- ☑ Bevor du **Apps** installierst, lies dir genau durch, **welche Rechte** sie fordern! Hinter jeder App steckt ein Programmierer oder eine Firma. Viele Apps wollen deine kompletten persönlichen Daten abgreifen, deinen Standort, dein Surfverhalten oder die Daten all deiner Kontakte, die darüber sicherlich nicht begeistert wären. Vor allem bei **Apps die SMS verschicken oder telefonieren wollen**, ist größte Vorsicht angesagt – viele davon haben es auf dein Geld abgesehen!
- ☑ Beachte die **Nutzungsbedingungen:** Bei allen US-Onlinediensten wie **Facebook, Instagram, Snapchat, Skype, etc.** darf man sich erst **ab 13 Jahren** anmelden, bei **WhatsApp sogar erst ab 16**!
- ☑ Bitte deine Eltern, für dein Handy eine **Drittanbietersperre** einrichten zu lassen, das kostet nichts und hilft gegen Abofallen und andere Abzockmaschen.
- ☑ **Sei höflich beim Umgang mit dem Smartphone:** Eine anwesende Person hat immer Vorrang gegenüber dem Handy. Sie verdient Blickkontakt und volle Aufmerksamkeit.
- ☑ **Kommt es doch einmal zu einem Problem**, wende dich sofort an Personen deines Vertrauens: Deine Eltern, Freunde, Mitschüler, Vertrauenslehrer, die Schulsozialarbeit, etc. Abwarten verschlimmert das Problem fast immer!

Hinweise für Lehrkräfte

- ☑ **Gehen Sie nicht aktiv mit Freundschaftsanfragen auf SchülerInnen zu und behandeln Sie Anfragen einheitlich.**
- ☑ **AGB beachten!** Da man viele Apps laut deren Nutzungsbedingungen erst **ab 13 Jahren oder gar 16 Jahren** nutzen darf, sollte grundsätzlich keine Kommunikation mit jüngeren Schülern über diese Netzwerke stattfinden.
- ☑ Prüfen Sie sehr sorgfältig, welche **privaten Informationen** Sie mit Schülern teilen möchten und dürfen. Legen Sie gegebenenfalls ein **Zweitprofil** zur schulischen Nutzung an.
- ☑ Wenn möglich sind in Sozialen Netzwerken **Gruppen** persönlichen Kontakten vorzuziehen: Darin können Sie mit Schülern kommunizieren ohne mit ihnen direkt „befreundet“ zu sein.
- ☑ **Nutzen Sie kommerzielle Anbieter für schulische Zwecke nur, wenn alle Schüler sowie deren Eltern damit einverstanden sind** und verlangen Sie keinesfalls von Schülern, sich bei einem Sozialen Netzwerk anzumelden.
- ☑ **Soziale Netzwerke sind kein akzeptabler Weg zur Übermittlung datenschutz- und schulrechtlich relevanter Daten**.
- ☑ Für hessische Lehrkräfte gilt die Handreichung des Hessischen Kultusministeriums zu Sozialen Netzwerken: **https://t1p.de/hkm**

Günter Steppich
Gutenbergschule Wiesbaden
www.medien-sicher.de
Stand: Oktober 2021

www.medien-sicher.de

Leitlinien

für

Soziale Netzwerke und Messenger

Richtig umgehen mit

Instagram, WhatsApp, SnapChat & Co.

- ☑ Erstelle für **Apps und Websites eine zusätzliche Emailadresse, die nicht deinen Namen enthält**. Verwende nicht deine private oder berufliche Adresse, damit sie nicht bei Adresshändlern und Spamversendern landet. **Nutze möglichst nicht deine Handynummer zur Anmeldung, sie sollte unbedingt privat bleiben!**
- ☑ **Verwende nicht deinen vollen Namen,** wenn du dich bei einer App oder Website anmeldest, sondern einen Spitznamen (Nickname), der keine persönlichen Angaben enthält und auch nicht sexy klingt – so bist du für Fremde und Datensammler anonym und weckst nicht das Interesse von Pädophilen.
- ☑ Nutze **sichere Passwörter** und verrate sie auch besten Freunden, Geschwistern und Partnern nicht. Wenn dieses Wissen bei Streitigkeiten für gemeine Dinge ausgenutzt wird, kannst du nicht beweisen, dass dein Passwort missbraucht wurde. Passwort-Rezept: mindestens 10 Zeichen, Groß- und Kleinschreibung plus Zahlen oder ein langer Satz. Verwende nicht überall (Apps, E-Mail, Websites…) dasselbe Passwort. Wenn es ausspioniert wird, übernimmt der Täter dein Onlineleben!
- ☑ **Halte deine Geräte mit Updates aktuell** und informiere dich über **Virenschutz**. Gegen einen Trojaner nützt das beste Passwort nichts!
- ☑ **Verwende auf keinen Fall die Funktion „Freunde finden“** von Snapchat oder Facebook! Das wäre ein Verstoß gegen das deutsche Datenschutzgesetz, weil du dem Anbieter damit die Daten all deiner Kontakte auslieferst. Manchmal versteckt sich das hinter der Aufforderung, die Kontakte zu „synchronisieren“.
- ☑ **Privatsphäre-Einstellungen** müssen sehr sorgfältig gewählt werden, damit nicht Milliarden Menschen in dein Profil schauen können. Informiere dich im Netz über jede neue App und ihre Einstellungen.
- ☑ Stelle deine Profile bei TikTok, Instagram, etc. auf privat und die Sichtbarkeit der **Freundesliste** in Facebook auf „**Freunde**“ ein. Öffentliche Profile verraten viel mehr über dich als du ahnst und können für Abzocke, Erpressung und sexuelle Übergriffe missbraucht werden.
- ☑ **Wähle deine Kontakte sorgfältig und bewusst aus** – soll jeder auf deiner „Freundesliste“ wirklich all deine Posts, Kommentare, Likes, Fotos und Videos sehen können? **Nimm niemals Freundschaftsanfragen von Unbekannten an** und denke daran, dass böswillige Menschen sich auf Internetseiten und in Apps häufig mit falschem Namen und Alter anmelden.
- ☑ **Sei dir bei Posts und Kommentaren immer bewusst, wer das alles sehen kann!** Frage dich bei Fotos, wem du sie geben würdest, wenn es Papierfotos wären.
- ☑ **Profil- und Titelbilder** sind weltweit für jeden sichtbar, auch wenn dein Profil ansonsten privat eingestellt ist. Darauf solltest du nicht zu erkennen sein.
- ☑ **Private Dinge verrät man nicht jedem**, auch nicht im Internet. Teile persönliche Informationen nur mit echten Freunden und überlege genau, was du schreibst oder hochlädst und wer diese Inhalte sehen soll! Poste nur, was du wirklich jedem zeigen und in der Stadt aushängen würdest. **Wenn Freunde deine Fotos und Posts teilen, sind sie öffentlich und lassen sich nicht mehr zurückholen! Was auf einem Bildschirm erscheint, kann man speichern und weiterleiten, auch bei Snapchat!**
- ☑ **Beachte die Urheberrechte!** Wenn du online Bilder verwendest, die andere erstellt haben, z.B. Comics oder Fotos von Popstars, kann das teure Abmahnungen zur Folge haben.
- ☑ **Beachte das Recht am eigenen Bild!** Du darfst niemanden ungefragt fotografieren und schon gar nicht Bilder oder Videos von anderen ohne deren Einverständnis posten oder teilen. Das ist nicht legal, selbst in geschlossenen Gruppen und gut geschützten Profilen! Sind Kinder abgebildet, müssen deren Eltern zustimmen.
- ☑ **Laut den Nutzungsbedingungen erteilst du Snapchat, Instagram, Facebook und anderen Anbietern komplett und für immer alle Rechte an all deinen Inhalten**, die sie sogar weiterverkaufen dürfen. Überlege also sehr genau, was du dort einstellst!
- ☑ Pass auf, dass beim Posten vom Smartphone aus nicht dein **Standort** per GPS oder über das Mobilfunknetz mit veröffentlicht wird. Dein Aufenthaltsort ist ein wichtiger Teil deiner Privatsphäre und sollte nicht jedem zugänglich sein.
- ☑ **Äußere dich online nicht abfällig oder beleidigend über andere,** damit kannst du dich sogar strafbar machen. Kläre Meinungsverschiedenheiten immer im persönlichen Gespräch, niemals auf elektronischem Weg, denn dabei entstehen sehr leicht Missverständnisse, die das Problem noch verschlimmern. Man schreibt aus der Entfernung auch sehr leicht Dinge, die man niemandem offen ins Gesicht sagen würde.