

DAS KÖNNEN SIE TUN PERSÖNLICHER DATENSCHUTZ

1. DAS PASSWORT

Wählen Sie eine ausreichende Länge:

- Das Passwort sollte mind. 12-16 Zeichen lang sein.

Nutzen Sie verschiedene Zeichenarten:

- Kombinieren Sie Groß- und Kleinbuchstaben,
- Zahlen und Sonderzeichen (z. B. ? ! & % \$).

Vermeide einfache oder persönliche Wörter:

- Nutzen Sie keine leicht zu erratenden Begriffe wie Ihre Namen,
- Ihr Geburtsdatum oder einfache Passwörter wie „Passwort123“.

Machen Sie jedes Passwort einzigartig:

- Verwenden Sie für jedes Konto ein eigenes Passwort,
- damit nicht mehrere Accounts gleichzeitig gefährdet sind.



2. EINSTELLUNGEN PRÜFEN!

Schaun Sie regelmäßig in die Einstellungen der Apps und Konten:

- Stellen Sie die Profile auf privat
- Prüfen Sie, wer die Inhalte sehen kann
- Deaktivieren Sie unnötige Berechtigungen (z. B. Standort, Kontakte)
- Aktivieren Sie Sicherheitsfunktionen (z. B. Zwei-Faktor-Anmeldung)



**DATENSCHUTZ
BEI ANDROID**



**DATENSCHUTZ
BEI APPLE**



APPS MIT ERHÖHTEM DATENSCHUTZ-RISIKO

SOCIAL MEDIA

- TikTok
- Instagram
- Snapchat



Risiken:

- Zugriff auf Kamera, Mikrofon, Standort
- Öffentliche Profile & Fremde können Inhalte sehen
- Daten werden für Werbung genutzt

Wichtig:

- Profil auf privat stellen
- Standort ausschalten
- Kontakte & Kamera nur bei Bedarf erlauben

MESSENGER

- WhatsApp
- Discord
- Telegram



Risiken:

- Zugriff auf Kontakte
- Fremde können Nachrichten senden
- Gruppen & Server können unsicher sein

Wichtig:

- Nur bekannte Kontakte zulassen
- Privatsphäre-Einstellungen prüfen
- Keine sensiblen Daten teilen

VIDEO & STREAMING

- YouTube
- Twitch



Risiken:

- Tracking des Nutzungsverhaltens
- Kommentare & Kontakt mit Fremden

Wichtig:

- Verlauf & Empfehlungen prüfen
- Kommentare einschränken

SPIELE & GAMING-PLATTFORMEN

- Roblox
- Fortnite
- Minecraft

Risiken:

- Chats mit Fremden
- In-Game-Käufe
- Verknüpfung mit anderen Accounts

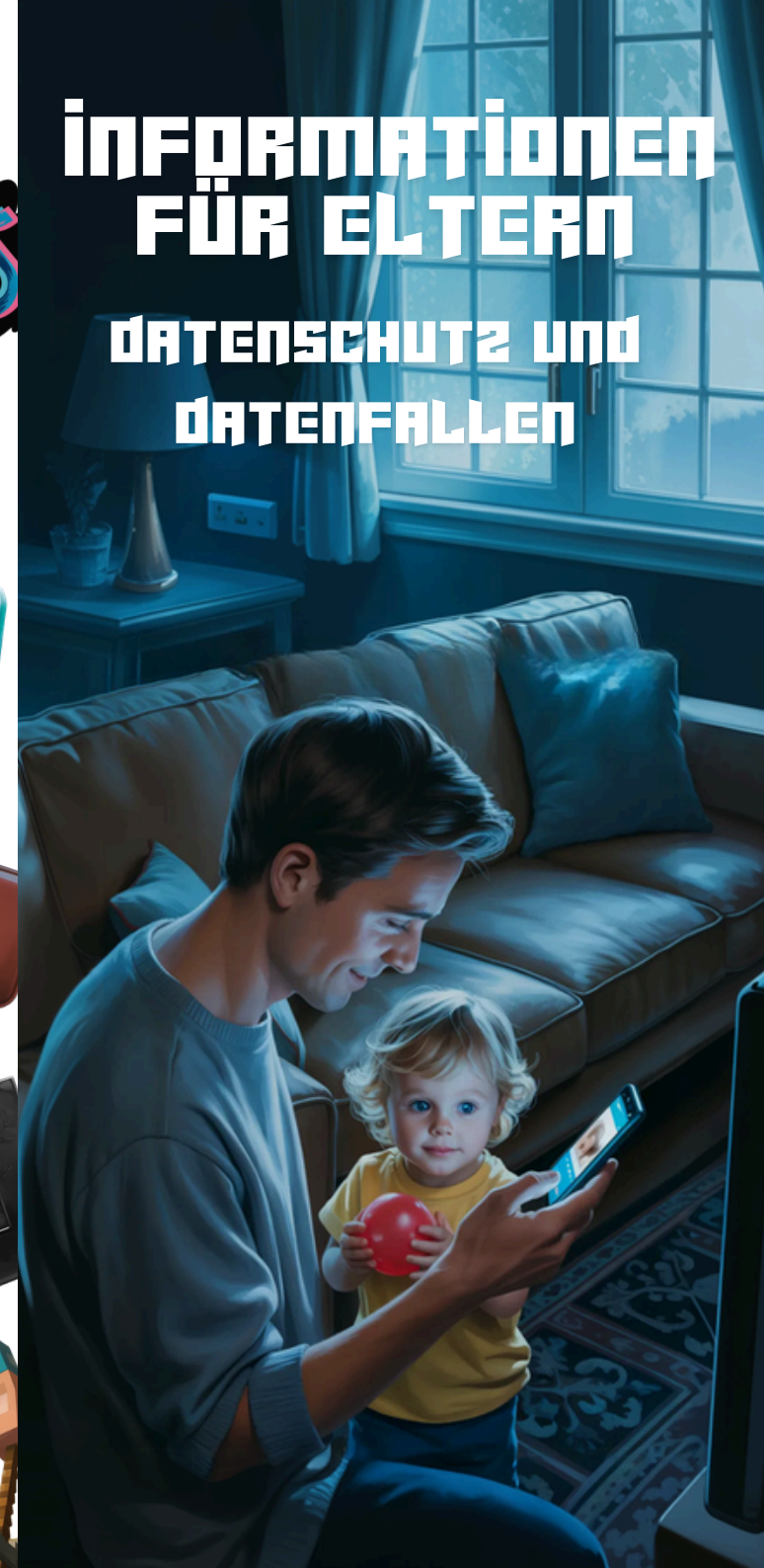
Wichtig:

- Chat einschränken
- Käufe absichern (z. B. PIN)
- Freundeslisten kontrollieren



INFORMATIONEN FÜR ELTERN

DATENSCHUTZ UND DATENFALLEN



DATENSCHUTZ

WICHTIGE FAKTEN ZUM DATENSCHUTZ:

Datenschutz bedeutet, dass persönlichen Daten geschützt werden. Dazu gehören zum Beispiel Name, Adresse, Fotos oder Nachrichten.

Wichtig:

Sie sollten selbst entscheiden können:

- Wer Ihre Daten sieht.
- Was mit Ihren Daten passiert.

WARUM IST DAS WICHTIG?

Ohne Datenschutz können:

- Fremde Daten sehen oder missbrauchen
- Dritte herausfinden, wo man sich aufhält oder was man gerade oder routinemäßig macht
- Daten für Werbung oder Betrug genutzt werden

WAS SIND PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte Person beziehen oder sie identifizierbar machen. Dazu gehören zum Beispiel:

- Name (Vor- und Nachname)
- Geburtsdatum
- Adresse / Wohnort
- Telefonnummer
- E-Mail-Adresse
- Geburtsort
- Bankkontonummer / IBAN
- Kreditkartendaten
- Politische Meinungen
- Sexuelle Orientierung

DATENSCHUTZ- FALLEN & GESETZE



DIE WICHTIGSTEN REGELN FÜR ELTERN

1. So wenig Daten wie möglich teilen

Geben Sie nur die Daten preis, die wirklich notwendig sind. Auch scheinbar harmlose Informationen können zusammen ein vollständiges Profil ergeben.

2. Keine sensiblen Daten veröffentlichen

Vermeiden Sie die Weitergabe von:

- Adresse
- Schule
- Standort
- Telefonnummer
- persönlichen Gewohnheiten

3. Vorsicht bei Fotos und Videos

Überlegen Sie vor jedem Post:

- Ist das Bild privat oder könnte es später unangenehm sein?
- Würde mein Kind dem zustimmen?

Einmal im Internet = schwer kontrollierbar

4. Privatsphäre-Einstellungen nutzen

Achten Sie darauf:

- Profile auf „privat“ stellen
- Standortfreigaben deaktivieren
- App-Berechtigungen prüfen

5. Mit dem Kind sprechen – nicht nur kontrollieren

Sprechen Sie regelmäßig über:

- Erlebnisse im Internet
- Risiken
- eigene Entscheidungen

Vertrauen ist der wichtigste Schutz

6. Fehler zulassen und begleiten

Reagieren Sie ruhig, wenn etwas passiert.

Vorwürfe führen dazu, dass Kinder Probleme verheimlichen.

7. Klare, faire Regeln vereinbaren

Regeln sollten:

- verständlich sein
- gemeinsam festgelegt werden
- im Alltag umsetzbar sein



8. Altersfreigaben ernst nehmen

Plattformen und Spiele haben Altersgrenzen aus gutem Grund. Diese bieten Orientierung und Schutz.

- Instagram → ab 13
- TikTok → ab 13
- Snapchat → ab 13 (mit Zustimmung)
- WhatsApp → ab 13
- Spotify → ab 16 (mit Zustimmung)
- YouTube → Nutzung unter 18 nur mit Zustimmung
- Netflix → Nutzung unter 18 nur unter Aufsicht

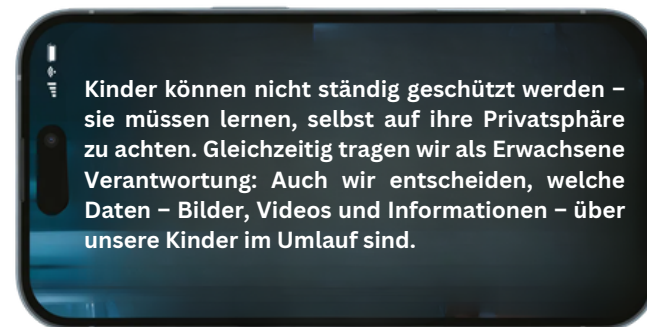
9. Vorbild sein

Kinder orientieren sich am Verhalten der Eltern. Gehen Sie selbst bewusst mit Daten um.

10. Bewusst entscheiden statt automatisch handeln

Stellen Sie sich immer die Frage:

„Muss ich diese Information wirklich teilen?“



WO FINDEN SIE HILFE?

AUCH FRAU PLÄTTNER HILFT IHNEN

ANJA PLÄTTNER

Schulsozialarbeiterin am
Gustav-Hertz-Gymnasium

Zimmer X-37
(Gang - hinterm
Sekretariat)

0163- 741 72 98 (SMS, Signal)

sozialarbeit@ghg-leipzig.lernsax.de



SELBSTTEST

