

# Das erste Smartphone für mein Kind



Abbildung 1: Foto von Andrea Piacquadio von Pexels **Quelle:** <https://www.pexels.com>

## Der Versuch einer Hilfestellung zu Themen rund ums erste Smartphone für Kinder.

**Version 1.1**  
**Oktober 2021**

**Der Inhalt des folgenden Skripts stammt zu großen Teilen von einschlägigen Webseiten wie [saferinternet.at](https://saferinternet.at), [schau-hin.info](https://schau-hin.info), [mobilsicher.de](https://mobilsicher.de), [klicksafe.de](https://klicksafe.de), uvm. und wurde von mir zusammengefasst und stellenweise erweitert.**

**Eventuelles Feedback bitte an: [markus.signitzer@htlinn.ac.at](mailto:markus.signitzer@htlinn.ac.at)**

**no © by Markus Signitzer**  
**September 2021**

**Typesetting by  $\LaTeX$**

# Inhaltsverzeichnis

<b>1</b>	<b>Vorwort</b>	<b>1</b>
1.1	Verwendung des Leitfadens	1
1.2	Ganz wichtig!	1
<b>2</b>	<b>Rechtliche Aspekte</b>	<b>2</b>
2.1	Jugendschutz Gesetz	2
2.2	Eigentümer des Smartphones	2
2.3	Recht am eigenen Bild	2
2.4	Cyber-Mobbing-Paragraph	3
2.5	Kinderpornographie	3
2.6	Hass im Netz	3
2.7	Nationalsozialistische Wiederbetätigung	4
<b>3</b>	<b>Soziale Aspekte und Themen die ich mit meinem Kind besprechen sollte</b>	<b>5</b>
3.1	Rechtliche Besitzer des Smartphones und Vertragsdetails	5
3.2	Einen eigenen Mediennutzungsvertrag mit dem Kind erstellen	5
3.2.1	Wann und wo schläft das Handy?	5
3.3	Recht am eigenen Bild	5
3.4	Cyber-Mobbing	6
3.4.1	Wie bereite ich mein Kind auf mögliches Mobbing vor?	6
3.4.2	Was tun wenn mein Kind von Mobbing betroffen ist?	6
3.4.3	Mobbing in der Schule	6
3.4.4	Was sage ich meinem Kind zu Cyber-Mobbing?	6
3.5	Sex	6
3.6	Pornographie	7
3.6.1	Warum unreflektierter Pornokonsum problematisch ist	7
3.6.2	Ein Porno ist ein Film	7
3.6.3	Was sage ich meinem Kind zu Pornographie?	7
3.6.4	Was tun bei Kinderpornographie?	7
3.7	Sexting	7
3.7.1	Was sage ich meinem Kind zu Sexting?	8
3.8	Cyber-Grooming	8
3.8.1	Was sage ich meinem Kind zu Cyber-Grooming?	8
3.9	Selbstwertgefühl und Schönheitsideale	8
3.9.1	Was sage ich meinem Kind zum Thema Schönheitsideale	8
3.9.2	Pro-Ana und Pro-Mia Chatgroups und Coaches	9
3.10	Nationalsozialistische Wiederbetätigung	9
3.11	Allgemeines zu Privatsphäre und Vergessen im Netz	9
3.11.1	Zwei kleine Beispiele zum Thema: Warum Datenschutz wichtig ist	10
3.11.2	Was sage ich meinem Kind zum Thema Privatsphäre?	10
3.11.3	Wie erstelle ich in drei Schritten eine gute Passwort-Phrase?	10
3.12	Social-Media und Messenger	10
3.12.1	Welcher Messenger?	10
3.12.2	Was sage ich meinem Kind zum Thema Messenger?	11
<b>4</b>	<b>Technische Hilfsmittel</b>	<b>12</b>
4.1	Android interne Hilfsmittel	12
4.1.1	Google Family Link	12
4.1.1.1	Kurzinfo	12
4.1.1.2	Funktionsumfang	12
4.1.1.3	Installation	12
4.1.1.4	Fazit zu Google Family Link	13
4.1.2	YouTube	14
4.2	Browser und Suchmaschinen	14
4.2.1	Browser Erweiterungen	14
4.2.2	Suchmaschinen für Kinder	14
4.3	In-App-Käufe vermeiden	14
4.4	Sprach-Assistenten deaktivieren	14
4.5	Externe FOSS Apps	14

4.5.1	F-Droid . . . . .	15
4.5.2	Blokada . . . . .	15
4.5.3	Time Limit . . . . .	15
4.5.4	UsageDirect . . . . .	15
4.5.5	App Locks . . . . .	15
4.6	Alternative Betriebssystem . . . . .	15
4.6.1	LinageOS . . . . .	15
4.6.2	GrapheneOS . . . . .	15
4.6.3	e-OS . . . . .	16
5	Abschließende Worte	16

# 1 Vorwort

Das Smartphone ist aus unserer Gesellschaft nicht mehr wegzudenken. Das kleine Gerät ist für uns Kommunikationsmittel, Nachschlagewerk, Kamera, Navigationsgerät, Zahlungsmittel, Tor zum Internet und damit Zugang zum **social networking** in all seinen Aspekten. Kein Smartphone zu besitzen, bedeutet heute oft, nicht an allen sozialen Interaktionen im Freundeskreis teilnehmen zu können. Je nach Alter und Freundeskreis kann dies zu Ausgrenzung und sozialer Isolation führen. Besonders im Kindes- und Jugendalter ist der Gruppendruck ein Smartphone zu besitzen, sehr groß.

Meine Motivation für diesen Leitfaden war die Tatsache, dass ich mit dem Smartphone für meine älteste Tochter lieber noch warten würde, der Gruppendruck in der ersten Klasse Mittelschule aber sehr groß ist. Da ich mich mit diesem Thema nun ausführlich auseinandergesetzt habe, möchte ich das Ergebnis meiner - doch recht zeitaufwendigen - Recherchen in kompakter Form gerne an andere Eltern weitergeben.

Die Inhalte des Leitfadens sind natürlich nicht alle von mir, sondern von vielen sehr guten Organisationen (z.B. [saferinternet.at](https://saferinternet.at), [klicksafe.de](https://klicksafe.de), [schau-hin.info](https://schau-hin.info), [mobilsicher.de](https://mobilsicher.de), uvm., zusammengetragen - bitte die Quellenangaben beachten.

## 1.1 Verwendung des Leitfadens

Dieser Leitfaden ist dafür ausgelegt **online gelesen** zu werden, da er viele Links (die entsprechenden URLs sind nur verkürzt dargestellt) zu weiterführenden Seiten enthält.

Auf detaillierte Anleitungen wird nur verlinkt, da Anleitungen mit Darstellungen bzw. Screenshots den Leitfaden zu umfangreich machen würden.

Der Leitfaden gliedert sich grob in drei Bereiche:

- **Rechtliche Aspekte:** z.B. wer ist Besitzer des Smartphones? wer haftet? was ist verboten?
- **Soziale Aspekte:** z.B. über welche Themen sollte ich mit meinem Kind sprechen und auf was muss ich es vorbereiten, damit es richtig reagiert wenn es mit problematischen Inhalten konfrontiert wird?
- **Technische Aspekte:** z.B. welche technischen Hilfestellungen gibt es um z.B. das surfen sicherer zu gestalten, In-App-Käufe zu vermeiden, Bildschirmzeit zu begrenzen, usw.

## 1.2 Ganz wichtig!

Vorausstellend möchte ich noch festhalten, dass der beste Schutz gegen möglich Probleme mit und ums Smartphone, eine **solide Vertrauens- und Gesprächsbasis mit ihrem Kind ist!** Bestärken sie es darin, bei Inhalten die es verunsichern oder verstören, zu ihnen zu kommen. Drohen oder strafen sie nicht mit Handy-Entzug wenn mal was schief läuft, dies zerstört nur die Vertrauensbasis. Verbringen sie Online-Zeit mit ihrem Kind und bleiben sie über das Online-Leben ihres Kindes informiert.

## 2 Rechtliche Aspekte

In diesem Kapitel werden kurz die wichtigsten rechtlichen Grundlagen aufgezeigt. Was diese Grundlagen für sie und ihr Kind bedeuten wird im Kapitel 3 auf Seite 5 genauer besprochen.

### 2.1 Jugenschutz Gesetz

Die Jugenschutzgesetze in Österreich werden von den Bundesländern geregelt und sind zum Teil leicht unterschiedlich. Für diesen Leitfaden wird nur auf den Punkt **Jugendgefährdende Medien, Gegenstände & Dienstleistungen** eingegangen: Der folgende Text sowie eine ausführliche Erklärung zu den Jugenschutzbestimmungen findet man auf [eltern-bildung.at](http://eltern-bildung.at):

Medien (z.B. Filme), Datenträger (z.B. Computerspiele), Gegenstände (z.B. Softguns), Dienstleistungen (z.B. Telefonsex) oder Veranstaltungen, die besonders brutal, diskriminierend oder pornografisch sind, dürfen von Jugendlichen unter 18 Jahren nicht erworben, verwendet oder besucht werden.

Das bedeutet auch, dass diese Filme, Spiele und Dienstleistungen Kindern und Jugendlichen nicht angeboten werden dürfen. Erwachsene sind dazu verpflichtet, durch geeignete Vorkehrungen dafür zu sorgen, dass jungen Menschen diese Gegenstände nicht in die Hände fallen.

Dieser Punkt setzt das Mindestalter für den Konsum von Pornographie auf 18 Jahre.

Im Pornographie Gesetz wiederum ist festgeschrieben, dass Porno-Clips nur an Personen ab 16 Jahren verschickt werden dürfen. Dies gilt auch für das Laden eines Links z.B. in einer WhatsApp Gruppe!

Siehe dazu auch Kinderpornographie im Kapitel 2.5 auf Seite 3.

### 2.2 Eigentümer des Smartphones

Der Eigentümer ist die Person auf die der Vertrag mit dem Mobilfunkanbieter läuft. Diese Person, meist ein Elternteil, ist letztendlich verantwortlich für etwaige rechtliche Probleme.

### 2.3 Recht am eigenen Bild

Der folgende Text stammt von [www.oesterreich.gv.at](http://www.oesterreich.gv.at):

Das Recht am eigenen Bild ist wie das Namensrecht ein Persönlichkeitsrecht. Es besteht darin, dass Bilder von Personen **nicht der Öffentlichkeit zugänglich gemacht werden dürfen**, wenn dadurch **berechtigte Interessen** der/des Abgebildeten oder unter Umständen einer/eines nahen Angehörigen **verletzt** würden. Ob die Veröffentlichung eines Bildes zulässig ist, hängt davon ab, ob nach objektiven Gesichtspunkten schutzwürdige Interessen der/des Abgebildeten entgegenstehen.

Dabei sind nicht nur das Bild selbst, sondern auch **Bildunterschriften, Begleittexte und der Gesamtzusammenhang** zu berücksichtigen. Bei einer nicht-genehmigten Verwendung von Personenbildern für Werbezwecke liegt regelmäßig eine Verletzung von Interessen der/des Abgebildeten vor.

Da schwer beurteilt werden kann, ob die Veröffentlichung eines Bildes jemanden verletzen könnte, **sollte in jedem Fall die Zustimmung** der/des Abgebildeten eingeholt werden.

Weiters findet man eine sehr gute Erklärung auf der Internet Ombudsstelle: [Mein Bild im Netz](#) und noch genauer unter: [Was ist das Recht am eigenen Bild?](#)

## 2.4 Cyber-Mobbing-Paragraf

Seit dem 1. Jänner 2016 ist Cyber-Mobbing laut Strafgesetzbuch §107c strafbar. Wenn es zu einem Selbstmord des Opfers kommt ist der Strafraum bis zu drei Jahre Haft.

Der folgende Text stammt von [www.oesterreich.gv.at](http://www.oesterreich.gv.at):

Wegen *Cyber-Mobbings* strafbar macht sich, wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

- eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder
- Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen wahrnehmbar macht.

Das Gesetz spricht von Handlungen, die im Wege einer Telekommunikation oder unter Verwendung eines Computersystems erfolgen. Das sind beispielsweise Handlungen über SMS, E-Mails oder Anrufe bzw. Nachrichten über Messenger oder soziale Netzwerke wie beispielsweise WhatsApp.

Weitere Details und Erklärungen findet man auf der FAQ Seite von Saferinternet.at unter [Was sagt das Gesetz zu Cyber-Mobbing](#).

## 2.5 Kinderpornographie

Paragraf §207a Strafgesetzbuch.

Der folgende Text stammt von [www.oesterreich.gv.at](http://www.oesterreich.gv.at):

In Österreich ist der **Besitz** kinderpornografischer Darstellungen ebenso wie der **wissentliche Zugriff** auf kinderpornografische Darstellungen im Internet **strafbar**. Kinderpornografie können bildliche Darstellungen von geschlechtlichen Handlungen, in die Minderjährige involviert sind, oder die Abbildung der Genitalien oder der Schamgegend von Minderjährigen sein. Missbrauchsdarstellungen von Kindern unter 14 Jahren sind immer strafbar. Bereits der Eindruck, dass es zu einer sexuellen Handlung gekommen ist, reicht aus (z.B. Fotomontagen).

In der Regel werden die Inhalte einer Seite schon beim bloßen Ansehen im Internet automatisch auf der Festplatte gespeichert (meist in einem Ordner für temporäre Dateien) – **bereits das kann als Besitz eines Bildes gelten**. Wissentlicher Zugriff kann z.B. angenommen werden, wenn auf eine Seite mit eindeutigem Inhalt wiederholt zugegriffen wird.

[Sexting](#), der Trend erotische Selbstaufnahmen zu versenden, kann weitreichende Folgen haben, sepeziell wenn die Kinder noch nicht 14 Jahre alt sind (Besitzer des Smartphones ist ja meist ein Elternteil!). Ab 14 Jahre könne Jugendliche erotische Fotos oder Videos von sich selbst einvernehmlich tauschen, aber nicht an dritte weitergeben.

## 2.6 Hass im Netz

Der folgende Text stammt von [www.oesterreich.gv.at](http://www.oesterreich.gv.at):

Seit 1. April 2021 müssen Onlineplattformen wie Facebook, Instagram oder Twitter einfachere Möglichkeiten bieten, rechtswidrige Inhalte zu löschen. Enthalten Beiträge beispielsweise offensichtlich **Hetze, Verleumdung, gefährliche Drohungen**, oder stellen **Mobbing** dar, müssen die Plattformbetreiber den betroffenen Inhalt innerhalb von 24 Stunden entfernen. Ist eine genauere Prüfung der Inhalte nötig, muss gegebenenfalls eine Löschung innerhalb von sieben Tagen erfolgen.

Details findet man unter [parlament.gv.at](http://parlament.gv.at)

## 2.7 Nationalsozialistische Wiederbetätigung

Nationalsozialistische Wiederbetätigung ist gemäß Verbots- und Abzeichengesetz verboten. Auszüge aus den Gesetzestexten und Erklärungen dazu findet man gut erklärt auf [stopline.at](https://stopline.at).

Prinzipiell gilt, dass

- die Leugnung von NS-Verbrechen
- die Verherrlichung von NS-Gedankengut
- die Darstellung verbotener Abzeichen und Uniformen

verboten ist.

### 3 Soziale Aspekte und Themen die ich mit meinem Kind besprechen sollte

Im Laufe seiner Internetnutzung kommt ihr Kind früher oder später mit problematischen Inhalten in Kontakt. In diesem Kapitel werden Themen aufgelistet, die man mit seinem Kind besprechen sollte um es darauf vorzubereiten. Da diese Themen sehr umfangreich sind werden jeweils kurze Inputs oder Stichworte angegeben, ohne Anspruch auf Vollständigkeit.

#### 3.1 Rechtliche Besitzer des Smartphones und Vertragsdetails

- Dem Kind klarmachen, dass man als Elternteil der Besitzer des Smartphones ist, und damit auch **rechtlich verantwortlich** ist, wenn damit problematische Dinge gemacht werden.
- Die Details des Vertrages sollten auch mit dem Kind besprochen werden z.B. Roaming, Datenlimits, usw.

#### 3.2 Einen eigenen Mediennutzungsvertrag mit dem Kind erstellen

- Es ist sehr sinnvoll einen eigenen Mediennutzungsvertrag mit dem Kind zu erstellen. Bei auftretenden Problemen oder Unstimmigkeiten kann man sich auf den Vertrag berufen.
- Im Zug dieser Vertragserstellung können über problematische Dinge gesprochen werden und Zeitlimits festgelegt werden.
- Es sollte auch eine Klausel enthalten sein, in dem man dem Kind versichert, dass man zwar gemeinsam mit dem Kind manchmal z.B. Chatverläufe kontrolliert, aber das Kind **nie heimlich überwacht** (z.B. mit Tools wie Google Family Link siehe Kapitel 4.1.1 auf Seite 12).

Eine sehr gute Webseite um einen individuellen (mit vielen vordefinierten Regeln) Mediennutzungsvertrag zwischen mir und meinem Kind zu erstellen findet man auf: [mediennutzungsvertrag.de](https://mediennutzungsvertrag.de)

##### 3.2.1 Wann und wo schläft das Handy?

Eventuell auch in den Medienvertrag mit aufnehmen:

- Von wann bis wann ist das Smartphone ausgeschaltet?
- Wo schläft es und wo wird es aufgeladen?
- Eventuell eine Handy-Garage bauen wo die Smartphones über Nacht abgelegt und aufgeladen werden (nicht in den Schlafträumen und eventuell feuerfest (Akku-Brand) bauen).

#### 3.3 Recht am eigenen Bild

- Dass man keine Fotos oder Videos, die Menschen verletzen oder bloßstellen, im Internet posten darf.
- Am besten ist es immer die Erlaubnis der Personen, die im Foto abgebildet sind, einzuholen.
- Wenn es Bilder vom eigenem Kind im Netz gibt, die es peinlich oder verletzend findet, soll es sich an die Eltern wenden.



### 3.4 Cyber-Mobbing

OECD Studie aus dem Jahr 2015: Einer von fünf Schulbuben zwischen 11 und 15 ist von *Bullying* betroffen - doppelt so viele wie im OECD-Schnitt, fünfmal mehr als in Schweden! Mehr Information dazu auf [derstandard.at](http://derstandard.at)

#### 3.4.1 Wie bereite ich mein Kind auf mögliches Mobbing vor?

- Erklären was Mobbing bzw. Cybermobbing ist.  
[Was-ist-Cybermobbing?](#)
- Erklären dass es seit 2016 verboten und strafbar ist: Strafgesetzbuch § 107c  
[Erklärung-Gesetzestext](#)
- Wenn es mobbing wahrnimmt, aber selber nicht Opfer ist:  
Es loben wenn es zu ihnen kommt. Es ermutigen dem Täter zu widersprechen, ihn auffordern es zu unterlassen, es als mobbing benennen, eventuell mit Freunden gemeinsam auftreten;
- Es allgemein zu ermutigen für die *Schwachen* einzustehen; Misstände anzusprechen und nicht *wegschauen*.

#### 3.4.2 Was tun wenn mein Kind von Mobbing betroffen ist?

Mobbing muss immer in der Gruppe gelöst werden in der es stattfindet, also z.B. in der Schule, im Verein, usw.

- Nicht das Kind nach dem *WARUM* fragen! (Impliziert ein Schuld: Was hast du getan um diese Reaktion hervorzurufen?)
- Es loben, dass es sich damit an sie wendet, denn dies ist kein einfacher Schritt für das Kind!
- Die Beweise sichern und dann wenn möglich vom Smartphone des Kindes löschen, da diese meist belasten.
- Gemeinsam überlegen wer helfen kann: Unbedingt die Lehrperson, den Trainer, den Vereinsverantwortlichen informieren! Dieser muss das Problem in der Gruppe lösen z.B. mit *no blame approach*!  
[no-blame-approach](#) oder sich qualifizierte Hilfe holen.

#### 3.4.3 Mobbing in der Schule

Wenn das Mobbing in der Schule auftritt, muss unbedingt der Lehrer informiert werden!

Geben sie den Verantwortlichen Zeit die Lage zu klären. Wenn sie das Gefühl haben, dass die Lehrperson mit der Situation selbst überfordert ist, dann empfehlen sie doch:

- Professionelle Hilfe holen z.B. von [Saferinternet.at](http://Saferinternet.at) oder nach [no-blame-approach](#) vorgehen.
- Einzelgespräche mit Täter und Opfer.
- Nicht im Plenum besprechen!
- Eventuell mit den *Beobachtern* arbeiten, sie sensibilisieren und dazu bringen, sich gegen Mobbing stark zu machen.

#### 3.4.4 Was sage ich meinem Kind zu Cyber-Mobbing?

- **Schreibe oder poste nichts** im Netz was du der entsprechenden Person **nicht auch von Angesicht zu Angesicht sagen würdest**.
- Sein höflich und ehrlich in deinen Posts.
- Wenn du Mobbing gegen jemand anderen bemerkst, dann schau nicht weg, sondern benenne es klar und fordere den Täter auf, es zu unterlassen.
- Hol dir Hilfe wenn du dich überfordert fühlst!

### 3.5 Sex

Bevor man Themen wie Pornographie und Kinderpornographie mit seinem Kind besprechen kann, muss zuerst ein oder mehrere allgemeine Aufklärungsgespräche stattfinden.

Eine sehr gute Webseite zu dem Thema ist [firstlove.at](http://firstlove.at).

Ebenfalls eine sehr gute Webseite zu diesem Thema ist [s-talks.at](http://s-talks.at). Hier liegt der Schwerpunkt auf einem vertrauensvollen und sicheren Umgang mit dem Internet als Informationsquelle zu Liebe und Sexualität.

### 3.6 Pornographie

Kinder kommen bei der Mediennutzung unweigerlich mit Pornographie in Kontakt. Sei es aus eigenem Interesse, durch Zufall, oder weil es einem der oder die beste Freundin auf ihrem Smartphone zeigt. Auf eventuelle technische Jugendschutzfilter kann man sich nicht zu hundert Prozent verlassen, deshalb ist es wichtig das Thema Pornographie anzusprechen.

Eine ausführliche Broschüre gibt es von der Bayrischen Landeszentrale für neue Medien und der Aktion Jugendschutz: [Wie erkläre ich das meinem Kind? Darstellung von Sexualität in den Medien.](#)

#### 3.6.1 Warum unreflektierter Pornokonsum problematisch ist

Kinder und Jugendliche entwickeln nach und nach ihr Körperbewusstsein und suchen dabei nach Vorbildern, auch in den Medien. Stolpern sie dabei über Pornographie und wird diese als *normal* oder *standard* angesehen, kann dies sehr problematisch für die Entwicklung der eigenen Sexualität sein.

Deshalb ist Pornographie erst ab 18 Jahren freigegeben!

#### 3.6.2 Ein Porno ist ein Film

Die folgende Definition stammt von der Beratungsstelle [sex-profamilia.de](#) vom deutschen Bundesland Nordrhein-Westfalen:

In Pornofilmen werden sexuelle Fantasien in einem **Drehbuch** beschrieben und die Szene wird von den Darstellenden **gespielt**. Es werden sexuelle Praktiken gezeigt, die erregend sein sollen, Gefühle sind nicht sichtbar. Pornos zeigen nicht, wie Sexualität im Leben wirklich funktioniert, und auch nicht, wie vielfältig die Körper von Menschen sind. In vielen Pornos werden **Frauen schlecht behandelt**.

#### 3.6.3 Was sage ich meinem Kind zu Pornographie?

- Ein Porno stellt in den allermeisten Fällen keine normale Sexualität dar!
- Die Schauspieler (Pornostars) werden nach ihren körperlichen Eigenschaften ausgewählt! d.h. dein Penis / deine Brust muss nicht gleich groß sein wie bei Pornostar XYZ!
- Pornos werden hauptsächlich für Männer und männliche Fantasien gemacht und zeigen meist ein verfälschtes Frauenbild!
- Messe und vergleiche deine eigene Sexualität nicht mit Pornos, mit den *Marvel Avengers* vergleichst du dich ja auch nicht!

#### 3.6.4 Was tun bei Kinderpornographie?

Wenn das Kind Bilder oder Videos bekommt, auf denen Kinder oder sehr jung aussehende Jugendliche nackt oder bei sexuellen Handlungen zu sehen sind:

- Die Inhalte nicht weiter verschicken!
- Eltern oder Vertrauensperson informieren!
- Rad auf Draht anrufen und/oder bei [stopline.at](#) melden.
- Löschen erst nach Aufforderung durch autorisierte Personen z.B. Stopline-Mitarbeiter, weil eventuell zur Beweissicherung notwendig.
- Beim Löschen ist es wichtig alle Inhalte zu löschen, also auch an versteckte Dateien, Backups, Cloudspeicher usw. denken!

### 3.7 Sexting

Sexting passiert laut Umfragen unter Jugendlichen relativ häufig. Solange die Jugendlichen 14 Jahre alt oder älter sind und es einvernehmlich passiert hat es auch keine rechtlichen Folgen. Probleme entstehen jedoch oft im Nachhinein, wenn Beziehungen einseitig auseinander gehen und Sexting Inhalte dann aus Rache mit Dritten geteilt werden oder für Erpressung benutzt werden.

### 3.7.1 Was sage ich meinem Kind zu Sexting?

- Lass dich nicht unter Druck setzen ein Nacktbild oder Video von dir zu versenden! Es gibt auch andere Liebes- und Vertrauensbeweise!
- *Wenn ich das nicht schicke, liebt er mich nicht* - stimmt nicht! - **wenn er verlangt, dass du das schickst, liebt er dich nicht!**
- Auch wenn du momentan so verliebt bist und dem Menschen sehr vertraut, können Beziehungen auch leider im Streit auseinandergehen, und dann möchtest du sicher nicht, dass jemand Nacktbilder von dir hat.
- Wenn du Sexting-Inhalte bekommst, dann teile sie nicht mit anderen und lösche sie, sobald du mit der betroffenen Person nicht mehr in einer Beziehung bist.

## 3.8 Cyber-Grooming

Cybergrooming ist das gezielte Ansprechen Minderjähriger über das Internet mit dem Ziel, sexuelle Kontakte anzubahnen – oft anonym oder unter falschem Namen.

Dabei werden Kinder belästigt und aufgefordert Nacktaufnahmen zu übersenden oder sich mit den TäterInnen im realen Leben zu treffen. Die TäterInnen gehen gezielt vor – anonym oder unter falschem Namen. Sie suchen Kontakt zu den Minderjährigen, versuchen Vertrauen aufzubauen und das Kind in Abhängigkeiten zu verstricken oder zu erpressen.

Mehr Informationen dazu auf [schau-hin.info](https://schau-hin.info) und [saferinternet.at](https://saferinternet.at).

Ein sehr guter TV-Spot um auf Cyber-Grooming aufmerksam zu machen: [Cyber-Grooming TV-Spot](#)

### 3.8.1 Was sage ich meinem Kind zu Cyber-Grooming?

- Cyber-Grooming erklären.
- Fremden in Online-Medien (Chatträumen, Social-Messenger, usw.) nicht blind vertrauen, auch wenn der Kontakt sehr freundlich und nett zu sein scheint.
- Fremde nach Möglichkeit überprüfen und auf die Probe stellen.
- Keine Bilder oder Ortsangaben verschicken - auch auf die Privatsphäreinstellung der verschiedenen Dienste achten! Dazu siehe [saferinternet.at/privatsphaere-leitfaeden](https://saferinternet.at/privatsphaere-leitfaeden)
- Wenn einseitige Aufforderungen kommen Bilder zu schicken oder die Webcam einzuschalten, skeptisch werden und üben wie man **stop** und **halt** sagt!
- Wenn das Bauchgefühl nicht passt, den Kontakt abbrechen und die Eltern informieren.
- Falls man schon Bilder geschickt hat und erpresst wird, unbedingt zu den Eltern gehen! Auch wenn gedroht wird, dass den Eltern oder dem Kind etwas Schlimmes passieren wird wenn man dies macht.

## 3.9 Selbstwertgefühl und Schönheitsideale

Es ist mittlerweile sehr einfach, Fotos von sich oder anderen mit diversen Filterprogrammen zu verändern. Vor allem durch die Werbung oder auch auf YouTube werden uns stark veränderte Inhalte präsentiert und erzeugen neue Schönheitsideale.

Es gibt von der Kosmetikfirma Dove ein paar super Videos zu diesem Thema, hier die Links:

[Reverse-Selfie](#)

[Frau-aus-der-Werbung](#)

[Selfie](#)

### 3.9.1 Was sage ich meinem Kind zum Thema Schönheitsideale

- Dass es völlig okay ist so auszusehen wie man ist!
- Dass Schönheit von innen kommt.
- Dass es nichts bringt wenn man sich online übertrieben verändert, weil man sich im richtigen Leben ja meistens doch von Angesicht zu Angesicht gegenüber steht.
- Achtung auf die Vorbildwirkung von Eltern, vor allem von Vätern! Bitte bedenken, wie man selbst über das Aussehen von anderen vor den eigenen Kindern spricht.

### 3.9.2 Pro-Ana und Pro-Mia Chatgroups und Coaches

Ein kurze Erklärung zum Thema von [saferinternet.at](http://saferinternet.at):

**Ana** ist die Abkürzung für Anorexia Nervosa (**Magersucht**), **Mia** für Bulimia Nervosa (**Ess-Brechsucht**). Beide Krankheitsbilder fallen in den Bereich der Essstörungen. Als Essstörung wird ein auffälliges und von der Norm abweichendes Essverhalten bezeichnet. Betroffene dieser beiden Erkrankungen bezeichnen sich selbst oft als *Ich bin (Pro-)Ana* bzw. *Ich bin (Pro-)Mia*.

Im Internet können sich Betroffene schnell und einfach über die Krankheit informieren und sich bei professionellen Angeboten Hilfe holen. Über Suchmaschinen stolpern Jugendliche aber immer wieder über privat initiierte Pro-Ana- und Pro-Mia-Plattformen, z. B. auf der Suche nach Diät-Tipps. In vielen Fällen suchen die Betroffenen aber auch gezielt Kontakt zu anderen Essgestörten.

Auf diesen Pro-Ana- bzw. -Mia-Plattformen werden die Risiken von Essstörungen verharmlost und die Krankheit als Lifestyle propagiert – **dünn sein** ist das einzige Lebensziel. Die BetreiberInnen – meist selbst essgestört – zeichnen sich durch mangelnde Krankheitseinsicht aus und glorifizieren Essstörungen in Blogs, Diskussionsforen, Sozialen Netzwerken (z. B. Instagram, Tumblr, Facebook) oder auf Video-Portalen (z. B. YouTube).

Als Motivation zum Abnehmen werden Bilder von extrem dünnen Menschen oder Models als Beispiele für Schlankheit gesucht und geteilt (sog. **Thinspirations**). In der Szene haben sich auch gefährliche Schönheitsideale etabliert, dazu finden sich im Internet leider tausende Fotos (z. B. **Thigh Gap** oder **Bikini Bridge**).

Betroffene organisieren sich oft in privaten Pro-Ana-Gruppen, etwa in WhatsApp oder Kik. Die Gruppenmitglieder folgen strengen Diät- und Sport-Regeln, führen Ess-/Gewichtstagebücher und schicken einander regelmäßig Fotos des eigenen Körpers. Fasten-Wettbewerbe und Abnehmverträge etc. binden die essgestörten Mitglieder an die Gemeinschaft – wer die Gebote nicht befolgt wird aus der Gruppe ausgeschlossen.

Leider gibt es mittlerweile eine Vielzahl von Webseite und Chaträumen zu Pro-Ana. Schlagwort oder Suchbegriff: **Schöne Mädchen essen nicht!**. Sollte ihr Kind Anzeichen von Aorexie oder Bulimie zeigen,holen sie sich unbedingt professionelle Hilfe! Ansprechpartner finden sie auf: [Österreichische Gesellschaft für Essstörungen](http://Österreichische Gesellschaft für Essstörungen).

Als wäre das Thema an sich noch nicht schlimm genug, treten nun auch Pädophile als sogenannte **Pro-Ana-Coaches** auf. Als selbst ernannte **Coaches** bieten sie auf Blogs und in Foren ihre Unterstützung beim Abnehmen an und verlangen in weiterer Folge regelmäßig Nacktfotos bzw. Bilder in aufreizenden Posen von den essgestörten Mädchen.

### 3.10 Nationalsozialistische Wiederbetätigung

Wenn das Kind Bilder, Videos oder Messages bekommt auf denen NS-Verbrechen geleugnet werden, NS-Gedankengut verherrlicht wird oder NS-Symbole, Abzeichen oder Uniformen sind:

- Die Inhalte nicht weiter verschicken!
- Eltern oder Vertrauensperson informieren!
- Rad auf Draht anrufen und/oder bei [stopline.at](http://stopline.at) melden.
- Löschen erst nach Aufforderung durch autorisierte Personen z.B. Stopline-Mitarbeiter, weil eventuell zur Beweissicherung notwendig.
- Beim Löschen ist es wichtig alle Inhalte zu löschen, also auch an versteckte Dateien, Backups, Cloudspeicher usw. denken!

### 3.11 Allgemeines zu Privatsphäre und Vergessen im Netz

Ein sehr umfangreiches Thema das von vielen Menschen mit der Aussage *Ich hab eh nichts zu verbergen* heruntergespielt wird.

Leider ist es aber so, dass persönliche Daten das Gold des 21. Jahrhundert sind. Facebook und Google sind an der Börse Milliarden wert, handeln aber eigentlich fast nur mit persönlichen Informationen ihrer Nutzer.

Es gibt online eine Vielzahl von Informationen zum Schutz der Privatsphäre z.B. von [saferinternet.at](http://saferinternet.at)

### 3.11.1 Zwei kleine Beispiele zum Thema: Warum Datenschutz wichtig ist

- Du bist ein leidenschaftlicher Mountainbiker und postest tolle Videos und Bilder von deinen spektakulären Abfahrten und Sprüngen. Jetzt bist du auf der Suche nach einer Unfallversicherung - diese recherchieren aber über dich und stufen dich als Hochrisiko-Person ein. Dies kann dazu führen, dass sie dir keinen Vertrag geben oder höhere Gebühren verlangen!
- Du bist der Chef eines kleinen Unternehmens und willst einen neuen Mitarbeiter einstellen. Du hast zwei tolle Bewerber, beide gleich gut qualifiziert, beide sehr sympatisch. Um dir die Entscheidung leichter zu machen, recherchierst du im Netz und findest heraus, dass einer der beiden bei einer Online-Apotheke regelmäßig Diabetes Medikamente für seine Mutter bestellt. Du weißt, dass Diabetes vererbt werden kann und er wahrscheinlich ein höheres Risiko hat an Diabetes zu erkranken.  
Wenn von den beiden stellst du ein?

### 3.11.2 Was sage ich meinem Kind zum Thema Privatsphäre?

- Überlege dir gut was du über dich ins Netz stellst, denn es vergisst nicht oder nur sehr schwer!
- Verwende keine Like-Buttons, denn darüber werden automatisch Benutzerprofile erstellt. Schreibe deine Zustimmung lieber als Post mit ein paar persönlichen Zeilen.
- Verwende für die verschiedenen Apps oder Services nicht überall das gleiche Passwort! Wenn eine App einem Hackerangriff zum Opfer fällt und deine e-mail Adresse und dein Passwort öffentlich werden sind alle deine Zugänge betroffen!
- Verwende einen Passwortmanager wie z.B. [keepassxc](#) damit du mit vielen Passwörtern besser klar kommst.
- Überlege dir eine gute, lange Passwort-Phrase für das Master-Passwort des Passwortmanagers! Sieh dazu Punkt [3.11.3](#) auf Seite [10](#).
- Achte auf die Datenschutzeinstellungen deiner Apps! Hilfe dazu gibt es z.B. auf [saferinternet.at](#)

### 3.11.3 Wie erstelle ich in drei Schritten eine gute Passwort-Phrase?

1. Überlege dir einen für dich passenden Satz z.B.:  
**Ich kann super gut klettern.**
2. Schreibe den Satz ohne Leerzeichen und mit einem Großbuchstaben bei jedem Wortanfang und mit einem Sonderzeichen z.B. ! am Satzende z.B.:  
**IchKannSuperGutKlettern!**
3. Nun ersetze ausgeählte Buchstaben durch Zahlen z.B. i=1, e=3, s=5, o=0 dann wird aus deinem Satz:  
**1chKann5up3rGutKl3tt3rn!**  
Ein starkes Passwort, dass du dir aber trotzdem relativ leicht merken kannst!

## 3.12 Social-Media und Messenger

An Social Media und Messengern führt heutzutage kein Weg mehr vorbei. Aber damit z.B. bei der ersten Klassen-gruppe in WhatsApp nicht jeden morgen 200 Nachrichten am Telefon sind, sind Regeln und die Mithilfe der Eltern notwendig.

Es ist z.B. sinnvoll bei einem Elternabend in der Schule über dieses Thema zu sprechen und Regeln zu vereinbaren z.B. dass keine Messages zwischen 19 und 7 Uhr verschickt werden. Wichtig ist dann aber auch, dass sich alle daran halten. Wenn man es nur seinem Kind vorschreibt kann es zu *FOMO - Fear of missing out* führen.

### 3.12.1 Welcher Messenger?

- **WhatsApp** ist eine Datenkrake und Facebook wird auch immer wieder wegen Verstößen gegen die DSGVO verurteilt, aber die Menschen sind bequem und ein bisschen faul und weil es eh jeder hat verwendet man es halt auch ;-)  
Mit dieser sarkastischen Einleitung möchte ich nur sagen, dass ihr Kind wahrscheinlich WhatsApp verwenden möchte - warum? Weil es alle anderen auch haben!  
In diesem Fall bitte die Privacy-Einstellungen entsprechende anpassen wie in diesem Link erklärt: [saferinternet.at](#)

- **Signal** ist eine open source Alternative und garantiert eine End zu End - Verschlüsselung (WhatsApp geht über Facebook Server). Ausserdem werden nicht alle Kontakte eines Nutzers automatisch übertragen (bei WhatsApp werden sie ungefragt an Facebook weitergegeben). Namhafte Sicherheitsexperten wie z.B. Edward Snowden empfehlen Signal! Link: [signal.org](https://signal.org)

### 3.12.2 Was sage ich meinem Kind zum Thema Messenger?

- Kein Spammen! Schreibe nur sinnvolle Nachrichten.
- Keine Beleidigungen! Kein Mobbing!
- Drücke dich vernünftig und klar aus und achte auf Rechtschreibfehler.
- Keine Kettenbriefe weiterleiten, auch wenn drin steht, dass sonst etwas Schlimmes passiert!  
Eine Möglichkeit mit Kettenbriefen umzugehen ist der Kettenbrief-Chatbot von Saferinternet.at! Mehr Infos dazu auf [der-kettenbrief-chatbot](#)
- Recht am eigenen Bild beachten! Andere Fragen bevor du Bilder von ihnen postest.

## 4 Technische Hilfsmittel

Ein Wort der Warnung zu den technischen Hilfsmitteln. Wie schon der Name der Überschrift suggeriert handelt es sich dabei nur um Hilfsmittel. Keine der vorgestellten Tools kann ein völlig sicheres Internetlebnis ihres Kindes garantieren. Aus diesem Grund möchte ich nochmals daran erinnern, wie wichtig es ist ein gutes Gesprächs und Vertrauensverhältnis zu ihrem Kind zu haben! Im folgenden werden nur Tools aus dem Android-Universum vorgestellt, da für den Autor aufgrund von Datenschutzbedenken Apples-iOS Systeme nicht in Frage kommen.

Man kann bei den Tools grob zwischen Android eigenen Hilfsmittel und zusätzlichen Sicherheits-Apps von externen Anbietern unterscheiden.

### 4.1 Android interne Hilfsmittel

#### 4.1.1 Google Family Link

##### 4.1.1.1 Kurzinfor

Google Family Link ist, wie der Name schon sagt, eine Eigenentwicklung von Google. Die Grundidee ist, dass jedes Familienmitglied ein eigenes Google-Konto hat und diese im Family-Link zusammengeführt sind. Von dort aus können Eltern die Konto-Einstellungen ihrer Kinder verwalten.

##### 4.1.1.2 Funktionsumfang

- Zeitbeschränkungen für die Nutzung von Android- oder Chrome OS-Geräten festlegen
- Standort der angemeldeten und aktiven Android-Geräte ihres Kindes sehen
- Downloads und Käufe ihres Kindes bei Google Play und Stadia genehmigen sowie festlegen, dass dem Kind nur Inhalte angezeigt werden, die seinem Alter entsprechen (*Hinweis -> dies funktioniert nicht zuverlässig, weil sich Google z.B. auf die Mindestalter Angaben von App-Herstellern verlässt und diese nicht überprüft!*)
- SafeSearch für die Google-Suche verwalten (*Hinweis -> dies funktioniert nicht zu 100% und ist nur eine Hilfestellung und keine Garantie, dass ihr Kind keine problematischen Suchergebnisse erhält!*)
- App-Berechtigungen ihres Kindes auf Android- und Chrome OS-Geräten prüfen, beispielsweise für den Zugriff auf Mikrofon, Kamera und Kontakte
- Inhalte, Berechtigungen und anderen Einstellungen für die Nutzung von YouTube und YouTube Kids

##### 4.1.1.3 Installation

Die folgenden Installationsschritte stammen von [www.medien-kindersicher.de](http://www.medien-kindersicher.de):

1. Laden Sie sich auf Ihrem eigenen Smartphone im Play Store die App Google Family Link für Eltern herunter und öffnen Sie diese.
2. Wählen Sie *Weiter*, um die Einrichtung zu starten.
3. Ihnen wird nun die Frage gestellt *Hat Ihr Kind ein Google-Konto?* Falls Ihr Kind bereits ein eigenes Google Konto besitzt und dieses auf dessen Smartphone oder Tablet hinterlegt ist, können Sie die Schritte (4) bis (20) überspringen und Ja auswählen. Falls Ihr Kind noch keinen eigenen Google-Account besitzt, wählen Sie Nein und folgen Sie weiter der Anleitung.
4. Tragen Sie Vorname und Nachname Ihres Kindes ein.
5. Tragen Sie Geburtsdatum und Geschlecht Ihres Kindes ein (Wichtig: tragen Sie das Geburtsdatum korrekt ein, damit die Jugendschutzeinstellungen passend konfiguriert werden).
6. Geben Sie einen Nutzernamen für Ihr Kind ein. Da dieser zukünftig auch als E-Mail-Adresse Ihres Kindes verwendet wird, empfehlen wir Ihnen einen Nutzernamen nach folgendem Muster zu erstellen: `vorname.nachname@gmail.com`
7. Erstellen Sie ein Passwort für Ihr Kind. Geben Sie das Passwort zur Bestätigung erneut ein.
8. Sie können nun je nach Erziehungsstil bereits an dieser Stelle Einstellungen für den Google-Account Ihres Kindes vornehmen. Scrollen Sie nach unten und setzen Sie die beiden Häkchen vor Datenschutzerklärung und Nutzungsbedingungen, um diese zu akzeptieren.



9. Möglicherweise müssen Sie nun Ihre Kreditkartendaten angeben, um zu verifizieren, dass Sie eine Erwachsene Person sind (Ihre Kreditkarte wird dadurch nicht belastet).
10. Nun müssen Sie das Google Konto Ihres Kindes mit dem Gerät Ihres Kindes verknüpfen. Falls auf dem Gerät bereits ein anderer Google Account als der Ihres Kindes (z. B. von Ihnen) hinterlegt ist, muss dieser zunächst entfernt werden - siehe Punkte 10 - 14. Wenn ihr Kind noch kein eigenes Google-Konto hat weiter bei 15.
11. Nehmen Sie nun das Gerät Ihres Kindes zur Hand und öffnen Sie die App Einstellungen.
12. Öffnen Sie Konten
13. Wählen Sie Google
14. Wählen Sie Konto entfernen; Bestätigen Sie Entfernen;
15. Nun können Sie das neu erstellte Google Konto Ihres Kindes mit dessen Gerät verknüpfen. Führen Sie zunächst Schritt (11) und (12) aus, um in den Bereich Konten zu gelangen. Wählen Sie Konto hinzufügen: Google
16. Geben Sie die Google-Mail-Adresse Ihres Kindes ein, die Sie erstellt haben.
17. Geben Sie das Google-Passwort Ihres Kindes ein, welches Sie festgelegt haben.
18. Nun wird nach der Erlaubnis der Eltern gefragt, um die Verknüpfung zwischen Gerät und Google-Account herstellen zu können → Geben Sie Ihr eigenes Google-Passwort ein.
19. Stimmen Sie Datenschutz und Bedingungen zu, indem Sie den Button «Ich stimme zu» auswählen.
20. Nun können Sie je nach Erziehungsstil die Einstellungen für das Google-Konto Ihres Kindes konfigurieren. Wenn Sie das korrekte Geburtsdatum Ihres Kindes eingegeben haben, nimmt Google bereits automatisch viele angemessene Einstellungen vor.
21. Folgen Sie den Aufforderungen im Einrichtungsprozess und laden Sie nun die App Family Link-Manager aus dem App Store oder Google Play Store auf das Gerät Ihres Kindes herunter. Hinweis: auf manchen Geräten ist diese schon vorinstalliert. → Geben Sie einen Gerätenamen für das Gerät Ihres Kindes ein.
22. Sie können nun je nach Erziehungsstil die angezeigten Apps für die Nutzung durch Ihr Kind ausschließen und weitere Jugendschutzeinstellungen vornehmen.
23. Sie erhalten abschließend auf beiden Geräten die Benachrichtigung Deine/Eure Geräte sind verbunden

Sie haben nun die Möglichkeit, von Ihrem Elterngerät (Android oder iOS) aus die Einstellungen auf dem Smartphone Ihres Kindes zu steuern. Öffnen Sie dazu die App Family Link für Eltern auf Ihrem Gerät und wählen Sie das Gerät Ihres Kindes aus. Die Einstellungsmöglichkeiten werden Ihnen umgehend angezeigt.

#### 4.1.1.4 Fazit zu Google Family Link

Dieses Fazit stammt von [mobilsicher.de](https://mobilsicher.de):

Die App ist praktisch und enthält viele Funktionen, ermöglicht aber auch eine recht detaillierte Überwachung des Kindes.

Das medienpädagogische Projekt *SCHAU HIN!* empfiehlt, die Standortsuche vor allem bei älteren Kindern nicht zu aktivieren und die App nicht als permanentes Überwachungstool zu nutzen. Besser sei es, im gemeinsamen Gespräch mit den Kindern klare Regeln für die Nutzung von Smartphones und Tablets zu besprechen, den Umgang mit fragwürdigen Inhalten zu klären und insgesamt ein gesundes Nutzungsverhalten vorzuleben. Je nach Einstellung landen darüber hinaus viele Nutzungsdaten des Kindes bei Google. Wenn Sie die Voreinstellungen übernehmen, übermittelt das Gerät viele Details zur Nutzung von Webseiten und Apps.

**Wir raten von Google Family Link ab** und empfehlen stattdessen die datensparsame Alternative TimeLimit des deutschen Entwicklers Jonas Lochmann.

Mehr Infos zu TimeLimit siehe Kapitel 4.5.3 auf Seite 15.



### 4.1.2 YouTube

Lässt sich nicht deinstallieren. Man hat drei Möglichkeiten:

- **YouTube mit App-Locks zu sperren:**  
Es gibt Apps, mit denen sie eine Passwortsperre vor andere Apps legen können. Damit ist YouTube für Ihr Kind nicht nutzbar. Nachteil: Ihr Kind lernt die YouTube-Welt nicht kennen und kann nicht selber experimentieren.
- **Filter:**  
Sie können in YouTube den *Eingeschränkten Modus* aktivieren. YouTube versucht dann, nicht jugendfreie Inhalte zu filtern. Ganz sicher ist der Filter aber nicht. Außerdem ist er nicht mit einer PIN gesperrt, Ihr Kind kann den Filter also deaktivieren.
- **YouTube Kids:**  
Google bietet mit YouTube Kids eine eigene App an, die den Zugang zur YouTube-Plattform kindersicher machen soll. Vorteil: Hier kann man bestimmte Sicherungen einbauen und Nutzungszeiten festlegen, die auch mit PIN gesichert sind. Nachteil: Auch hier können unangemessene Inhalte durchrutschen, aber seltener als auf YouTube. Die originale YouTube-App sollten sie dann mit einer *App Lock*-App sperren.  
Ein weiterer Nachteil sind die personalisierten Werbeeinschaltungen - Google weiß, was ihr Kind mag! Als mögliche Lösung dazu bietet sich *Blokada* an, siehe Kapitel 4.5.2 auf Seite: 15.  
YouTube Kids kann via Google Family Link konfiguriert werden, siehe dazu Kapitel 4.1.1 auf Seite 12.

## 4.2 Browser und Suchmaschinen

Auch Googles Browser Chrome lässt sich nicht deinstallieren und öffnet Ihrem Kind den Weg zu sämtlichen Inhalten des World Wide Web. Es gibt verschiedene Optionen, Kindern je nach Alter einen halbwegs geschützten Zugang ins Internet zu ermöglichen.

### 4.2.1 Browser Erweiterungen

- **Firefox** kann z.B. mit der Browsererweiterung [family-friendly-filter](#) ausgestattet werden. Es arbeitet mit Black- und Whitelists, um für Kinder unangemessene Inhalte zu filtern.
- **Chrome** kann ebenfalls erweitert werden: z.B. mit [TinyFilter](#).

### 4.2.2 Suchmaschinen für Kinder

Eine weitere Möglichkeit unangenehme Suchergebnisse zu vermeiden, sind spezielle Suchmaschinen für Kinder, die z.B. als Startseite im Browser eingestellt werden können. Besonders gute Referenzen hat die Deutsche Webseite [fragfinn.de](#)

## 4.3 In-App-Käufe vermeiden

Unter Android lassen sich die In-App-Käufe mit einem Passwort sichern. Wenn man es nicht schon über die Family-Link-App eingestellt hat, kann man es über den Google Play Store einrichten.

Eine Schritt für Schritt Anleitung findet man auf [saferinternet.at](#)

## 4.4 Sprach-Assistenten deaktivieren

Aus Privacy-Gründen sollte die Sprachunterstützung deaktiviert werden. Eine detaillierte Anleitung dazu findet man z.B. auf [zdnet.de](#)

## 4.5 Externe FOSS Apps

Es gibt eine Vielzahl von Apps, die alle möglichen und unmöglichen Sicherheitseinstellungen bieten. Der Markt ist unübersichtlich groß und man muss den App Anbietern meist blind vertrauen. Eine Alternative dazu sind FOSS - Free and Open Source Apps, deren Quellcode offen liegt. Im Folgenden werden ein paar ausgewählte FOSS-Apps vorgestellt, die eine ähnliche Kontrolle wie mit Google Family Link ermöglichen, aber ohne das Google über das Nutzungsverhalten ihres Kindes Bescheid weiß!

#### 4.5.1 F-Droid

[F-Droid](#) ist eine verbraucherfreundliche Alternative zu Googles Play-Store. Auf F-Droid wird nur FOSS (Free and Open Source Software) angeboten. Um ihn zu nutzen, muss man die F-Droid-App von der Webseite herunterladen und auf dem Handy installieren, das ist etwas ungewohnt aber notwendig weil Google aus Konkurrenzgründen die App nicht in seinem Play-Store haben will.

Eine detaillierte Installationsanleitung findet sich auf [mobilsicher.de](https://mobilsicher.de)

#### 4.5.2 Blokada

Die meisten Apps aus dem Google Play Store beinhalten Software-Bausteine von Drittanbietern, die dem Nutzer Werbung einblenden oder seine Aktivität auf Schritt und Tritt verfolgen. Mit [blokada.org](https://blokada.org) kann man der Werbung und dem Abfluss von persönlichen Daten an zweifelhafte Drittanbieter einen Riegel vorschieben.

Blokada blockiert Werbung und Tracker nicht nur im Browser, sondern in allen Apps, die auf dem Gerät installiert sind. Aus diesem Grund ist Blokada auch nicht im Google Play Store, da dies gegen das Geschäftsmodell von Google verstößt - auf F-Droid findet man Blokada aber sehr wohl.

Eine detaillierte Installationsanleitung findet man auf [kuketz-blog.de](https://kuketz-blog.de)

#### 4.5.3 Time Limit

[timelimit.io](https://timelimit.io) ist eine Open-Source Datenschutz-Alternative zu Family-Link um die Nutzungszeit des Smartphones einzustellen.

Es kann sehr genau eingestellt werden, wann und wie viel etwas genutzt werden darf. Es ist z.B. möglich, die Gesamtspieldauer am Wochenende einzuschränken oder Spiele ab 18 Uhr zu sperren. Dabei können für verschiedene Apps andere Einschränkungen gewählt werden.

TimeLimit erstellt kein detailliertes Protokoll. Im lokalen Modus bleiben sämtliche Daten auf dem Gerät und werden nicht übertragen. Wenn Sie den vernetzten Modus verwenden, werden Daten an einen Server Ihrer Wahl übertragen.

[timelimit.io](https://timelimit.io) ist ebenfalls auf [F-Droid](#) erhältlich.

#### 4.5.4 UsageDirect

[UsageDirect](#) ist ebenfalls über [F-Droid](#) beziehbar und bietet eine App-Nutzungs Aufzeichnungs-Alternative zu Family Link.

[UsageDirect](#) ermöglicht es per Nutzungsdatenzugriff die vom System geführte Nutzungsstatistik anzuzeigen; Damit kann man die Nutzungsdauer und den Zeitpunkt der letzten Nutzung je App sehen für den Tag, die Woche, den Monat oder das Jahr; Die Apps werden dort absteigend nach der Nutzungsdauer sortiert, sodass man schnell einen Überblick bekommen kann.

Achtung: Diese App geht schon wieder in Richtung Überwachung und der Einsatz sollte mit ihrem Kind besprochen werden!

#### 4.5.5 App Locks

App-Locks sind eine nützliche Alternative um nicht de-installierbare Apps zu sperren. Es gibt eine Vielzahl von App-Locks im Google Play-Store und auch auf F-Droid.

### 4.6 Alternative Betriebssystem

Für fortgeschrittene Nutzer, die ihre Privatsphäre besser schützen möchten, bietet sich auch die Möglichkeit an auf ein alternatives, Android basiertes Betriebssystem, aber ohne Google-Zwang, auszuweichen.

Leider werden nicht immer alle Smartphones unterstützt, daher am besten auf den Homepages der Projekte nach unterstützten Geräten suchen.

Die im Folgenden verlinkten drei Alternativen zu Googles-Android sind alle empfehlenswert und es wird dem interessierten Nutzer überlassen, das für ihn passende Betriebssystem zu finden.

#### 4.6.1 LineageOS

[lineageos.org](https://lineageos.org)

#### 4.6.2 GrapheneOS

[grapheneos.org](https://grapheneos.org)

#### 4.6.3 e-OS

e-OS

## 5 Abschließende Worte

Ich möchte nochmals darauf hinweisen, dass dieses Dokument keinen Anspruch auf Vollständigkeit hat. Ich hoffe aber, dass es als Leitfaden für technische Einstellungen am Smartphone und für Gespräche mit ihrem Kind hilfreich ist. Offene Gespräche, Vertrauen sowie die Bereitschaft online Zeit mit ihrem Kind zu verbringen erachte ich als ganz wichtig. Lassen sie sich zeigen, was ihr Kind schon alles am Smartphone kann, welche Spiele es spielt, welche Apps es toll findet usw. Bleiben sie informiert!

Wenn meine Tochter nun bald ihr Smartphone bekommt, nehme ich mir vor aufmerksam zu sein und Zeit mit ihr am Smartphone zu verbringen. Ich werde mir ihre Lieblings-Apps, Spiele und ihr Social-Media Verhalten ansehen und gegebenenfalls mit ihr gemeinsam kritisch hinterfragen.

Über konstruktive Kritik oder Ergänzungsvorschläge zu diesem Leitfaden freue ich mich!  
e-Mail: markus.signitzer@htlinn.ac.at