

DAS KÖNNEN SIE TUN PERSÖNLICHER DATENSCHUTZ

1. DAS PASSWORT

1. Passwort muss lang sein

Das Passwort sollte 12 bis 16 Zeichen haben.
Je länger das Passwort ist, desto sicherer ist es.

2. Verschiedene Zeichen benutzen

Mischen Sie:

- große Buchstaben (A, B, C)
- kleine Buchstaben (a, b, c)
- Zahlen (1, 2, 3)
- Sonderzeichen wie: ? ! & % \$

3. Keine einfachen Wörter nutzen

Verwenden Sie keine:

- Namen
- Geburtsdaten
- einfachen Wörter wie „Passwort123“

Diese sind leicht zu erraten.

4. Für jedes Konto ein eigenes Passwort

Nutzen Sie für jedes Konto ein anderes Passwort.
Wenn ein Passwort gestohlen wird, sind sonst alle
Konten gefährdet.

2. EINSTELLUNGEN PRÜFEN!

1. Profil auf privat stellen

Nur bekannte Personen können Inhalte sehen.

2. Sichtbarkeit prüfen

Kontrollieren Sie:

Wer kann Fotos, Videos und Beiträge sehen?

3. Berechtigungen einschränken

Schalten Sie unnötige Zugriffe aus, zum
Beispiel:

- Standort
- Kontakte

4. Sicherheitsfunktionen aktivieren

Nutzen Sie zusätzliche Sicherheit, zum Beispiel:

- Zwei-Faktor-Anmeldung (Bestätigung per
Code)



ZUM PASSWORT-



CHECK



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:

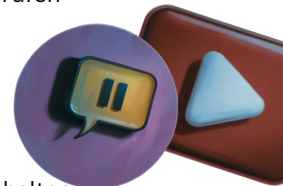
- Zugriff auf Kontakte
- Fremde können Nachrichten senden
- Gruppen & Server können unsicher sein

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

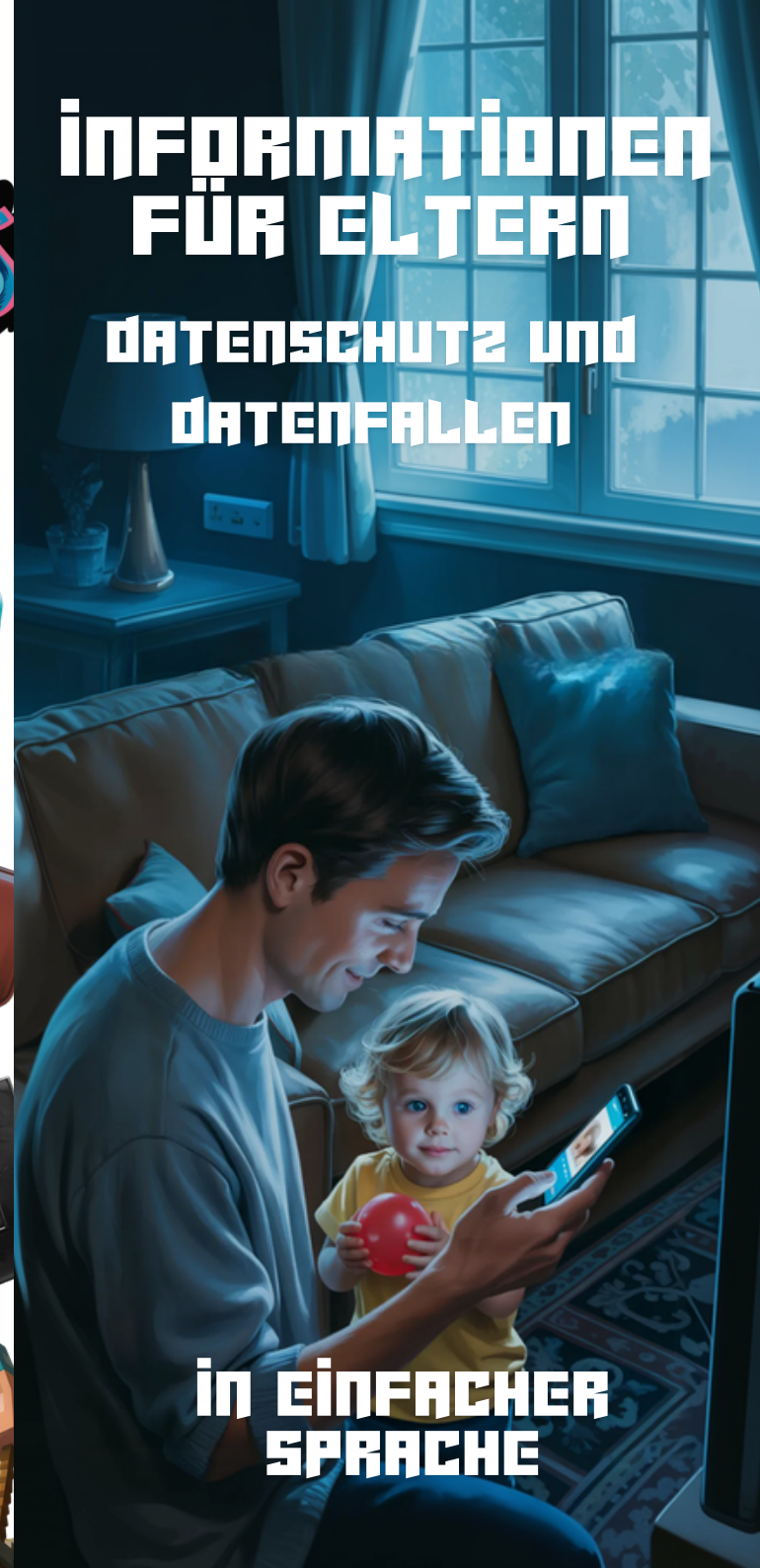
Wichtig:

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

INFORMATIONEN FÜR ELTERN

DATENSCHUTZ UND DATENFALLEN

IN EINFACHER SPRACHE



DATENSCHUTZ

WICHTIGE FAKTEN ZUM DATENSCHUTZ:

Datenschutz bedeutet:

Persönliche Daten werden geschützt.

Das sind persönliche Daten:

- Name
 - Adresse
 - Fotos
 - Nachrichten
- Wichtig**
Sie sollen selbst entscheiden können:
- Wer Ihre Daten sehen darf
 - Was mit Ihren Daten passiert

WARUM IST DAS WICHTIG?

- Fremde können Ihre Daten sehen oder missbrauchen
- Andere können herausfinden, wo Sie sind oder was Sie regelmäßig machen
- Daten können für Werbung oder Betrug genutzt werden

WAS SIND PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind Informationen, die zu einer bestimmten Person gehören oder mit denen man eine Person erkennen kann.

- 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 weiter, die wirklich nötig sind. Auch kleine Informationen können zusammen viele Daten ergeben.

2. Keine sensiblen Daten teilen

Teilen Sie keine wichtigen Daten, zum Beispiel:

- Adresse
- Schule
- Standort
- Telefonnummer
- persönlichen Gewohnheiten

3. Vorsicht bei Fotos und Videos

Überlegen Sie vor dem Posten:

- Ist das Bild privat?
- Könnte es später unangenehm sein?
- Würde mein Kind zustimmen?

Wichtig:

Einmal im Internet = schwer zu kontrollieren

4. Einstellungen nutzen

Achten Sie auf:

- Profil auf „privat“ stellen
- Standort ausschalten
- App-Berechtigungen prüfen

5. Mit dem Kind sprechen

Sprechen Sie regelmäßig über:

- Erlebnisse im Internet
- mögliche Risiken
- Entscheidungen

Vertrauen ist sehr wichtig.

6. Ruhig bleiben bei Fehlern

Wenn etwas passiert:

- ruhig reagieren
- keine Vorwürfe machen

Sonst erzählt das Kind vielleicht nichts mehr.

7. Klare Regeln vereinbaren

Regeln sollen:

- einfach zu verstehen sein
- gemeinsam festgelegt werden
- im Alltag funktionieren

SELBSTTEST



8. Altersfreigaben beachten

Viele Apps und Spiele haben Altersgrenzen. Diese sind wichtig und schützen Kinder.

Beispiele:

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

9. Vorbild sein

Kinder lernen von den Eltern.

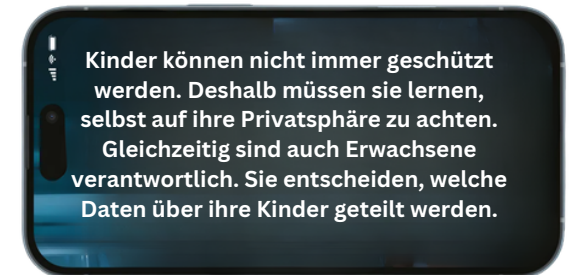
Gehen Sie selbst vorsichtig mit Daten um.

10. Bewusst entscheiden

Denken Sie kurz nach, bevor Sie etwas teilen.

Fragen Sie sich:

„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

