Kinder und Jugendliche zu bewussten, interessierten und kritischen Online-Nutzer:innen auszubilden, sollen sie ihren Interessen entsprechend in einem sozial verantwortlichen Umgang mit Online-Medien unterstützt und gefördert werden. Die Beziehung zwischen Heranwachsenden und Eltern verändert sich ständig, und das Ziel sollte immer eine möglichst offene Gesprächsbasis ohne Verurteilungen und mit klaren Regeln sein.

## TECHNISCHEN KINDERSCHUTZ BESPRECHEN

---

Jedes Kind hat ein Recht auf Privatsphäre (Art. 16 KRK), und eine Totalüberwachung der Internetaktivitäten würde diese beschneiden. Es soll also ein Gleichgewicht zwischen der Wahrung der Privatsphäre des Kindes und Maßnahmen zum Schutz des Kindes angestrebt werden. Das Kind soll jedenfalls darüber informiert werden, welche Maßnahmen gesetzt wurden und wie diese genau aussehen. Der Einsatz von Kinderschutzsoftware soll an das Alter des Kindes angepasst sein, damit das Kind in seiner Entwicklung nicht davon abgehalten wird, sich selbst Bewältigungsmechanismen anzueignen. Problematisch kann z. B. eine zu strenge Blacklist sein, die Seiten sperrt, obwohl sie gar nicht bedenklich für Kinder sind. Eine normale Nutzung des Internets ist in diesem Fall nicht mehr möglich, und auch die positiven Möglichkeiten sind eingeschränkt.

## WAS IST IN WELCHEM ALTER SINNVOLL?

---

Je jünger Kinder sind, desto eher werden technische Schutz- oder Überwachungsmaßnahmen greifen und sinnvoll sein. Mit zunehmendem Alter werden diese von den Kindern oft umgangen. Außerdem können sie die Geräte ihrer Freund:innen nutzen, um an Inhalte zu gelangen, die möglicherweise zu Hause verboten sind. Eltern wähnen sich dann in einer vermeintlichen Sicherheit, die tatsächlich aber nicht gegeben sein muss.

Folgende Empfehlungen von Saferinternet.at geben einen Überblick über sinnvolle Maßnahmen – angepasst an das Alter der Kinder und Jugendlichen.

ALTER	INHALTE BESCHRÄNKEN	ZEIT BESCHRÄNKEN
0 - 3 JAHRE	<ul style="list-style-type: none"> <li>• sehr wichtig</li> <li>• nicht allein nutzen, z. B. kein Autoplay in YouTube</li> </ul>	<ul style="list-style-type: none"> <li>• durch Eltern steuern</li> <li>• sehr kurze Zeitspannen, max. 3–7 min</li> </ul>
4 - 7 JAHRE	<ul style="list-style-type: none"> <li>• wichtig</li> <li>• Begleitung der Eltern</li> </ul>	<ul style="list-style-type: none"> <li>• je nach Alter, Aufgaben, Tagesablauf und Konzentrationsfähigkeit des Kindes unterschiedlich</li> <li>• Eltern müssen Rahmen schaffen, Kinder brauchen alternative Beschäftigungen</li> <li>• max. 30–60 min (auf allen digitalen Geräten mit Bildschirmen) pro Tag</li> <li>• vor dem Schlafengehen 1 h bildschirmfrei</li> </ul>
8 - 11 JAHRE	<ul style="list-style-type: none"> <li>• wird zunehmend weniger wichtig</li> </ul>	<ul style="list-style-type: none"> <li>• bei manchen Kindern notwendig</li> <li>• Ziel muss sein, dass Kinder die Zeit selbst einschätzen und steuern können</li> <li>• im Zeitraum von 6 bis 20 Uhr erlauben, Nacht ist frei von digitalen Geräten</li> <li>• max. 120 min pro Tag</li> </ul>
12 - 14 JAHRE	<ul style="list-style-type: none"> <li>• eher nein, da die Beschränkung oft umgangen wird</li> </ul>	<ul style="list-style-type: none"> <li>• bei manchen Kindern notwendig</li> <li>• Ziel muss sein, dass Kinder die Zeit selbst einschätzen und steuern können</li> <li>• im Zeitraum von 6 bis 21 Uhr erlauben, Nacht ist frei von digitalen Geräten</li> </ul>
15+ JAHRE	<ul style="list-style-type: none"> <li>• kontraproduktiv</li> </ul>	<ul style="list-style-type: none"> <li>• nur in Ausnahmefällen, dann nach Absprache</li> </ul>





## FUNKTIONEN SPERREN

- auf ganz wenige beschränken (Sandbox)
- auch Handys der Eltern entsprechend einrichten

- Apps nicht allein installieren
- Kostenfallen sperren
- bei Online-Spielen auf Rahmenbedingungen achten (z. B. gemeinsames Spielen mit Fremden)
- Fotos und Spiele: eigene Inhalte nur lokal am Gerät speichern

- Kostenfallen sperren
- Apps gemeinsam installieren, Kind hat Vorschlagsrecht

- Kostenfallen sperren
- in Ausnahmefällen auch Funktionen sperren (aber notwendigen Kontakt zu Freund:innen ermöglichen)

- Kostenfallen in Absprache sperren
- Passwort und Gerät im Besitz des Kindes

## ÜBERWACHEN

- durch Begleitung, da alleinige Nutzung nicht sinnvoll

- GPS-Tracker nicht ohne Wissen der Kinder
- Inhalte gemeinsam reflektieren (am Abend Verlauf und Tätigkeiten miteinander anschauen – ohne Vorwürfe an Kinder)

- GPS-Tracker nicht ohne Wissen der Kinder
- Inhalte gemeinsam reflektieren (am Abend Verlauf und Tätigkeiten miteinander anschauen – ohne Vorwürfe an Kinder)

- GPS-Tracker nur in Ausnahmefällen
- Inhalte fallweise miteinander reflektieren, keine Überprüfungen ohne Wissen und Beisein des Kindes

- keine Überwachung bzw. nur in Ausnahmefällen

**TIPP:** Haben Kinder noch kein eigenes Gerät, sondern nutzen die Geräte der Eltern oder Geräte, die die ganze Familie verwendet, so sollten auch diese entsprechend eingerichtet werden.

Denn in der Regel machen Kinder schon lange, bevor sie ihre ersten Geräte besitzen, Erfahrungen mit dem Internet, auch wenn die eigenen Eltern das nicht immer so wahrhaben wollen. Wenn Eltern dem Kind das eigene Gerät zum Spielen überlassen, sollten gewisse Sicherheitsmaßnahmen gesetzt werden. Erfordert das Spiel z. B. keine Internetverbindung, können WLAN bzw. mobile Daten deaktiviert werden.

Eine andere Möglichkeit ist, dass auch auf dem Elternhandy ein Kinderschutzprogramm installiert wird, das bei Bedarf aktiviert wird.

## **TIPPS FÜR DAS EINRICHTEN VON SCHUTZMASSNAHMEN**

---

- Geben Sie Passwörter niemals an Kinder weiter.
- Richten Sie eigene Kinder-Accounts bzw. -Profile auf den Geräten ohne Administrationsrechte ein.
- Bevor man zusätzliche Kinderschutzprogramme installiert, ist es ratsam, sich genau zu informieren. Eventuell bieten das Betriebssystem und der Anbieter schon ausreichend Hilfestellung.
- Suchen Sie auf Video-Plattformen oder in Suchmaschinen nach den Programmen, die Sie für den Kinderschutz verwenden möchten. Ihre Kinder tun das auch und erhalten so Tipps, wie sie den Kinderschutz umgehen können.

# TIPPS FÜR ELTERN



Nutzen Sie digitale Medien **gemeinsam**. Lassen Sie sich zeigen, was ihr Kind gern online macht und unterstützen Sie es beim sicheren Surfen durchs Internet.



Seien Sie **aufmerksam** und offen, damit Ihr Kind Vertrauen hat, sich bei Problemen im Internet an Sie zu wenden.



Richten Sie für Ihr Kind jeweils ein **eigenes Profil** mit entsprechenden Kinderschutzmaßnahmen ein, wenn Sie internetfähige Geräte gemeinsam benutzen.



Informieren Sie sich über **Vor- bzw. Nachteile** in Bezug auf Ihre Anforderungen, bevor Sie ein bestimmtes Kinderschutzprogramm einsetzen.



Bei konkreten Erziehungsfragen bietet die **Elternseite von 147 - Rat auf Draht** Unterstützung.



Sollten Sie online auf sexuelle Missbrauchsdarstellungen von Kindern stoßen, melden Sie diese anonym unter **[www.stopline.at](http://www.stopline.at)**.

# 02

## ÜBERBLICK – WELCHE FUNKTIONEN GIBT ES?



## ÜBERBLICK – WELCHE FUNKTIONEN GIBT ES?

Um einen Überblick über die Funktionen des technischen Kinderschutzes zu geben, werden folgend die gängigsten Möglichkeiten vorgestellt. Die verfügbaren Kinderschutz-Produkte bieten zumeist eine bestimmte Kombination der hier vorgestellten Funktionen. Mit den konkreten Kinderschutz-Produkten beschäftigt sich anschließend das Kapitel „Leitfaden – Wie stellt man Kinderschutzmaßnahmen ein?“.

### INHALTE STEUERN: CONTENT-FILTER UND SPERREN

---

Filterprogramme können entweder auf dem Gerät oder beim Internetzugang, also direkt beim Provider, implementiert werden. Dabei werden unterschiedliche Filterungssysteme genutzt, die teilweise auch in Kombination auftreten. Wer die Auswahl und Einrichtung der Filter vornimmt, muss daher selbst bereits sehr genau wissen, welche Inhalte ausgeschlossen und welche zugelassen werden sollen.

#### STICHWORT-FILTER

Die einfachste Form ist das Keyword-Blocking (Stichwort-Filterung), das alle Seiten sperrt, die bestimmte „verbotene Wörter“ enthalten. Bei dieser einfachen Form des Filterns werden alle Wörter einer Website nach bestimmten Stichwörtern, die in einer Datenbank bzw. Liste vermerkt sind, durchsucht. In dieser Datenbank steht z. B. das Stichwort „Sex“ als Kriterium, eine Website nicht anzuzeigen. Dies würde bedeuten, dass alle Seiten, die die Zeichenfolge „Sex“ beinhalten, blockiert werden. Diese einfache Filterung würde aber auch Seiten ausfiltern, die das Wort „RechtSEXpertise“ beinhalten. Deshalb werden in modernen Kinderschutzprogrammen intelligente Filtersysteme eingesetzt. Hier entscheiden mehrere Faktoren darüber, ob ein Angebot zugänglich ist oder nicht. So untersuchen z. B. Filtersysteme die Websites nach bestimmten Mustern und blockieren Seiten, die als problematisch eingeschätzt werden. Die Datenbanken und Listen im Hintergrund gibt es trotzdem, es wird aber nicht jede Übereinstimmung von Zeichenfolgen zu einer Blockierung führen. Die intelligenten Filtersysteme werten verschiedene typische Merkmale einer Website aus (z. B. statistische Analyse des gesamten Textes einer Website), um sie automatisiert zu kategorisieren.

#### URL-FILTER, INHALTE-FILTER (BLACKLIST UND WHITELIST)

Mithilfe von Kinderschutzfiltern können Websites blockiert werden, die für Kinder unangemessen sind. Dazu werden als für Kinder ungeeignet eingestufte URLs auf einer sogenannten Blacklist vermerkt. Versucht das Kind, eine Website zu öffnen, wird die eingegebene URL mit jenen

auf der Blacklist abgeglichen. Stimmt die vom Kind eingegebene URL mit einer auf der Blacklist überein, wird der Zugriff verweigert. An ihre Grenzen stößt die Blacklist bei Inhalten, die noch nicht auf der Blacklist vermerkt wurden (weil sie z. B. so neu sind oder andere Websites zur Umgehung der Sperre dienen), deshalb werden sie nicht durch den Filter erfasst und angezeigt. Kinderschutzprogramme liefern meist eine Blacklist mit, die aktualisiert werden muss und oft individuell bearbeitet werden kann. Die umgekehrte Vorgehensweise beim Filtern erfolgt mithilfe einer Whitelist. Bei Aktivierung des Kinderschutzes können nur mehr URLs abgerufen werden, die zuvor auf dieser Liste vermerkt worden sind, alle anderen URLs sind gesperrt. Durch diese Filtermethode wird zwar fast ausgeschlossen, dass unpassende Inhalte angezeigt werden, die Nutzung des Internets ist aber nur mehr sehr eingeschränkt möglich. Seiten, die kindgerechte Inhalte zeigen, aber nicht auf der Liste vermerkt sind, werden dennoch ausgefiltert. Ein reines Whitelist-System wird daher selten eingesetzt. Eine Kombination aus White- und Blacklist kommt bei den meisten Programmen zum Einsatz. Durch die URL-Filterung können oft auch gesamte Gruppen von Websites ausgeschlossen werden, z. B. Filesharing-Dienste, soziale Netzwerke etc.

Um sicherzugehen, dass sich bestimmte URLs nicht bzw. doch aufrufen lassen, ist es sinnvoll, Black- und Whitelist individuell anzupassen. Außerdem sollte darauf geachtet werden, dass Updates von den Herausgebern zur Verfügung gestellt werden. Bei der Auswahl des Kinderschutzprogramms können diese Faktoren neben Alter und Erfahrung des Kindes Kriterien sein, welches Produkt besser den Bedürfnissen des Kindes und der Eltern entspricht.

## **EINSATZ VON FILTERN**

Diese beiden Grundkonzepte der Filterung werden inzwischen in fast allen Filterprogrammen kombiniert, um die Wirksamkeit zu erhöhen, aber auch, um altersdifferenzierte Zugänge zu schaffen. Die zahlreichen Filterprogramme auf dem Markt werden ständig weiterentwickelt und dem aktuellen technischen Standard angepasst. Allerdings arbeitet keiner dieser „Internetaufpasser“ absolut zuverlässig. So filtern diese Programme auch Unbedenkliches aus oder lassen problematische Inhalte durchgehen, weil die Software den tatsächlichen Inhalt von Webangeboten eben nicht erkennen kann.

VORTEILE	NACHTEILE
<ul style="list-style-type: none"> <li>• Für Kinder unpassende Inhalte werden nicht angezeigt.</li> </ul>	<ul style="list-style-type: none"> <li>• Internetnutzung ist stark eingeschränkt.</li> <li>• Filter sind fehleranfällig, sie können den konkreten Inhalt nicht erkennen</li> <li>• Je nachdem auf welcher Ebene (Smartphone, Laptop, Router, Spielkonsole) der Filter installiert ist, ist er auch nur begrenzt wirksam.</li> <li>• Kinder finden meist andere Möglichkeiten (z. B. bei Freund:innen).</li> </ul>

### FÜR WELCHE KINDER SIND FILTER GEEIGNET?

Bei jüngeren Kindern (bis sieben Jahre) kann der Einsatz von Filtern sinnvoll sein, um die konsumierten Inhalte zu beschränken. Obwohl gerade sie beim Surfen durch Erwachsene begleitet werden sollen, kann der Einsatz von Filtern hilfreich sein. Ab einem gewissen Alter bzw. wenn das Kind bereits technische Kompetenzen erworben hat, sind Filter eher ungeeignet, da die Filtersoftware oft umgangen oder außer Kraft gesetzt wird.

### AUFWAND FÜR DIE ELTERN

Die Filter sollen an die Bedürfnisse des Kindes angepasst werden, weshalb die Einrichtung durchaus aufwendig sein kann. Viele Kinderschutzprogramme bieten deshalb verschiedene Eingabemasken an, die funktionell und einfach sein sollen. Ein-Klick-Lösungen gibt es aber trotzdem nicht, denn die einzelnen Funktionen können und sollen individuell angepasst werden, um die individuellen Bedürfnisse der Familie zu erfüllen. Wer z. B. ein aufwendiges Whitelist-System verwenden möchte, muss sich vorab erst informieren, welche Seiten freigegeben werden sollen.

## ZEITBESCHRÄNKUNG SETZEN

Einen zeitlichen Rahmen festzulegen, wann und wie lange das Kind online sein darf, kann durchaus sinnvoll sein. Manche Kinderschutzprogramme bieten ein umfassendes Zeitmanagement an. Je nach Ausführung lässt sich ein absolutes Zeitkontingent einstellen. Verfeinerte Systeme bieten eine Unterscheidung an, für welche Inhalte wie viel Zeit zur Verfügung steht. Bei manchen Softwarelösungen können auch unterschiedliche Zeitlimits für Schultage und Wochenenden festgelegt werden. Ist das Limit erreicht bzw. wird versucht, zu einem Zeitpunkt außerhalb des definierten Zeitraums online zu gehen, wird der Zugriff verweigert.

Medienfreie Zeiträume einzurichten, kann sich positiv auswirken, und technische Zeitlimits können dabei helfen, diese auch durchzusetzen. Zeitlimits und Nutzungsregeln sollten aber immer gemeinsam mit den Kindern erarbeitet werden und für alle Personen im Haushalt gelten. Unterstützung beim Aufstellen der Regeln für digitale Medien findet man im Artikel „Wie stellen wir Familienregeln für Internet und Handy auf?“ von Saferinternet.at.

VORTEILE	NACHTEILE
<ul style="list-style-type: none"><li>• automatisches Abschalten bzw. Verweigerung des Zugriffs</li><li>• keine Diskussionen mit dem Kind, dass es nun aufhören muss</li></ul>	<ul style="list-style-type: none"><li>• Kinder lernen nicht selbst, wann es genug ist</li><li>• frustrierend für das Kind, wenn im „falschen“ Moment abgeschaltet wird</li></ul>

## FÜR WELCHE KINDER SIND ZEITBESCHRÄNKUNGEN GEEIGNET?

Vor allem bei sehr jungen Kindern ist eine Zeitbeschränkung sinnvoll, die aber auch ohne technische Mittel durchsetzbar ist, da die Kinder ohnehin nicht allein mit den digitalen Geräten hantieren. Bei Kindern, die selbstständig mit Geräten aktiv sind und nicht abschätzen können, wie lange sie schon spielen bzw. surfen, kann die automatische Zeitbeschränkung sinnvoll sein. Ziel muss aber sein, dass Kinder selbst in der Lage sind zu steuern, wie viel Zeit sie mit digitalen Medien verbringen, und sich selbst einschränken.

## AUFWAND FÜR DIE ELTERN

Zeitbeschränkungen einzurichten, kann mitunter aufwendig sein, wenn differenzierte Einstellungen möglich sind. Gibt es nur ein absolutes Zeitlimit pro Tag, hält sich der Aufwand in Grenzen. Möchte man aber unterschiedliche Zeiten für unterschiedliche Wochentage/Programme/Geräte einstellen, ist die Wartung dementsprechend mit Arbeit verbunden.



## SICHERE UMGEBUNG SCHAFFEN (SANDBOX)

Viele Kinderschutzeangebote arbeiten mit einer Art Sandbox (Sandkiste), um den Kindern die Bewegung in einer sicheren Umgebung zu ermöglichen. Nur zuvor definierte Apps und Programme können verwendet werden, der Rest der Applikationen und Funktionen des Geräts steht nicht zur Verfügung. In der sicheren Umgebung kann das Kind auch herausfinden, wie man mit dem Gerät umgeht, und, solange die Sandbox aktiv ist, die Software gefahrlos ausprobieren. Darin ausgeführte Programme erhalten nur einen simulierten Zugriff auf das Betriebssystem und können daran keine potenziell gefährlichen Änderungen vornehmen. Die Sandbox lässt sich je nach Bedürfnis des Kindes mit mehr oder weniger möglichen Funktionen ausstatten.

Ist die Sandbox aktiv, ist die Nutzung des jeweiligen Geräts sehr eingeschränkt. Die Eltern sollten sich aber nicht in falscher Sicherheit wiegen, denn oft gibt es Möglichkeiten für die Kinder, die Sandbox zu verlassen. Obwohl es sich hier um Fehlfunktionen der jeweiligen Programme handelt, scheinen die Programmhersteller dieses Problem noch nicht vollständig gelöst zu haben.

### VORTEILE

- Eltern haben die Kontrolle darüber, welche Dinge das Kind am Computer, Smartphone oder Tablet machen kann.
- Geräteeinstellungen können nicht verändert werden.
- Unerwünschte Programme können nicht verwendet werden.
- In der sicheren Umgebung kann das Kind vieles ausprobieren, ohne nachhaltigen Schaden anzurichten.

### NACHTEILE

- Die Kinder können die Geräte nur sehr eingeschränkt nutzen.
- Ein zu restriktives Vorgehen verwehrt den Kindern die Möglichkeit, sich auch in unbekannten Terrains zurechtzufinden.
- Die jungen Nutzer:innen können dadurch keine neuen Funktionen entdecken und sich selbst beim Ausprobieren keine neuen Kompetenzen aneignen.

## FÜR WELCHE KINDER IST EINE SANDBOX GEEIGNET?

Diese Art von Einschränkung ist bei jüngeren Kindern bis sechs Jahre sinnvoll. Je älter ein Kind wird, desto weniger entspricht diese Einschränkung den Bedürfnissen des Kindes. Oftmals wissen ältere Kinder auch, wie sie die Sandbox verlassen, weshalb sie dann keinen Schutz mehr bietet.

## AUFWAND FÜR DIE ELTERN

Die Sandbox-Funktion ist meistens in den Kinderschutzprogrammen und -Apps integriert und kann auf Wunsch aktiviert werden. Oft ist die Aktivierung mit wenigen Klicks möglich. Aufwendig wird erst die Anpassung an die Bedürfnisse des Kindes. Einzelne Funktionen und Programme/Apps müssen häufig extra freigeschaltet werden, um sie nutzen zu können. Ein Beispiel: Wenn nur drei Apps auf dem Gerät benutzt werden, ist der Aufwand relativ gering. Wenn das Kind aber immer neue Apps nutzen möchte, müssen sich die Eltern auch vergewissern, dass diese für das Kind geeignet sind, und sie dann manuell freischalten. Je nachdem wie oft dies vorkommt, kann das durchaus zeitintensiv sein.

## BLOCKIEREN VON ANWENDUNGEN

Wenn diese Funktion aktiviert ist, kann etwa das Starten eines Protokolls einer Anwendung blockiert werden, z. B. Streaming-Anwendungen oder Video-Anwendungen. Ob die blockierte Anwendung bzw. das blockierte Protokoll inhaltlich für die jungen Nutzer:innen angemessen ist, wird nicht überprüft. Es werden alle zuvor definierten Anwendungen und Protokolle gesperrt, ungeachtet ihres Inhalts und ihrer Bedeutung.

VORTEILE	NACHTEILE
<ul style="list-style-type: none"><li>• Eltern können kontrollieren, welche Anwendungen das Kind verwendet.</li></ul>	<ul style="list-style-type: none"><li>• Inhalte werden ungeachtet ihres Inhalts blockiert.</li></ul>

## FÜR WELCHE KINDER IST DAS GEEIGNET?

Für Kinder, deren Eltern nicht möchten, dass sie bestimmte Anwendungen wie z. B. Chats, soziale Medien, Streamingdienste, Spiele oder diverse andere Programme verwenden.

## AUFWAND FÜR DIE ELTERN

In der Einrichtung bzw. Aktivierung ist die Funktion meistens nicht sehr aufwendig. Die Überlegungen dahinter, welche Anwendungen man als Elternteil sperren möchte, sind das aber sehr wohl. Wer nicht möchte, dass Kinder Social-Media- oder Chat-Anwendungen nutzen, kann diese zwar sperren, aus der Lebenswelt der Kinder sind sie aber trotzdem nicht weg. Kinder und Jugendliche tauschen sich gerne mit ihren Freund:innen aus, und heutzutage werden dafür zumeist elektronische Kommunikationsmittel verwendet.

## AUFZEICHNEN DER ONLINE-AKTIVITÄTEN

Eltern sollten einen groben Überblick darüber haben, was die Kinder im Internet machen. Viele Eltern greifen deshalb zu Software, die die Aktivitäten und auf Wunsch auch die Aufenthaltsorte der Kinder aufzeichnet. Dies steht jedoch im Widerspruch zum Recht des Kindes auf Privatsphäre (Art. 16 KRK), weshalb Kontrollen immer im Einverständnis mit den Kindern durchgeführt werden sollten. Auf jeden Fall sollte das Kind informiert werden, dass seine Online-Aktivität dokumentiert wird, und genau gezeigt bekommen, was konkret aufgezeichnet wird. Eine geheime Totalüberwachung untergräbt das Vertrauen zwischen Kindern und Erwachsenen und erschwert die Kommunikation über Herausforderungen, denen das Kind im Internet begegnet.

Die Möglichkeiten der Aufzeichnung reichen von der ausschließlichen Dokumentation der besuchten Websites bis hin zu detaillierten Nutzungsdaten (Verweildauer auf Bildern, Schweben mit der Maus über Begriffen, Herunterladen von Inhalten etc.).

Manche Programme bieten auch die Möglichkeit einer automatisierten statistischen Auswertung. Wer lieber selbst das Material durchsehen möchte, kann durchaus von der Menge an Daten überfordert sein. Die Programme bieten eine Hilfestellung, die Daten zu strukturieren und dadurch überschaubar zu machen.

### VORTEILE

- Man erhält einen Überblick über die Aktivitäten des Kindes im Internet.

### NACHTEILE

- Das Recht auf Privatsphäre (Art.16 KRK) kann unter Umständen verletzt werden.
- Die Aufzeichnung allein bietet keinen Schutz für das Kind, weil es einen Weg finden wird, Inhalte zu konsumieren, die „nicht erlaubt“ sind.
- Nur weil am Smartphone bzw. PC des Kindes in der Aufzeichnung nichts Auffälliges auftaucht, bedeutet das nicht, dass keine ungeeigneten Inhalte konsumiert werden (z. B. bei Freund:innen).

## FÜR WELCHE KINDER IST ES GEEIGNET?

Jedes Kind hat ein Recht auf Privatsphäre, deshalb sollte diese Art von Überwachung nur dann eingesetzt werden, wenn die Kinder zuvor darüber aufgeklärt wurden. Je älter die Kinder sind, desto unpassender ist eine Totalüberwachung.

## AUFWAND FÜR DIE ELTERN

Je nachdem wie aktiv die Kinder im Internet sind, sind auch die dokumentierten Tätigkeiten mehr oder weniger umfangreich. Manche Programme bieten eine statistische Auswertung an, die den Eltern die Kontrolle erleichtern soll.

**TIPP:** Machen Sie es zur Routine, am Ende des Tages gemeinsam die Verläufe anzuschauen, wenn Kinder anfangen, das Internet ohne erwachsene Begleitung zu erforschen. Seien Sie neugierig und lassen Sie sich von der Begeisterung der Kinder anstecken. So schaffen Sie eine Vertrauensbasis, kennen die Vorlieben des eigenen Kindes und müssen nicht auf geheime Kontrollen zurückgreifen.

## AUFENTHALTSORTE MITVERFOLGEN/GEOFENCING (GPS-TRACKING)

Unter Geofencing versteht man im Zusammenhang mit digitalem Kinderschutz die Möglichkeit, einen Raum zu definieren, in dem sich das Kind frei bewegen kann (z. B. Schulweg und nähere Umgebung des Wohnorts). Zu diesem Zweck wird der Standort des Kindes mittels GPS in der Regel durch das Smartphone oder ein spezielles Gerät wie eine spezielle Kinderuhr übermittelt. Verlassen Kind und Gerät die definierte Gegend, wird am Smartphone der Eltern ein Signal ausgelöst. Da es sich bei Standortdaten um sensible Daten handelt, sollten regelmäßige Sicherheitsupdates durchgeführt werden. Bei der Auswahl der Geräte sollte deshalb darauf geachtet werden, dass der Hersteller spätere Updates ermöglicht bzw. zur Verfügung stellt.

### VORTEILE

- Als Elternteil weiß man zu jeder Zeit, wo sich das Kind bzw. das GPS-sendende Gerät gerade befindet.

### NACHTEILE

- Das GPS-Signal kann innerhalb von Gebäuden oder Fahrzeugen abgeschwächt sein.
- Bei schwacher Mobilfunkabdeckung können die GPS-Geräte keine Positionsmeldungen mehr absenden.
- Die versendeten Daten sind nicht zuverlässig, da die GPS-Sender sehr fehleranfällig sind.
- Damit die Funktion eingesetzt werden kann, muss der GPS-Tracker aktiv sein, eine Datenübertragung an Dritte, z. B. den Hersteller, kann nicht ausgeschlossen werden.
- Da ständig GPS-Signale gesendet werden, ist auch der Batterie- bzw. Akkuverbrauch erhöht.
- Das Kind kann unvorsichtig werden, wenn es sich in falscher Sicherheit wiegt, weil die Eltern vermeintlich sowieso wissen, wo es gerade ist.
- Dem Kind wird verwehrt, selbst Alltagsprobleme zu lösen.
- Das Recht auf Privatsphäre (Art.16 KRK) kann unter Umständen verletzt werden.

### FÜR WELCHE KINDER IST ES GEEIGNET?

Jedes Kind hat ein Recht auf Privatsphäre, deshalb sollte diese Art von Überwachung nur in Ausnahmefällen eingesetzt werden. Je älter die Kinder sind, desto unpassender ist eine Totalüberwachung.

## AUFWAND FÜR DIE ELTERN

Die Einrichtung des GPS-Trackers kann unter Umständen sehr aufwendig sein, z. B. wenn die GPS-Uhr erst kalibriert und die sicheren Zonen (Schulweg) erst definiert werden müssen.

**TIPP:** Üben Sie mit Ihrem Kind, wie es sich in Krisensituationen verhalten muss. Denn Kinder, die sich mit ihren Eltern via GPS-Tracker vernetzt wähnen, werden manchmal leichtsinnig, da sie das Gefühl haben, immer von den Eltern geschützt zu sein. Dies ist aber ein Trugschluss, denn Eltern sind nicht physisch anwesend und können im Krisenfall auch nicht schnell eingreifen.

Sinnvolle Maßnahmen können sein:

- weglaufen
- einen Erwachsenen um Hilfe bitten
- sich verstecken
- in ein Geschäft gehen und das Verkaufspersonal um Hilfe bitten
- um Hilfe schreien

## KOSTENFALLEN AUF MOBILEN ENDGERÄTEN DEAKTIVIEREN

Kinder nutzen mobile Endgeräte in einem zunehmend jüngeren Alter. Daher ist es sinnvoll, einzelne Funktionen zu deaktivieren. Diese sind zwar per se meistens nicht jugendgefährdend, führen aber unter Umständen zu Mehrkosten oder anderen negativen Auswirkungen. Die Funktionen können manuell deaktiviert werden bzw. bieten manche Softwarelösungen eine automatische Deaktivierung an.

### MOBILE DATEN DEAKTIVIEREN (BZW. LIMIT SETZEN)

Kinder vermögen nicht gut einzuschätzen, wie viel Datenvolumen sie verbrauchen. Um als Elternteil die Kontrolle darüber zu bewahren, kann ein Datenlimit gesetzt werden. Nach dessen Erreichen wird keine Internetverbindung über die mobilen Daten mehr hergestellt.

### IN-APP-KÄUFE

Sogenannte Free-to-Play-Spiele können kostenlos heruntergeladen werden. Durch kostenpflichtige Zusatzfunktionen ist es möglich, den Spielfortschritt positiv zu beeinflussen. Diese In-App-Käufe lassen sich unterbinden. Dazu setzt man ein Passwort, und in der Folge können die Eltern entscheiden, welche In-App-Käufe durchgeführt werden.

## ROAMING DEAKTIVIEREN

Um zusätzliche Kosten im Ausland zu vermeiden, kann das Roaming deaktiviert werden. 2017 wurde das europaweite EU-Roaming abgeschafft. Das bedeutet, dass Mobilfunkbetreiber keine zusätzlichen Gebühren für Anrufe, SMS und Datenvolumen innerhalb der EU sowie in Norwegen, Liechtenstein und Island verrechnen dürfen. Konkret bedeutet das, dass Anrufe, die aus dem EU-Ausland getätigt werden, nicht mehr kosten dürfen als jene, die im Inland erfolgen. Freieinheiten (Freiminuten und -SMS), die durch das Bezahlen einer Grundgebühr zur Verfügung stehen, können auch im EU-Ausland genutzt werden. Das gilt ebenso für Datenpakete, hier kann der Betreiber aber eine eingeschränkte Nutzung vorgeben. Von inkludierten fünf GB dürften dann z. B. nur zwei GB auch im EU-Ausland genutzt werden.

## WAP- BZW. WEB-BILLING

WAP- bzw. WEB-Billing ist eine spezielle Verrechnungsmöglichkeit von mobilen Diensten, die direkt über die Handyrechnung läuft. Durch das Klicken auf Werbebanner in manchen Gratis-Apps oder auch auf mobilen Website-Versionen kann es zu Abo-Fallen kommen. Kosten und andere Vertragsbedingungen wie Laufzeit oder Kündigungsmöglichkeiten werden dabei nur schwer lesbar dargestellt oder gut versteckt. Erst auf der nächsten Handyrechnung werden diese Dienste verrechnet. Um diese versteckten Kostenfallen zu beseitigen, kann man solche Dienste beim Mobilfunkbetreiber sperren lassen. Dort sind diese unter Namen wie „Contentdienste“, „Premiumdienste“, „Dienste von Drittanbietern“, „Zahlen per Handyrechnung“ oder „digitale Güter“ bekannt.

**TIPP:** Falls Sie oder Ihr Kind in die Falle getappt sind, können Sie die Handyrechnung innerhalb von drei Monaten nach Erhalt beim Mobilfunkbetreiber schriftlich beeinspruchen. Bei Problemen bietet die Rundfunk und Telekom Regulierungs-GmbH ein kostenloses Schlichtungsverfahren an. Die Internet Ombudsstelle berät ebenfalls kostenlos bei Fragen und Problemen.

### VORTEILE

- Eine manuelle Deaktivierung ist auch ohne Kinderschutzsoftware möglich.

### NACHTEILE

- Eine manuelle Deaktivierung ist von Kindern sehr rasch leicht zu umgehen.

## FÜR WEN IST ES GEEIGNET?

Das Deaktivieren von Kostenfallen kann besonders bei jüngeren Kindern vor unliebsamen Überraschungen bewahren. Je älter die Kinder werden, desto mehr sollte jedoch die Medienkompetenz gefördert werden.

## AUFWAND FÜR DIE ELTERN

Bei der manuellen Deaktivierung gibt es für Eltern kaum einen Aufwand, da sich die Einstellungen rasch vornehmen und wieder aufheben lassen. Ist die Deaktivierung von Kostenfallen Teil einer umfangreichen Kinderschutzsoftware, hängt es nicht zuletzt von der Übersichtlichkeit der Software ab, wie umständlich Einstellungen vorgenommen werden können.

## INHALTE FÜR BESTIMME ALTERSGRUPPEN

Damit Kinderschutzprogramme für verschiedene Altersgruppen verschiedene Websites anzeigen, gibt es die Selbstklassifizierung auf Websites. Die Betreiber einer Website können im Quellcode (age-de.xml) angeben, für welche Altersgruppe die Inhalte geeignet sind. Dabei wird eine Datei im Format XML von den Website-Betreibern auf dem Webserver abgelegt. Gängige Kinderschutzprogramme auf den Endgeräten sind in der Lage, auf diese Klassifizierung zurückzugreifen. Dadurch kann die Software des Kinderschutzprogramms unterscheiden, welche Websites für welche Altersgruppe geeignet sind, und so eine differenzierte Auswahl für verschiedene Zielgruppen treffen.

Bei den Einstellungen des Kinderschutzprogramms kann man z. B. das Alter des Kindes eingeben bzw. Altersgruppen auswählen. Hat man angegeben, dass das Kind sechs Jahre alt ist, und es möchte eine Website besuchen, bei der im Quellcode angegeben ist, dass die Seite erst für die Altersgruppe ab zwölf Jahren geeignet ist, wird die Kinderschutzsoftware die Seite blockieren.



VORTEILE	NACHTEILE
<ul style="list-style-type: none"> <li>• Die Website-Betreiber haben sich selbst Gedanken darüber gemacht, für welche Altersgruppen ihre Inhalte zugänglich sein sollen.</li> </ul>	<ul style="list-style-type: none"> <li>• Bei Weitem nicht alle Website-Betreiber hinterlegen die für eine Klassifizierung notwendigen Informationen im Quellcode.</li> <li>• Kinder entwickeln sich unterschiedlich, weshalb absolute Altersgrenzen oft unpassend sind.</li> <li>• Wenn Inhalte für ein Kind unzugänglich gemacht werden, mit denen es aufgrund seiner persönlichen Entwicklung bereits umgehen könnte.</li> </ul>

### AUFWAND FÜR DIE ELTERN

Diese Funktion bedeutet keinen Aufwand für die Eltern, denn der Informationsaustausch zwischen Kinderschutzprogramm und Website findet automatisch statt.

# 03

## LEITFADEN FÜR DIE PRAXIS



## WIE STELLT MAN KINDERSCHUTZ-MASSNAHMEN EIN?

In diesem Kapitel werden konkrete Kinderschutz-Produkte vorgestellt. Sie beinhalten in der Regel eine bestimmte Kombination von Funktionen des Kinderschutzes. Ausführliche Beschreibungen der einzelnen Funktionen finden sich im Kapitel „Überblick – Welche Funktionen gibt es?“. Die genannten Produkte stellen keine vollständige Aufzählung dar, sondern stehen exemplarisch für viele verfügbare Kinderschutz-Produkte.

Die Linkliste zu den vorgestellten Maßnahmen finden Sie auch elektronisch unter [www.ispa.at/technischerschutz](http://www.ispa.at/technischerschutz).

Die Einstellungen können grundsätzlich auf vier Ebenen vorgenommen werden:

- am Gerät selbst, im Betriebssystem oder in Apps der Betriebssystemhersteller
- durch die Internet- und Mobilfunkanbieter, die entsprechende Zusatzangebote bieten
- durch Programme und Apps von Drittanbietern, die installiert werden müssen
- in manchen Programmen gibt es direkte Einstellungsmöglichkeiten (Browser, YouTube, Spiele ...)

Die besten Ergebnisse erzielt man, wenn man die Einstellungen auf das Kind ab-

stimmt und individuell wählt. Leider sind auch die besten Software-Lösungen keine Ein-Klick-Lösungen, sondern bedürfen regelmäßiger Wartung und Anpassung. Bei gemeinsam genutzten Geräten ist es sinnvoll, unterschiedliche Profile mit unterschiedlichen Zugriffsrechten einzurichten. Schließlich wollen Erwachsene nicht durch den Kinderschutz eingeschränkt sein.

## COMPUTER, STANDGERÄTE, LAPTOP UND PC

In modernen Betriebssystemen sind Basis-Kindersicherungen meist integriert, müssen aber erst aktiviert und an die jeweiligen Bedürfnisse angepasst werden. In der Regel können Sie bestimmte Websites sperren und die Nutzungszeiten regeln. Am besten legt man für das Kind ein eigenes Profil an, bei dem die Kindersicherung aktiviert wird. Zusätzliche Maßnahmen, wie in diesem Ratgeber beschrieben, können ergänzend eingesetzt werden.

### WINDOWS

#### „MICROSOFT FAMILY SAFETY“

Microsoft bietet unter dem Stichwort „Microsoft Family Safety“ viele der bereits beschriebenen Funktionen an. Mit dem Service lassen sich die Einstellungen von Windows- (Windows 10 und Windows 11), Xbox- (Xbox One, Xbox Series X, Xbox Series S) und Android-Geräten über die „Microsoft Family Safety“-App verwalten und Regeln für eine kontrollierte Online-Nutzung bestimmen.

Nach der Einrichtung einer „Familie“ und der Festlegung der Familiengruppenrollen („Mitglied“ oder „Organisator“) unter [account.microsoft.com/family](https://account.microsoft.com/family) stellen die „Familiengruppenorganisatoren“ Inhalts-, Such- und Appfilter ein und setzen Bildschirmzeitbeschränkungen fest. Weiters können Aktivitätsberichte eingesehen, Kaufberechtigungen und Kontolimits verwaltet und die Standorte der „Mitglieder“ angezeigt werden.

Bei der Verwendung eines so umfangreichen Service wie „Microsoft Family Safety“ ist es besonders ratsam, die Empfehlungen, welche Einschränkungen für die jeweilige Altersgruppe sinnvoll sind, zu beachten. Dabei sollte der verständliche Wunsch, die Internetaktivitäten der Kinder zu überprüfen, mit dem Kinderrecht auf Privatsphäre in Einklang gebracht und die vorgenommenen Einschränkungen mit dem Kind besprochen werden.

„Microsoft Family Safety“ liefert diese Anwendungen:

- Berichte über Web-, Such-, App- und Spielaktivitäten
- planbare Computerzeiten, an denen die Geräte den Kindern zur Verfügung stehen
- Blockieren von Apps
- Inhaltsbeschränkungen für unangemessene Websites und Suchvorgänge
- Ausgabenübersicht und -kontrolle
- Standortfreigabe und Standortwarnungen

Mehr Informationen finden Sie auf der [Microsoft-Support-Seite](#).

## MAC

Wird ein Mac als Familienrechner verwendet oder besitzt das Kind selbst einen, so steht eine Reihe von Möglichkeiten, Kinder zu schützen, zur Verfügung. Zunächst sollten ein oder mehrere Benutzer:innenkontos mit „Kindersicherung“ angelegt und darauf geachtet werden, dass nur über das Administrationskonto Änderungen an den Kindersicherungseinstellungen sowie systemweite Änderungen durchgeführt werden können.

In den Systemeinstellungen werden über den Optionpunkt „Kindersicherung“ die gewünschten Einstellungen zu den Themen Kamera, Spiele, E-Mails, App Store, Whitelist, feste Zeiten usw. vorgenommen. Auf Wunsch kann man sich auch das Nutzungsverhalten des Kindes auswerten lassen. Wie für alle anderen Geräte und Oberflächen gilt auch beim Mac, dass versierte Kinder und Jugendliche die Einstellungen umgehen können.

Eine übersichtliche und umfangreiche Darstellung Ihrer Möglichkeiten am Mac finden Sie auf der [Apple-Support-Seite](#).

## KINDERSCHUTZ IM BROWSER

Die meisten Browser bieten Kinderschutz durch Browser-Erweiterungen an, sogenannte Add-ons. Die meisten Add-ons dieser Art haben eine Blacklist-Filterung, die manuell bearbeitet werden kann. Über das Führen einer Whitelist werden einzelne Websites manuell freigeschaltet. Je älter und erfahrener die Kinder im Umgang mit digitalen Geräten sind, desto weniger wirkungsvoll sind Browser-Erweiterungen bzw. desto eher wissen die Kinder, wie man einen anderen Browser ohne Einschränkungen herunterlädt. Da die meisten Kinder und Jugendlichen diese deaktivieren können, sollte bei der Auswahl der Add-ons darauf geachtet werden, dass zum Deaktivieren und Ändern der Einstellungen ein Passwort eingegeben werden muss. Für die Browser Microsoft Edge, Chrome und Firefox gibt es zahlreiche Erweiterungen, an folgenden Beispielen wird deren Funktionsweise gezeigt.

### MICROSOFT EDGE

Die Browser-Erweiterung „Kids Safe Search“ ersetzt die Standardsuchmaschine durch eine sichere, kinderfreundliche Suchmaschine. Alle Websites mit unangemessenen Inhalten wie Pornografie oder Gewalt werden von dem Add-on blockiert und sind für das Kind somit nicht mehr zugänglich. Zusätzlich werden die Suchergebnisse für eine leichtere, kinderfreundliche Benutzung in Kategorien wie Bildung, Kreativität oder Spiele eingeordnet.

### FIREFOX

Firefox stellt mit der Aktivierung der Kindersicherung im Betriebssystem des Computers automatisch den „Prefer:Safe“-Modus ein. Dadurch werden die Sicherheitsfunktionen auf den von Ihrem Kind besuchten Websites aktiviert. Dieser Modus lässt sich nur über die passwortgeschützten Elterneinstellungen des Betriebssystems deaktivieren. Zusätzlich besteht die Möglichkeit, Kinderschutz-Add-ons für Firefox zu installieren.

Mit dem Add-on „FoxFilter“ können Websites festgelegt werden, deren Zugang gesperrt sein soll. Weiters ist möglich, einzelne Inhalte auf Websites zu blockieren, die benutzerdefinierte Schlüsselwörter enthalten. Einige Schlüsselwörter finden sich bereits in den Voreinstellungen des Add-ons, diese lassen sich in den passwortgeschützten „FoxFilter“-Einstellungen aber beliebig personalisieren. Das Add-on ist für die Verwendung mit Firefox auf Windows und Mac geeignet. Ein weiteres Add-on im Firefox-Browser ist „Block Site“. Mithilfe dieser Browser-Erweiterung werden Seiten festgelegt, zu denen der Zugang blockiert oder eine Umleitung zu einer anderen Seite stattfinden soll. Die Sperrung kann zeit- und datumsbasiert konfiguriert werden, und mithilfe eines Passworts ist eine Änderung oder Aufhebung dieser Einstellungen nur durch die Erziehungsberechtigten möglich.

## CHROME

Die Browser-Erweiterung „Tiny WebFilter: Anti-Porn & Block Adult Sites“ aktiviert für Chrome den Jugendschutz und blockiert automatisch anstößige Websites. Beschreibung und Oberfläche sind zwar nur auf Englisch, die Filterung funktioniert aber auch für Websites in anderen Sprachen. Nachdem die Erweiterung hinzugefügt wurde, nimmt man die gewünschten Einstellungen durch das Klicken auf das Symbol vor. Neben anstößigen oder pornografischen Seiten können auch Peer-to-peer-Portale oder soziale Netzwerke blockiert werden. Die Erweiterung hat eine vorhandene Blacklist, die individuell anzupassen ist. Unter dem Stichwort „Block Site“ ist es möglich, zusätzlich Websites einzutragen, die geblockt werden sollen. Unter dem Stichwort „Trusted Site“ können Ausnahmen hinzugefügt werden, die nie geblockt werden sollen. Damit die jungen Nutzer:innen nicht in der Lage sind, die Einstellungen zurückzusetzen, lässt sich die Erweiterung mit einem Passwort schützen.

Als Alternative kann die Kindersicherung in Chrome über „Family Link“ aktiviert werden. Nähere Informationen dazu finden Sie auf der Google-Support-Seite.

## BROWSER FÜR KINDER

Neben Software-Lösungen gibt es auch den Weg, einen separaten Browser zu verwenden, der speziell für Kinder eingerichtet wird. Wenn das Kind damit online geht,

kann es nur auf positive Seiten zugreifen, ungeeignete Inhalte werden ausgefiltert. Auf mobilen Geräten ist dies z. B. mit der „fragFINN“-App oder einem eigenen Browser möglich. Es können auch die zuvor erklärten Browser-Erweiterungen für das Kind eingerichtet werden.

Als Startseite eignet sich etwa eine dieser Seiten:

- [www.helles-koepfchen.de](http://www.helles-koepfchen.de)
- [www.fragfinn.de](http://www.fragfinn.de)

**TIPP:** Eine dieser genannten Seiten als Startseite im Browser des Kindes einrichten und dadurch die Wahrscheinlichkeit erhöhen, dass es eher dort als in den klassischen Suchmaschinen für Erwachsene suchen wird.

## MOBILE GERÄTE: SMARTPHONE UND TABLET

Beim Kinderschutz auf mobilen Geräten, sei es Smartphone oder Tablet, geht es zunächst um die Frage, ob das Gerät mit dem Betriebssystem iOS von Apple oder dem Betriebssystem Android arbeitet.

### ANDROID

Der Betriebssystemhersteller Google bietet auf neueren Android-Geräten mit der kostenlosen App „Family Link“ die Möglichkeit, dass Eltern die Aktivitäten ihrer Kinder ver-

folgen und nach Wunsch beschränken können. Die App gibt es im Play Store.

Weitere Apps werden im Abschnitt „Einstellungen durch Apps von Drittanbietern“ beschrieben.

Auch im Play Store selbst können Kinderschutzzeinstellungen vorgenommen werden, damit für das Alter des Kindes nicht empfohlene Apps nicht zur Verfügung stehen und App-Käufe nur von den Eltern durchgeführt werden dürfen. Eine detaillierte Anleitung, wie die Einstellungen vorzunehmen sind, ist in einem Artikel des Online-Fachmagazins [www.heise.de](http://www.heise.de) abrufbar. Für Tablets, die mit Android arbeiten, gibt es zudem noch die Möglichkeit, eingeschränkte Nutzungsprofile anzulegen. Diese werden in den Geräte-Einstellungen erstellt. Anschließend kann für jede auf dem Gerät installierte App entschieden werden, ob sie im eingeschränkten Profil zur Verfügung stehen soll oder nicht.

**IOS**

Anders als bei Android ist auf Apple-Geräten mit einem Betriebssystem ab iOS 12 das wohl wichtigste Hilfsmittel zum Kinderschutz bereits vorinstalliert. Die sogenannte Bildschirmzeit befindet sich in den Einstellungen. Unter „Bildschirmzeit“ ist zu sehen, für welche Apps man wie viel Zeit verwendet. Es können auch Zeitlimits für einzelne Apps und die Gesamtnutzungszeit des Geräts gesetzt werden.

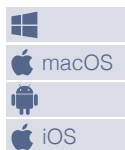
Außerdem lassen sich mit „Bildschirmzeit“ Einstellungen für anstößige Inhalte, Käufe und Downloads sowie den Datenschutz vornehmen. Wenn man die Aktivitäten des Kindes auf dem iPhone und dem iPad einschränken möchte, ist dies ebenfalls mit „Bildschirmzeit“ möglich, vorausgesetzt die beiden Apple-Geräte wurden mit derselben Apple-ID eingerichtet. Dadurch erspart man sich, die Einstellungen auf dem zweiten Gerät zu bearbeiten, und kann geräteübergreifende Zeitlimits setzen. Weitere Informationen finden Sie auf der Apple-Support-Seite. Eine detaillierte Anleitung, wie die Einstellungen vorgenommen werden, ist auf der Seite des Online-Fachmagazins [www.macwelt.de](http://www.macwelt.de) abrufbar.

Wer ein älteres Betriebssystem von iOS verwendet, kann bei den allgemeinen Einstellungen Einschränkungen setzen, unter anderem für den App Store, z. B. das Unterbinden von In-App-Käufen.

**EINSTELLUNGEN DURCH APPS VON DRITTANBIETERN**

.....  
Wer neben den Einstellungen, die in den verschiedenen Betriebssystemen möglich sind, noch weitere treffen möchte, kann zusätzliche Kinderschutzprogramme und -Apps installieren. Es gibt eine große Auswahl an Produkten, die einzelne der zuvor beschriebenen Funktionen anbieten. Folgende Aufzählung ist nicht vollständig, sondern exemplarisch und soll als Orientierung dienen.

## KASPERSKY SAFE KIDS



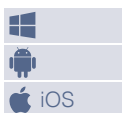
„Kaspersky Safe Kids“ gibt es sowohl für PC und Mac als auch für Android-Smartphones und iPhones und

wurde mit dem AV-Test-Zertifikat ausgezeichnet (nähere Informationen dazu auf [www.av-test.org](http://www.av-test.org)).

Folgende Funktionen sind in der Bezahlversion enthalten:

- Verwaltung der Geräte-Nutzungsdauer und App-Nutzung
- Berichte über öffentliche Facebook-Aktivitäten einschließlich Posts und neu hinzugefügter „Freunde“
- Rat und Tipps zu Online-Themen von Expert:innen und Kinderpsycholog:innen
- Zugriff auf unangemessene Websites und -Inhalte blockieren
- GPS-Tracker, um den Aufenthaltsort auf einer Echtzeit-Online-Karte ermitteln zu können
- Definieren eines sicheren Bereichs, in dem das Kind bleiben soll; Benachrichtigung, wenn der Bereich verlassen wird
- Information über den Akkustand

## NORTON FAMILY PREMIER



Das Programm „Norton Family Premier“ ist für Windows-PCs und Smartphones (iOS und Android) erhältlich.

Diese Funktionen bietet die kostenpflichtige Version von „Norton Family Premier“:

- Filtern von Websites
- E-Mail-Benachrichtigung, wenn versucht wird, blockierte Websites aufzurufen
- Überwachen von Suchbegriffen
- Sperren des Geräts

## KIDS PLACE



Für den Kinderschutz am Smartphone und am Tablet gibt es die weit verbreitete und in der Grundversion kostenlose App „Kids Place“. Von [netzwelt.de](http://netzwelt.de) wurde die App als „sehr gut“ eingestuft.

Folgende Funktionen stehen zur Verfügung:

- Apps beschränken, auf die vom Gerät aus zugegriffen werden kann
- „Kids Place“ auf einer unbegrenzten Zahl von Geräten aktivieren
- individuell an das Kind angepasstes Nutzungsprofil
- Zeitlimits pro Tag
- automatisches Starten der App bei Neustart des Geräts



## OHANA-KINDERSICHERUNGS-APP



Ohana gibt es als Gratisversion und als Bezahlversion mit mehr Funktionsumfang.

Der Mobilfunkanbieter Drei hat eine enge Kooperation mit Ohana.

- Apps und Websites blockieren
- Zeitlimits und Zeitpläne einstellen
- Standortermittlung
- Statistische Auswertungen

## JUSPROG



Das Programm „Jusprog“ kann kostenlos heruntergeladen werden. Der Herausgeber des Programms JusProg e.V. ist ein gemeinnütziger Verein

ohne Gewinnorientierung.

Die Software ist nach den gesetzlichen Vorgaben (JMStV) durch die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) in Deutschland gesetzlich anerkannt.

- Filterung von Inhalten
- Anpassung an verschiedene Altersstufen
- mehrere Nutzer:innen mit verschiedenen Altersbeschränkungen auf einem Gerät möglich

## KINDER NUTZEN DAS ELTERNHANDY

Um das Gerät ohne Bedenken an das Kind weitergeben zu können, wird am Gerät der Eltern eine Kinderschutz-App, z. B. „Kids Place“, installiert. Zuvor wird mittels der App ein PIN-Code definiert, mit dem die sichere Umgebung wieder verlassen werden kann. Danach wird die E-Mail-Adresse zur Wiederherstellung eingetragen und die einzelnen Apps, die das Kind verwenden darf, freigegeben. Dabei lässt sich jeweils einzeln einstellen, welche App Zugriff auf das Internet erhalten soll, bzw. kann der Internet-Zugriff auch für alle Apps im Kinderbereich gesperrt werden. Eine sinnvolle Einstellung ist „Homebutton sperren“. Wenn diese aktiviert ist, erscheint bei Drücken der Hometaste der Startbildschirm von „Kids Place“. „Auto-start“ ist eine weitere wichtige Funktion von „Kids Place“, dadurch wird beim Einschalten des Geräts die „Kids Place“-App automatisch geöffnet.

## EINSTELLUNGEN DURCH DIE MOBILFUNK-/INTERNETANBIETER

Viele Mobilfunk- und Internetanbieter bieten Produkte an, die einen technischen Kinderschutz versprechen. Es gibt unterschiedliche Zugangsmethoden, die vom jeweiligen Anbieter abhängig sind.

## MAGENTA

Magenta bietet einen Kinderschutz für Smartphone, Tablet und WLAN an. Damit kann man entscheiden, welche Inhalte für die Kinder sichtbar sind. Es gibt Pakete für ein bis drei Rufnummern.

Die Funktionen sind:

- bestimmte Websites erlauben oder sperren
- Kategorien bei der Auswahl der erlaubten bzw. gesperrten Inhalte
- internetfreie Zeiten verwalten
- Sicherheit im WLAN (nur für Smartphones mit Android-Betriebssystem)
- soziale Netzwerke und YouTube sperren
- mobile Verwaltung der Einstellungen in der „Mein Magenta“-App

## DREI

Drei bietet auf [www.drei.at/kids](http://www.drei.at/kids) einen Überblick über die Kinder- und Jugendtarife und mögliche Kinderschutzmaßnahmen. Sie bieten auch das Startklar-Service an, mit dem bereits beim Gerätekauf Zugangsbeschränkungen und Sicherungen aktiviert werden. Drei hat eine enge Kooperation mit der Ohana - Kindersicherungs-App. Von Drei gibt es außerdem die „Drei Schutzengel“-Jugendschutzsperre. Diese kann entweder selbst über die Drei-Kundenzone online, beim Drei-Service-Team oder im Drei Shop aktiviert werden.

Gesperrt werden können:

- Anrufe von Mehrwertnummern

- Einkaufen im Google Play Store
- Handynutzung im Ausland

**TIPP:** Manche Anbieter erlauben es den Eltern, Steuerungsmechanismen direkt auf der Ebene des Internet-Service-Providers einzurichten. Filter, die für Kinder unangemessene Inhalte blockieren, werden dann aktiv. Auf den ersten Blick wirkt diese Möglichkeit durchaus sinnvoll, es gibt aber auch Nachteile. Sobald das Kind ein anderes Netzwerk (z. B. ein freies WLAN) nutzt, greift der Schutz nicht mehr.

Damit Erwachsene eine unzensurierte Version des Internets nutzen können, bieten manche Anbieter den Service, mit einem Passwort die Kindersicherung ein- und auszuschalten. Je nach Anbieter ist es möglich, die verschiedenen Funktionen wie URL-Filter und Stichwort-Filter, Zeitbeschränkungen, Sperren von sozialen Netzwerken etc. zu nutzen.

## A1

A1 bietet das Produkt „Internetschutz“ an, mit dem optional auch die „A1 Kindersicherung“ genutzt werden kann.

Die „A1 Kindersicherung“ beinhaltet folgende Möglichkeiten:

- bestimmte Websites erlauben oder sperren
- Kindersicherung zeitsteuern
- Kindersicherung mit einem Passwort ein-

und ausschalten

- Websites aus bedenklichen Kategorien werden automatisch vom Webfilter gesperrt

## **ROUTER MIT KINDERSCHUTZ/WLAN**

.....

Mit einem Router, der mit Funktionen zur Kindersicherung ausgestattet ist, lässt sich das Heimnetzwerk so einrichten, dass Kinder mit ihren Geräten nicht auf das freie Internet zugreifen können. Die modernen Modelle bieten Lösungen an, bei denen die Eltern von der Kindersicherung ausgenommen sind. Der Vorteil besteht darin, dass sich alle Geräte, die mit dem Heimnetzwerk verbunden sind, über eine Oberfläche steuern lassen. Wenn das Kind also mit einem Laptop, einem Smartphone und einem Tablet online gehen kann, greift die Kindersicherung, die im Router eingestellt wurde, auf allen drei Geräten. Um den Kinderschutz zu aktivieren, muss eine Website im Browser aufgerufen werden, während das Gerät mit dem Heimnetzwerk verbunden ist, z. B. über WLAN. Manche Router-Hersteller bieten dafür auch eigene Apps an, um die Steuerung über das Smartphone zu ermöglichen. Um die Funktionsweise besser darzustellen, wird diese am Beispiel der Fritz-Box 7490, die das Magazin Computerwelt.de als „gut“ eingestuft hat, erklärt.

### **FRITZ-BOX 7490**

Die Fritz-Box-Modelle wie die Fritz-Box 7490 von AVM (neuere Modelle arbeiten

mit demselben Schema) verwenden als Webfilter das Modul der Bundesprüfstelle für jugendgefährdende Medien, kurz: BPjM-Modul. Dabei handelt es sich um eine nicht öffentliche Blacklist von Online-Angeboten, die die Bundesprüfstelle im Hinblick auf den Jugendmedienschutz als bedenklich eingestuft hat. Es gibt zusätzlich die Möglichkeit, eine eigene Blacklist mit URLs, die gesperrt werden sollen, anzulegen. Der Webfilter sperrt sowohl HTTP- als auch HTTPS-URLs.

Die Kindersicherung ist gut durchdacht und praktisch einzustellen: Für jede:n Benutzer:in kann ein Profil angelegt werden, in dem festgelegt wird, welche Inhalte gesperrt werden und wie lange die Internetnutzung dauern soll. Wenn für jedes Kind ein Profil angelegt wird, lassen sich mehrere Geräte (sogenannte Clients), also z. B. Smartphone, Laptop und Tablet, per Klick dem jeweiligen Profil zuordnen. Über die Profile werden auch die Zeitfenster und -limits gesteuert. Diese müssen nicht auf jedem Gerät einzeln eingetragen werden, sondern werden für das jeweilige Profil (Kind) definiert. Ist mit der Budgetfunktion eine maximale Nutzungsdauer festgelegt, wird die gesamte Nutzungszeit auf allen von diesem Kind verwendeten Geräten zusammengezählt. Die Dokumentation der Kindersicherung ist sehr ausführlich. Wie Sie die einzelnen Einstellungen der Fritz-Box an Ihre Bedürfnisse anpassen können, finden Sie auf der Seite von AVM.

**ACHTUNG!** Bis zu einem gewissen Alter bzw. digitalen Erfahrungsgrad des Kindes bietet die Kindersicherung im Router eine bequeme Lösung, um nicht kindgerechte Inhalte zu blockieren bzw. Zeitlimits zu setzen. Wenn die jungen Nutzer:innen aber ein eigenes Smartphone mit einer ausreichenden Menge an mobilen Daten besitzen bzw. sie mobile Endgeräte mit öffentlichen WLAN-Netzwerken verbinden, wird die Kindersicherung ausgehebelt. Technisch erfahrene Kids können auch die Kindersicherung im Router umgehen (z. B. durch VPN-Clients).

## KINDERSCHUTZMASSNAHMEN DER PLATTFORMEN

.....  
Soziale Medien dürfen in Österreich erst ab 14 Jahren genutzt werden. Viele Kinder haben aber trotzdem Profile auf den diversen Plattformen, da bei den meisten sozialen Netzwerken keine Altersverifizierung durchgeführt wird. Wenn Kinder also ein falsches Geburtsdatum angeben, können sie auf alle Inhalte des sozialen Netzwerks zugreifen. Die Plattformbetreiber bieten verschiedene Einstellungen an, um Kinder in ihren sozialen Netzwerken zu schützen. Diese Schutzmaßnahmen sind aber keine Garantie für ein sorgenfreies Online-Erlebnis. Medienkompetenz und gemeinsames Reflektieren mit den Kindern und Jugendlichen sind unerlässlich, damit Kinder und Jugendliche soziale Netzwerke sicher nutzen können.

### INSTAGRAM (META)

Konten von Minderjährigen sind automatisch auf privat eingestellt. Außerdem können Erwachsene nur Nachrichten an Minderjährige schicken, wenn diese zumindest dem Account des Erwachsenen folgen. Accounts von Kindern sind auch bei gezielten Werbungen besser geschützt als jene von Erwachsenen. Mit der Option „Einschränken“ kann man ausgewählte Profile ausblenden, ohne dass die Person dies weiß. Mithilfe von KI überprüft Meta laufend die Accounts ihrer User:innen, um jene auffindig zu machen, bei denen Kinder ein falsches Geburtsdatum angegeben haben.

### TIKTOK

Die Konten von 13-16-Jährigen sind standardmäßig auf Privat eingestellt. Bestimmte Funktionen stehen Nutzer:innen unter 18 Jahren nicht zur Verfügung, z. B. können sie kein LIVE veranstalten, Geschenke senden oder empfangen. Mit dem Begleiter Modus können Erziehungsberechtigte Privatsphäre-Einstellungen für die Accounts ihrer Kinder anpassen, einschließlich Kontotyp, wer Videos kommentieren darf und wie viel Zeit täglich auf TikTok verbracht werden darf. Nähere Informationen finden Sie im TikTok-Leitfaden für Erziehungsberechtigte.

## YOUTUBE

In den Kontoeinstellungen kann der „eingeschränkte Modus“ aktiviert werden, dadurch werden Inhalte, die potenziell nicht jugendfrei sind, ausgeblendet. Mit der „Elternaufsicht“ können die Konten eines Elternteils mit dem Konto des Kindes verknüpft werden, wodurch der Erwachsene verschiedene Inhaltseinstellungen wählen kann. Dem Konto des Kindes wird auch nur ausgewählte Werbung angezeigt und Funktionen sind beschränkt.

**YouTube Kids** ist eine App, die speziell für Kinder entwickelt wurde. Eltern können aus den drei Altersstufen „Vorschulalter“, „Jünger“ und „Älter“ oder manuell die Videos, Kanäle und Sammlungen wählen, deren Inhalte ihr Kind sehen darf.

**TIPP:** Nehmen Sie die Privatsphäre-Einstellungen gemeinsam mit Ihrem Kind vor. Informieren Sie sich direkt beim Plattformbetreiber über neue Kinderschutzmöglichkeiten. Diese entwickeln laufend neue Einstellungsmöglichkeiten, die zum Schutz von Kindern in sozialen Netzwerken beitragen sollen. Bitte bedenken Sie, dass die Schutzmaßnahmen der Plattformen nur für Konten von Kindern greifen, die ihr Geburtsdatum wahrheitsgemäß eingegeben haben.

## SPIELEKONSOLE

Mittlerweile geben die meisten Spielehersteller Alterskennzeichnungen an. Eltern sollten allerdings wissen, dass diese Angaben meist von den Anbietern selbst gemacht und oft nicht unabhängig geprüft werden. Ähnlich wie bei Filmen, wo sich mit der FSK-Kennzeichnung eine Art universeller Standard etabliert hat, existieren auch für Software (vor allem für Spiele) Altersfreigaben bzw. Altersempfehlungen anhand einheitlicher Kriterien. Der App Store von Apple zeigt vorrangig die Einstufung nach einer eigenen Bewertungsskala an. Altersempfehlungen sind naturgemäß als Annäherungen zu verstehen. Kinder entwickeln sich schließlich individuell. Eltern sollten immer zuvor bzw. gemeinsam mit dem Kind prüfen, ob Schwierigkeitsgrad, Komplexität, Lesekompetenz etc. wie vom Spiel gefordert den Bedürfnissen und Fähigkeiten des Kindes entsprechen.

**PEGI** (Pan European Game Information) ist ein europaweit genutztes System, um Eltern beim Kauf von Computerspielen zu beraten. Das System wird von den wichtigsten Spielekonsolenherstellern ebenso unterstützt wie von Spieleentwicklern in ganz Europa. Die Symbole des PEGI-Einstufungssystems unterscheiden zwischen den Alterskennzeichnungen 3, 7, 12, 16 und 18. Sie informieren darüber, ob ein Spiel für eine Altersgruppe unbedenkliche Inhalte

enthält. Ob ein Spiel jedoch wirklich für ein Kind in diesem Alter geeignet ist, lässt sich daraus nicht so einfach ableiten. So kann etwa ein hochkomplexes Simulationsspiel, bei dem es darum geht, eine Stadt aufzubauen, zwar mit „PEGI 3+“ gekennzeichnet sein, aber nur ältere Spieler:innen werden die Zusammenhänge und die Spielmechanik so weit verstehen, dass sie das Spiel auch erfolgreich spielen können. Eltern sollten sich allerdings bewusst sein, dass diese Angaben meist von den Anbietern selbst stammen und selten unabhängig geprüft werden.

Moderne Spielekonsolen bieten die Möglichkeit, sich mit anderen Spieler:innen zu vernetzen und auszutauschen. Wenn Eltern nicht möchten, dass die Kinder mit fremden Personen chatten, können diese Chatfunktionen oft deaktiviert werden.

### **NINTENDO/NINTENDO 3DS**

Um das Gerät für die Altersgruppe des Kindes einzustellen, muss in den System-einstellungen im Home-Menü die Altersbeschränkung aktiviert werden. Zur Einrichtung wählt man eine Geheimzahl, damit das Kind die Einstellungen ohne den Code nicht bearbeiten kann.

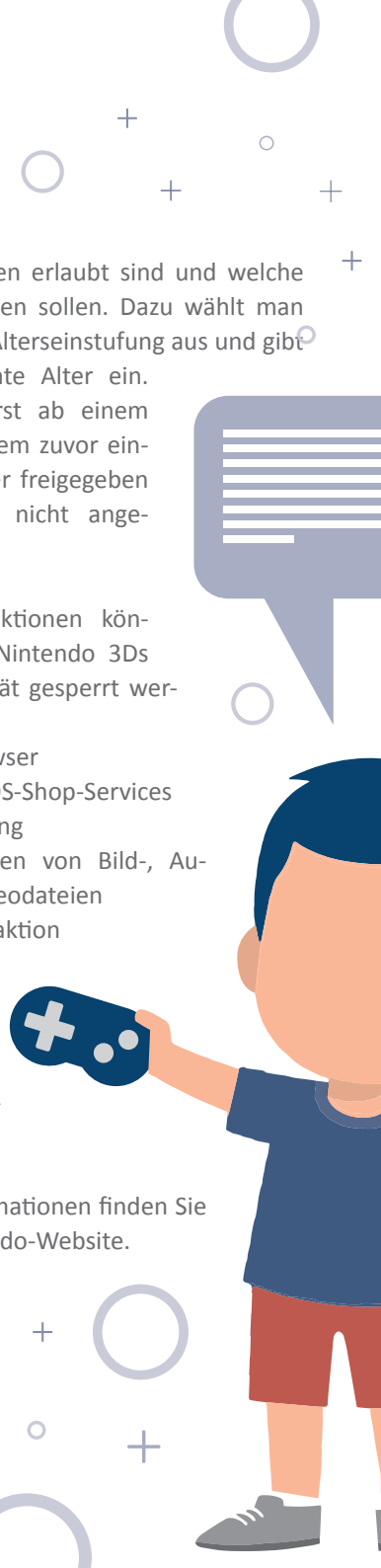
Um nur Spiele zuzulassen, die für das Alter des Kindes geeignet sind, wird bei den Altersbeschränkungen angegeben, welche

Alterskategorien erlaubt sind und welche gesperrt werden sollen. Dazu wählt man die Software-Alterseinstufung aus und gibt das gewünschte Alter ein. Spiele, die erst ab einem höheren als dem zuvor eingestellten Alter freigegeben sind, werden nicht angezeigt.

Folgende Funktionen können auf der Nintendo 3DS direkt am Gerät gesperrt werden:

- Internetbrowser
- Nintendo-3DS-Shop-Services
- 3D-Darstellung
- Übertragungen von Bild-, Audio- und Videodateien
- Online-Interaktion
- StreetPass
- „Freunde“-Registrierung
- DS-Download-Spiel

Weitere Informationen finden Sie auf der Nintendo-Website.



## NINTENDO SWITCH

Neben dem Sperren von Spielen, die nicht für eine eingestellte Altersgruppe geeignet sind, können auch andere Einstellungen direkt am Gerät vorgenommen werden. Dazu muss man die Altersbeschränkung aktivieren.

Folgendes kann direkt auf der Konsole gemacht werden:

- Speicherdaten und Screenshots verwalten

- Nutzer:in löschen
- Interneteinstellungen festlegen

Zusätzlich kann zur weiteren Regulierung die App „Nintendo Switch-Altersbeschränkung“ auf dem Smartphone (iOS oder Android) installiert werden.

Dort lassen sich diese weiteren Massnahmen treffen:

- gespielte Software und Spiele ansehen
- maximale Spieldauer festlegen

Wollen Erwachsene alle Funktionen uneingeschränkt nutzen, können sie die Altersbeschränkung pausieren. Dazu

muss man den Code eingeben, den man bei Einrichtung der Altersbeschränkung eingestellt hat. Geht die Konsole in den Stand-by-Modus, wird die Altersbeschränkung beim nächsten Neustart automatisch aktiviert.

Es ist nicht möglich, verschiedene Einschränkungen für unterschiedliche Altersgruppen auf einer Konsole einzurichten. Alle Einstellungen gelten für alle Nutzer:innen der Nintendo-Switch-Konsole. Wenn mehr als ein Kind auf der Konsole spielt, sollte die Altersbeschränkung an das jüngste Kind angepasst und bei Bedarf für ältere Kinder pausiert werden.

Mehr Informationen finden Sie auf der Nintendo-Hilfe-Seite.

**TIPP:** Alle Einstellungen zur Altersbeschränkung können auch im Browser über die Nintendo-ID eingerichtet werden, was sehr übersichtlich ist. Dazu benötigen Sie Ihre Nintendo-ID und Ihr Passwort.

## SONY PLAYSTATION 4 und 5

Für die Playstation wird die Altersbeschränkung über die Familienverwaltung eingestellt. Die Kindersicherung kann über die Playstation-App mobil verwaltet oder über die Playstation-Website im Browser eingerichtet werden.

Als Familienmanager:in ist es einer:m Erwachsenen möglich, ein Familienkonto zu erstellen, weitere Konten von Familienmitgliedern hinzuzufügen und die Einstellungen für deren Kindersicherung zu bearbeiten. Alle Kinderkonten, die Erwachsene erstellen, werden automatisch zu ihrer „Familie“ hinzugefügt. Minderjährigen Familienmitgliedern und der:m Familienmanager:in ist es nicht möglich, ihre „Familie“ zu verlassen.

Wenn ein Kinderkonto der „Familie“ hinzugefügt wurde, kann die Kindersicherung direkt auf der Konsole eingestellt werden. Um zu verhindern, dass das Kind die getroffenen Einstellungen aufhebt, sollte der Passcode, der standardmäßig „0000“ lautet, unbedingt geändert und nicht an das Kind weitergegeben werden. Dieser Passcode ist auch nötig, wenn auf Inhalte zugegriffen werden soll, die gemäß den Kinderschutzeinstellungen nicht erlaubt sind. So können Erwachsene dieselbe Konsole ver-

wenden, sind aber nicht an die Einschränkungen gebunden.

Folgende Einstellungen lassen sich treffen:

- Einschränkung der Spielzeit
- Sperren der Kommunikation mit anderen Spieler:innen
- Ausgabelimit für Spieleeinkäufe im Playstation Store
- benutzerdefinierte Altersstufen für Spiele- und Videoinhalte
- Sperren des Webbrowsers
- Sperren des VR-Headsets

Weitere Informationen finden Sie auf der Playstation-Hilfe-Seite.

## MICROSOFT XBOX ONE

Die Sicherheitseinstellungen für Kinder können bei der Xbox entweder direkt auf dem Gerät oder über die „Microsoft Family“-Einstellungen vorgenommen werden.

Die Xbox-Einstellungen zu Datenschutz und Online-Sicherheit für ein Kinderkonto lassen sich nur von Erziehungsberechtigten ändern, die den „Microsoft Family“-Dienst verwenden.

Im Microsoft-Konto kann überprüft werden, welchen Familienmitgliedern Beschränkungen zugewiesen wurden. Um die



Anpassungen für das Kind vorzunehmen, wählt man in den Xbox-Einstellungen das jeweilige Gamertag des Kindes aus und aktiviert danach alle gewünschten Einschränkungen. Damit die Änderungen übernommen werden, muss sich das Kind ab- und wieder anmelden.

Folgende Einstellungen können getroffen werden:

- altersdifferenziertes Sperren von Inhalten
- Webfilterung der „Microsoft Edge“-App
- Einschränkung der Kaufoptionen im Microsoft Store
- Einholung der Erlaubnis einer:s Erziehungsberechtigten
- Zeitlimit

Zeitlimits festzulegen, ist nur über die „Microsoft Family“-Einstellungen möglich, nicht direkt auf der Konsole.

Für den Fall, dass das Kind Anfragen an die Erziehungsberechtigten stellt – wenn es

sich z. B. mehr Zeit wünscht oder ein bestimmtes Spiel kaufen möchte –, können diese entweder per E-Mail, direkt auf der Konsole oder über das „Microsoft Family“-Konto beantwortet werden.

## SMART TOYS

Die Digitalisierung hat mit vernetzten Spielzeugen Einzug ins Kinderzimmer gehalten. Doch die antwortenden Puppen und die per App steuerbaren Roboter sind nicht nur unterhaltsam, sondern bergen auch Risiken.

Wer sichergehen möchte, dass das Spielen der Kinder harmlos bleibt, sollte sich einige Aspekte bewusst machen – beginnend bei der Auswahl des passenden Produkts bis hin zum richtigen Umgang damit. Insbesondere der Schutz von Daten und Privatsphäre sollte bei vernetzten Spielzeugen Beachtung finden.

### TIPPS:

- Recherche vor dem Kauf: Ist das Spielzeug vernetzt? Werden persönliche Daten verarbeitet?
- Produkte mit verschlüsselter und passwortgeschützter Datenübertragung auswählen.
- Spielzeuge mit Mikrofonen sollten nach der Nutzung ausgeschaltet werden.
- Vernetzte Spielzeuge sind keine Babysitter:innen, die Begleitung durch Erwachsene ist ratsam.

Weitere Themen wie Fragen zu technischen Sicherheitsstandards, zur altersgerechten Auswahl oder zur optimalen Beschäftigungsdauer mit smarten Spielsachen werden im digitalen Folder von [Saferinternet.at](http://Saferinternet.at) thematisiert.

## GPS-KINDERUHREN

---

Sogenannte Kinderuhren, die über einen GPS-Tracker verfügen, können zur Überwachung des Aufenthaltsorts des Kindes verwendet werden. Ähnliche Produkte, bei denen die GPS-Tracker z. B. in einem Armband oder einem kleinen Anhänger angebracht sind, haben ähnliche Funktionen. Die GPS-Tracker werden in die Hosentasche gesteckt oder am Rucksack angebracht. Sie enthalten einen Akku, eine SIM-Karte sowie einen Micro-Controller.

Je nach Version können Eltern die aktuelle Position ihres Kindes bzw. des Geräts per SMS, App oder online abrufen. Manche der Geräte erlauben es dem Kind auch, anzurufen bzw. Kurznachrichten zu verfassen. Bei einzelnen Produkten lassen sich zudem räumliche Sicherheitszonen festlegen, innerhalb derer ein Kind sich bewegen darf. Zusätzlich können verschiedene gesundheitliche Parameter kontrolliert werden (von der Wegstrecke über den Kalorienverbrauch bis hin zum Schlafrhythmus). Im Abschnitt „Geofencing“ wird erläutert, welche Risiken mit der Verwendung dieser Geräte einhergehen.

