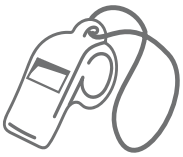

Handlungstipps

Wert von persönlichen und privaten Daten besprechen und klare Regeln vereinbaren

Erklären Sie Ihrem Kind den Wert von privaten Daten. Besprechen Sie gemeinsam, dass Daten auch missbraucht werden können, z. B. für unerwünschte Werbung und Spam, für Belästigung und Mobbing oder sogar Identitätsdiebstahl. Um Missbrauch zu vermeiden, können gemeinsame Regeln helfen, z. B. welche Daten geteilt werden oder welche Personen sie sehen dürfen. Machen Sie Ihrem Kind deutlich, dass es personenbezogene und persönliche Daten nicht ohne Rücksprache mit Ihnen herausgeben sollte.

Über AGB und Altersfreigaben von Social-Media-Angeboten informieren

Beim ersten Anmelden in Social-Media-Angeboten ist es wichtig, sich mit den Allgemeinen Geschäftsbedingungen (AGB) zu beschäftigen. Die wichtigsten Punkte sollten Sie mit Ihrem Kind besprechen. Erkundigen Sie sich z. B. vorab, ab welchem Alter das jeweilige Social-Media-Angebot genutzt werden darf. Viele Angebote geben ein Mindestalter vor. AGB sind jedoch in der Regel nicht sehr nutzerfreundlich aufbereitet – sehr lang, kompliziert geschrieben und schwer verständlich. In der **„Linkliste: Weiterführende Informationsangebote“** finden Sie für verschiedene Social-Media-Angebote die „Nutzungsbedingungen kurzgefasst“ von handysektor. Dort sind die wichtigsten Punkte übersichtlich aufbereitet. Die Betreiber können die AGB auch ändern. Daher kann es helfen, regelmäßig nachzusehen. Besprechen Sie mit Ihrem Kind, dass es Sie informiert, wenn der Anbieter auf AGB-Änderungen hinweist.

Möglichst wenig Daten preisgeben

Wer sich ein Profil in Social-Media-Angeboten anlegt, gibt in der Regel viele persönliche Daten an. Dabei ist es wichtig, nur die nötigsten Angaben zu machen. Angaben, die wirklich notwendig sind, sind mit einem „*“ gekennzeichnet. Vor allem persönliche Daten wie Nachname, Adresse, Geburtsdatum und Telefonnummer sollte man nur angeben, wenn sie für die Nutzung des Profils gebraucht werden. Auch der gewählte Nickname sollte keine Hinweise auf das Alter oder den Nachnamen enthalten.
Tipps, wie sich persönliche Daten verhüllen lassen, finden Sie im Bereich „Privatsphäre und Selbstdatenschutz“ in der **„Checkliste: Daten verbergen und schützen“**.

Alternative Angebote wählen

Fragt ein Angebot zu viele persönliche Daten ab, können Sie gemeinsam mit Ihrem Kind überlegen, ob es das Angebot wirklich nutzen muss. Manchmal finden sich zu bestimmten Angeboten auch datensparsame Alternativen. Ganz allgemein gilt bei der Preisgabe der eigenen Daten die Faustregel: Weniger ist mehr. Daten, die nicht online stehen, können nicht so leicht missbraucht werden.

Zugriffsrechte von Apps beschränken

Bei der Installation und, je nach Betriebssystem, auch danach können Sie die Zugriffsrechte von Apps einschränken, z. B. das Taggen von Fotos mit GPS-Daten. Generell ist es sinnvoll, vor der Installation zu prüfen, auf welche Daten eine App zugreift und ob sie diese Zugriffsrechte wirklich benötigt. Falls eine App zu viele Zugriffsrechte fordert, können Sie überlegen, ob die App wirklich genutzt werden soll.

Privatsphäre-Einstellungen von Angeboten nutzen und regelmäßig überprüfen

Die meisten Social-Media-Angebote haben eigene Privatsphäre-Einstellungen. Z. B. kann man seine Daten vor der Öffentlichkeit verbergen und nur für ausgewählte Personen (den „Freunden“) sichtbar machen. Diese Einstellungen können bei der Weiterentwicklung eines Angebotes aber verändert werden, ohne dass die Nutzerinnen bzw. Nutzer informiert oder um ihre Einwilligung gebeten werden. Daher ist es wichtig, die Einstellungen regelmäßig zu überprüfen und bei Bedarf neu anzupassen. Privatsphäre-Einstellungen bieten zwar keinen 100-prozentigen Schutz vor Datenmissbrauch, doch das Risiko wird eingedämmt. Die Privatsphäre-Leitfäden von **saferinternet.at** u. a. für Snapchat, TikTok oder Instagram zeigen in Schritt-für-Schritt-Anleitungen, wie Sie mögliche Sicherheitseinstellungen vornehmen können.

Datenmissbrauch melden

Sind Sie oder Ihr Kind einem Datenmissbrauch zum Opfer gefallen, können Sie das beim jeweiligen Anbieter melden und dagegen vorgehen. Dafür sollten Sie Beweise sichern, z. B. mittels eines Screenshots. Bei Datenmissbrauch können Sie sich z. B. an die **Verbraucherzentrale** wenden. In schweren Fällen wie Identitätsdiebstal sollte Anzeige bei der **Polizei** gestellt werden.