# Das Social Network Training
# Tipps & Empfehlungen

## *Hintergründe*

Die Nutzung von Smartphones beginnt heute in der Regel mit dem Übergang in die weiterführenden Schulen, immer häufigerschon davor. Ohne Anleitung entstehen erste Schäden meist sofort mit Beginn der Nutzung, vor allem in Bezug auf:

- Umgang mit sensiblen persönlichen Daten
- Preisgabe von kritischen Inhalten wie Fotos und Videos
- Viren, Schadsoftware und fehlende Kenntnisse über die Standardeinstellungen
- Negative soziale Erfahrungen in der Gruppe

Nachfolgend haben wir einige Tipps zusammengestellt, wie Sie als Eltern Ihre Kinder im Umgang mit den Neuen Medien unterstützen und voneinander lernen können.

## *Software-Tipps*

Sie können bereits mit wenigen Einstellungen das Smartphone Ihres Kindes sicherer machen.

**1.Schützen Sie das Smartphone Ihres Kindes vor Viren**

Viren können nicht nur großen Schaden am Gerät anrichten, sondern auch alle möglichen Daten ausspionieren. Oft sind diese Viren sogar als Werbung oder Gewinnspiele getarnt. Installieren Sie deshalb unbedingt eine Antivirus-App. Es gibt eine Vielzahl an kostenlosen und kostenpflichtigen Apps für Android und iOS – kostenlose Varianten sind beispielsweise:

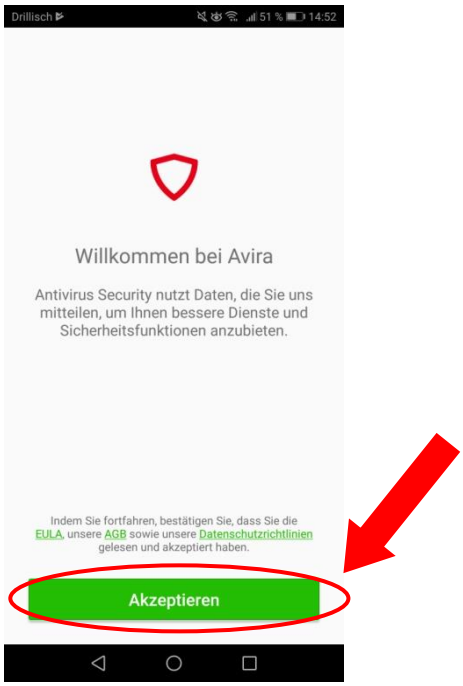
***Avast Mobile Antivirus*** (momentan nur für Android) und

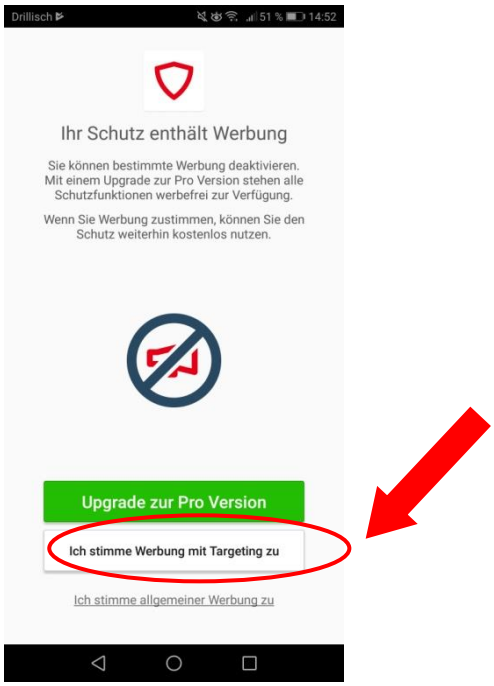
***Avira Antivirus Security*** (Android und iOS).

Diese beiden Programme bilden Platz 1 und 2 in den „Top 100 Antivirus-Downloads aller Zeiten“ beim Computermagazin CHIP[1]. Neben Virenschutz und Datenmüllbereinigung verfügen beide Apps über folgende hilfreiche Zusatzfunktionen: Nach einer Registrierung können Sie ihrSmartphone aufspüren, wenn sie es verlegt haben oderkönnen es im Falle von Verlust oder Diebstahl aus der Ferne sperren.Zusätzlich haben Sie die Möglichkeit, Telefonnummern auf eine Blacklist zu setzen. Einmal gelistet, empfangen Sie von dieser Nummer weder Anrufe noch Nachrichten.Die kostenlosen Versionen von Antivirenprogrammen enthalten zwar auch Werbung, diese ist aber nicht gefährlich. WICHTIG: Bitte nur eine der beiden Apps installieren, da sie sich gegenseitig bekämpfen! Installationsanleitung:

- Suchen Sie die App im Play Store (bei Android) oder im App Store (bei iOS).
- Achten Sie darauf, dass es die kostenlose Version ist!
- Klicken Sie auf „Installieren“ bzw. „Laden“.
- Öffnen Sie die App.

Die Installation von **Avira Antivirus Security** sieht z.B. bei Android so aus:



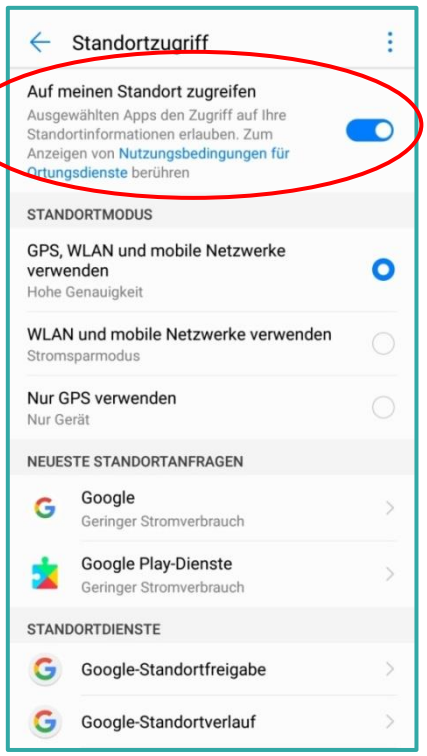

[1]http://www.chip.de/Downloads-Download-Charts-Top-100-aller-Zeiten_32417798.html?xbl_category=39008. Stand: 23.10.2018.

**2. Versperren Sie nerviger Werbung den Weg**

Ständig aufpoppende Fenster mit Sonderangeboten, Empfehlungen, Gutscheinen etc. sind nicht nur nervig, sie können auch gefährlich sein. Denn auch hinter vermeintlichen Werbeanzeigen verstecken sich oft Viren, die durch einen Klick heruntergeladen werden. Es empfiehlt sich daher, einen so genannten AdBlocker zu installieren, der einen Großteil der Werbung abhält. Ein kostenloser AdBlocker ist beispielsweise ***AdBlock Plus*** (Android und iOS).

**3. Schalten Sie Ortungsdienste aus**

Sind die Ortungsdienste auf einem mobilen Gerät aktiviert, werden ständig Standortinformationen gesendet. Das bedeutet zum Beispiel, dass bei jedem Foto, das aufgenommen wird, gleichzeitig der Aufnahmeort gespeichert und bei jeder Google-Suche der momentane Standort gesendet wird. Ortungsdienste sollten nur aktiviert werden, wenn man sie wirklich braucht, z.B. bei der Nutzung von Navigations-Apps wie Google Maps. Bei Android finden Sie unter *Einstellungen* den Menüpunkt *Datenschutz und Sicherheit.* Hier wählen Sie die Option *Standortzugriff*, um Ortungsdienste zu deaktivieren oder bestimmten Apps den Zugriff zu erlauben. Bei iOS finden Sie unter *Einstellungen* den Punkt *Datenschutz* – auch hier können Sie unter *Ortungsdienste* Standortinformationen generell deaktivieren oder für jede App individuell Einstellungen vornehmen:



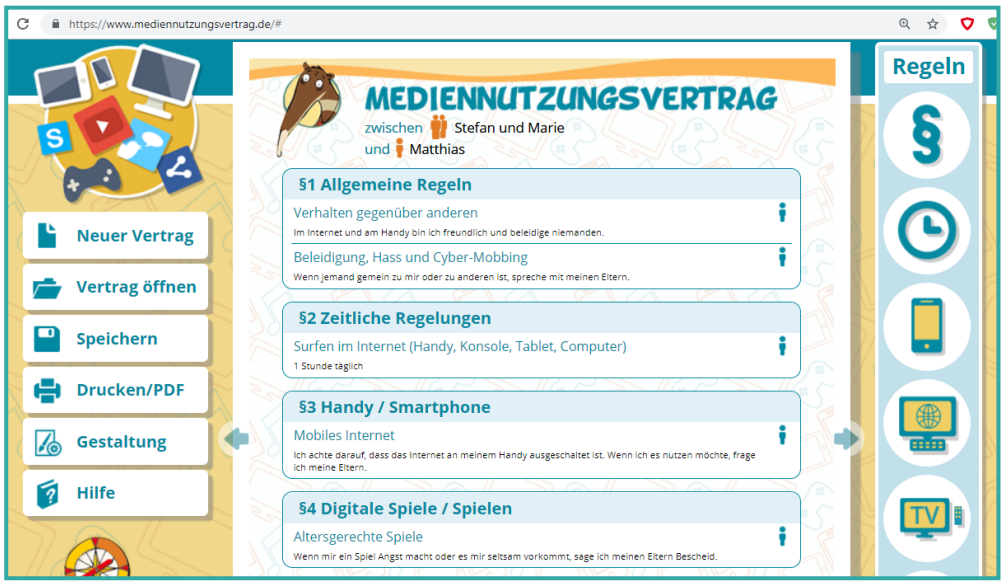

Nur das GPS zu deaktivieren reicht nicht, Standortinformationen werden auch über WLAN und mobile Daten gesendet.

## *Nutzungsgewohnheiten*

Erwachsene können Jugendliche wesentlich darin bestärken, verantwortungsbewusst im Netz zu handeln. Sie wiederum können von Ihren Kindern viel über den Umgang mit sozialen Netzwerken lernen. Sprechen Sie mit ihrem Kind darüber, wo und wie es sich im Internet bewegt. Machen Sie Ihrem Kind bewusst, wo Gefahren lauern können (siehe unter „Typische Internetfallen“).

### 1.Vereinbaren Sie Regeln zur Nutzung des Internets

Sie können hierfür das Angebot der EU-Initiativeklicksafe.de nutzen: Über ein Baukastensystem kann dort ein altersgerechter und für die jeweilige Familie passender Vertrag erstellt werden. Vorbereitete Regeln für die Altersgruppen 6–12 Jahre und für über 12-Jährige erleichtern die Erstellung: [www.mediennutzungsvertrag.de](http://www.mediennutzungsvertrag.de)




Zwei Regeln jedoch sollten auch ohne Vertrag unbedingt beachtet werden:

***Intime Fotos von einem selbst oder von anderen dürfen niemals verschickt oder weitergeleitet werden!***

Leider verschicken Mädchen und Jungs immer öfter und immer früher intime Fotos von sich selbst an ihren Schwarm. Dass diese Fotos dann weitergeleitet werden, belastet die Betroffenen oft jahrelang, viele wechseln sogar Schule und Wohnort. Klären Sie Ihr Kind

darüber auf und besprechen Sie mit ihm, was es tun kann, wenn von einem Mitschüler solche Fotos auftauchen: nicht lachen, sondern helfen!

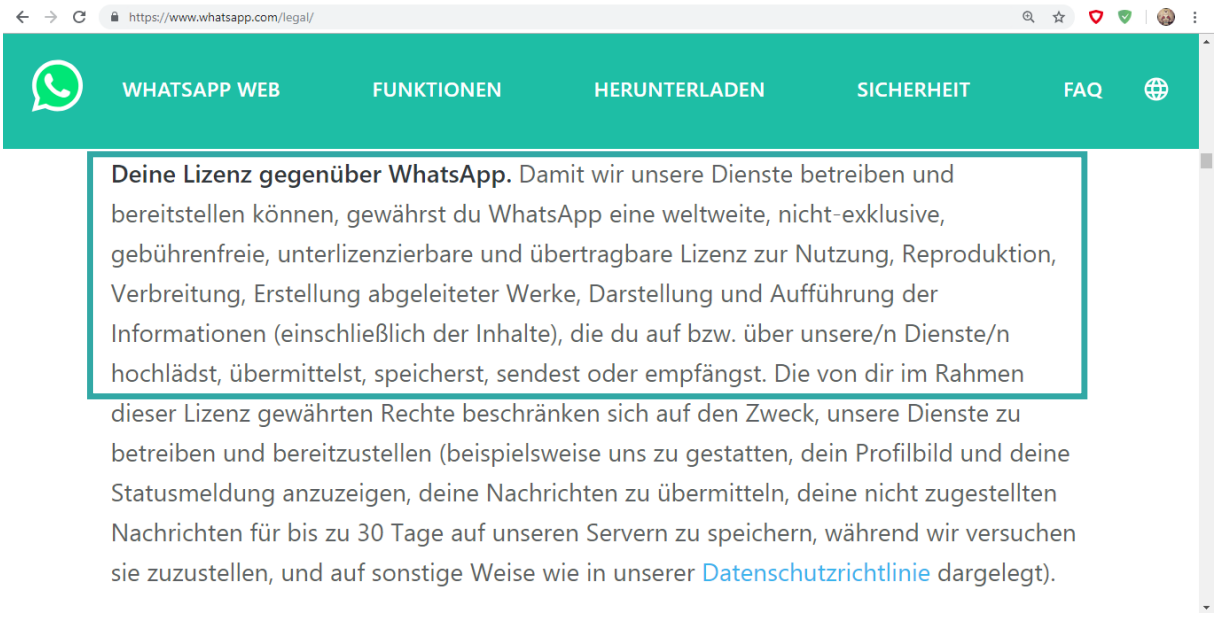
***Sich für andere einsetzen, die gemobbt werden!***

In WhatsApp-Gruppen und anderen sozialen Netzwerken schlägt ein flapsiger schnell in einen beleidigenden Kommentar um, und durch die Gruppendynamik schaukelt sich die Stimmung hoch. Ermutigen Sie Ihr Kind dazu, bei solchen Beleidigungs-Fluten nicht mitzumachen, sondern die anderen dazu aufzufordern, damit aufzuhören. Generell gilt es, so gut es geht darauf zu achten, welchen Umgangston ihr Kind in sozialen Netzwerken pflegt und welchem es ausgesetzt ist. Wenn jemand gemobbt wird reicht es nicht aus, nicht mitzumachen –am wirkungsvollsten ist es als Gruppe hinter dem Opfer zu stehen.

## *Typische Internetfallen*

### 1.WhatsApp ist zwar kostenlos, aber sehr teuer

Kostenlose Apps bezahlt man meist mit seinen Daten. WhatsApp, Instagram und Co. haben in ihren AGBs genau festgelegt, welche Rechte die Programme an den Daten ihrer Nutzer haben. In den Nutzungsbedingungen von WhatsApp beispielsweisefindet man folgende Informationen[2]:




Dieser Satz bedeutet im Prinzip, dass WhatsApp alles, was man dort hochlädt, (Bilder, Texte, Videos oder Audiodateien) nutzen darf, und zwar ganz offiziell mit der Erlaubnis des Nutzers.

[2]In:www.whatsapp.com/legal, Nutzungsbedingungen, Absatz „Lizenzen“. Stand: 18.10.2018.

WhatsApp sammelt außerdem folgende Daten: Telefonnummer, E-Mail-Adresse, Profilnamen, Telefonnummern aus der Kontaktliste und natürlich das Profilbild. WhatsApp speichert auch Nutzungs- und Log-In-Informationen (z.B. wie häufig und wie lange ihr WhatsApp nutzt), und sogar Geräte- und Verbindungsdaten (Modell des Smartphones, Sprache, Zeitzone, Mobilfunknetz) sowie Standortinformationen.

Es gibt kostenpflichtige Alternativen zu WhatsApp, die aber garantieren, alle privaten Daten zu schützen. Sie funktionieren fast genau gleich wie WhatsApp und bieten dieselben Möglichkeiten. Überlegen Sie, ob die gesamte Klasse für den Klassenchat zu einem der folgenden Dienste wechselt: Threema, Signal oder SIMSme.

Da leider immer noch eher wenige Nutzer bei bspw. Threema sind, empfehlen wir den Schülern eine Kombination aus kostenfreier und kostenpflichtiger App. Auf dem eigenen Smartphone, auf dem unzählige private Dateien (Fotos, Videos und Kontakte) und sensible Daten (Standortinformationen etc.) gespeichert sind, soll eine sichere, kostenpflichtige App installiert werden. Auf einem alten Gerät zuhause (altes Smartphone oder iPad), auf dem zuvor alle privaten Dateien gelöscht wurden, kann WhatsApp installiert werden. So kann nichts ausspioniert werden und die Schüler können, wann immer sie zuhause sind, mit ihren WhatsApp Kontakten weiterhin in Verbindung sein.

**2. Was einmal im Netz ist, bleibt im Netz**

Alle Fotos, Videos und sonstige Inhalte, die in sozialen Netzwerken hochgeladen werden, bleiben gespeichert, auch wenn sie vom Nutzer gelöscht werden. Oft tauchen sie sogar trotzdem weiterhin in Suchmaschinen auf. Man sollte sich genau überlegen, welche „lustigen“, oft peinlichen oder sogar intimen Fotos man mit anderen teilt.

**3. Nichts ist, wie es scheint:**Sprechen Sie mit Ihrem Kind über Fake-Accounts und böse Absichten mancher Menschen, die ihm im Internet begegnen können. Eine hohe Anzahl an Freunden und Followern zu haben wird weniger attraktiv, wenn man weiß, dass viele davon nicht „echt“ sind. Es sollten nur Freunde angenommen werden, die man persönlich kennt und das Profil von „öffentlich“ auf „privat“ gestellt werden. Bestärken Sie ihr Kind darin, soziale Kontakte vor allem persönlich zu pflegen anstatt nur digital.

## *Weiterführende Informationen:*

Noch mehr Informationen zum Thema finden Sie auf den umfangreichen Seiten:

http://www.klicksafe.de

http://www.mimikama.at

http://www.elternguide.online

http://www.handysektor.de

http://www.schau-hin.info