„Wer ‚digital' sagt, muss das auch analog begründen können."

– padeluun

digitalcourage

Kommunikation (mit Schüler.innen)

- **Kommunikation über Messenger und Soziale Netzwerke** ist private Kommunikation. Der Austausch von Informationen, die einen expliziten Bildungs- oder Erziehungsauftrag erfüllen (z.B. Hausaufgaben), liegt in einem rechtlichen Graubereich. Trennen Sie grundsätzlich private und berufliche Kommunikation!
- **Personenbezogene Schüler.innendaten** müssen immer nach geltendem Recht geschützt werden. Dieser Schutz ist bei Anbietern wie WhatsApp, Facebook & Co. nicht gegeben, da Daten an Dritte weitergegeben werden. Außereuropäische Anbieter unterliegen zudem nicht ausreichenden Datenschutzbestimmungen.
- **Extremfall „WhatsApp":** Bei der Nutzung des Messengers werden enorm viele Daten verarbeitet. Zudem werden alle im Telefon gespeicherten Kontakte an den Anbieter übertragen, unabhängig davon, ob die Kontakte selbst WhatsApp nutzen oder nicht. Jede.r App-Nutzer.in ist für die Übermittlung der personenbezogenen Daten datenschutzrechtlich verantwortlich und benötigt zuvor eine Erlaubnis zur Datenverarbeitung von jeder Person im Adressbuch. Wir raten ausdrücklich vom Gebrauch der App ab!
- Sprechen Sie sich laut gegen die Nutzung von WhatsApp und ähnlichen Diensten aus! Informieren Sie sich und andere über legale Kommunikationswege.

Hilfreiche Tipps ...

Unsere AG „Digitale Selbstverteidigung" beschäftigt sich mit Anleitungen zur Selbsthilfe zum Schutz Ihrer Privatsphäre. Wir zeigen Ihnen Alternativen zu verschiedenen Diensten, die Vorteile freier Software und wie die Verschlüsselung von E-Mails funktioniert.
digitalcourage.de/digitale-selbstverteidigung

Diese Arbeit aktuell zu halten, ist sehr mühsam. Unterstützen Sie unsere Arbeit mit einer Spende:
digitalcourage.de/spende

Kommunikation (mit Eltern & Kolleg.innen)

- **E-Mail:** Die beste Möglichkeit, private und berufliche Kommunikation zu trennen, sind dienstliche Mailadressen. Diese sollten von den Schulen zur Verfügung gestellt werden. Wenn keine schulinterne Lösung vorliegt, raten wir zu datenschutzfreundlichen Anbietern wie Posteo.de oder Mailbox.org.
- **Verschlüsselung:** Verschlüsseln Sie Ihre E-Mails. Informieren Sie sich und andere darüber, wie Sie die Inhalte Ihrer E-Mails schützen können.

„Keine Ausstattung ohne pädagogisches Konzept."

(Bundesministerium für Bildung und Forschung)

Die Digitalisierung von Schulen bedeutet nicht, dass analoges durch digitales Lernen abgelöst werden soll – im Vordergrund stehen Vernetzung und Kommunikation. Bei jeglichem Einsatz digitaler Medien ist jedoch zwingend der Schutz sensibler Schüler.innendaten mitzudenken.

Zu den wichtigsten inhaltlichen Medienkompetenzen, die Kindern und Jugendlichen vermittelt werden müssen, gehören der Schutz der Privatsphäre und personenbeziehbarer Daten. Wer im Web „surft", digital mit anderen kommuniziert oder mobile Endgeräte nutzt, hinterlässt nicht rückholbare Datenspuren, aus denen sich Nutzungs- und Kommunikationsprofile erstellen lassen. Kinder müssen von klein auf lernen, sich zu schützen!

- Für den Unterricht empfehlen wir unser Buch: „#Kids #digital #genial – Das Lexikon von App bis .zip":
shop.digitalcourage.de/kids-digital-genial
- Weitere Tipps für Lehrkräfte:
kidsdigitalgenial.de/unterricht
- Weitere Informationen:
digitalcourage.de/kinder-und-jugendliche

Digitalcourage wirkt. Wirken Sie mit!

- Sprechen Sie mit anderen über Datenschutz und Grundrechte.
- Lernen Sie digitale Selbstverteidigung. Bleiben Sie wachsam.
- Bestellen Sie unseren Newsletter. Verteilen Sie Infomaterial.
- Organisieren Sie Infostände und Aktionen in Ihrer Stadt.
- Sprechen Sie mit Ihren Bundestagsabgeordneten.
- Engagieren Sie sich in einer unserer AGs.
- Unterstützen Sie unsere Arbeit mit Geldspenden.
- Geben Sie uns Ihr Mandat: werden Sie Fördermitglied.

Wir mischen uns ein – mit charmanten und wirksamen Aktionen.

(Foto: photocube · Verena Hornung)

Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Telefon: 0521 1639 1639
Telefax: 0521 61172
Web: digitalcourage.de
bigbrotherawards.de

Mail: mail@digitalcourage.de
PGP: 0x2DC2A7D0
Fediverse: @digitalcourage@digital-courage.social
Twitter: @digitalcourage

Spendenkonto:
IBAN: DE69 3702 0500 5459 5459 20 · BIC: BFSWDE33XXX · Sozialbank
oder online unter: digitalcourage.de/spende

Unsere Arbeit wird durch Mitgliedsbeiträge und Spenden finanziert.
Wirken Sie mit – damit wir gemeinsam etwas bewirken können.

Wir sind Mitglied bei:
Initiative Transparente Zivilgesellschaft

Wir danken:
stiftung bridge – Bürgerrechte in der digitalen Gesellschaft

Text: Jessica Wawrzyniak
Gestaltung: Jens Reimerdes
Bilder: Cover: Imgorthand · Getty Images

Flyer Datenschutz an Schulen v1.2 – 12.2019

Digitalisierung oder „Kreidezeit"?

Datenschutz an Schulen

Dieses Faltblatt gibt Tipps, wie sensible Daten von Schüler.innen besser geschützt werden können.

digitalcourage

Digitalisierung an Schulen

Schulbildung ist Ländersache. Schön ist: Durch die Änderung eines Gesetzes (Art. 104c GG) ist es Schulen nun bis 2023 möglich, staatliche Unterstützung im Rahmen des „DigitalPakts Schule“ zu erhalten. Der Bund stellt etwa 5 Milliarden Euro für den Aufbau digitaler Infrastrukturen zur Verfügung (≈ 500 Euro pro Schüler.in). Klar ist: Die Förderung reicht leider höchstens als Anschubfinazierung.

- Das Geld darf für technische Infrastruktur (z.B. WLAN im Gebäude) und für Supportstrukturen (z.B. Systemadministration und Wartung) eingesetzt werden. Für mobile Endgeräte sind max. 20% des Fördertopfs vorgesehen und an die Bedingung geknüpft, dass eine entsprechende IT-Infrastruktur bereits gegeben ist.

- Gefördert wird nur, wenn ein Medienkonzept vorliegt, das klare, langfristige, pädagogische und strukturelle Ziele zur Umsetzung digitaler Bildung formuliert. In dieses Konzept gehören auch Maßnahmen zu Datenschutz und Datensicherheit.

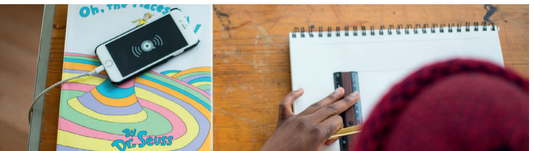
- Lehrerinnen und Lehrer sollen sich auf die Vermittlung inhaltlicher Kompetenzen konzentrieren – wie in ihrer Berufsausbildung vorgesehen – und nicht in Doppelfunktion als IT-Expert.innen fungieren.

Länderspezifische Infos:
bfb.org/digitalpakt

Unser Tipp:

Nutzen Sie die Förderung, um in Wartung und Beratung durch Administrator.innen zu investieren. Diese können Grundbausteine legen, die den technischen Datenschutz an Ihrer Schule langfristig verbessern.

(Foto: StockSnap via Pixabay)



Digitale Verwaltung & Schulclouds

- **Cloudbasierte Lösungen zum Verwalten von Schülerdaten sind nicht immer sinnvoll.** Prüfen Sie, welchen Nutzen Sie durch digitale Klassenbücher und ähnliche Dienste erlangen und ob Sie verschiedene Aspekte in Bezug auf die Sicherheit der Daten erfüllen können.

- **Nutzen Sie keine Cloudlösungen kommerzieller Anbieter.** Großkonzerne wie Microsoft, Google und Apple haben ein wirtschaftliches Interesse daran, ihren Datenpool um Schülerdaten zu erweitern. Besonders „Office 365“ ist wegen des mangelnden Datenschutzes teilweise bereits als unzulässig für Schulen erklärt worden. Wir raten: Verzichten Sie auch auf Dienste wie GoogleDocs oder Dropbox.

- **Speichern Sie die Daten in kommunalen Rechenzentren.** Die Nutzung von dezentralen Schulclouds ermöglicht, dass nicht jede Schule ihr eigenes Süppchen kochen muss, doch alle Daten zentral in die Hände eines Unternehmens zu legen, wäre aus Datenschutzgründen unverantwortlich. Wir empfehlen, kommunal verwaltete Server zu nutzen.

- **Stellen Sie genügend Schularbeitsrechner zur Verfügung.** Werden die Plattformen von privaten Geräten genutzt, müssen Lehrkräfte eine Erklärung abgeben, in der sie verschiedene Maßnahmen zum Schutz sensibler Daten garantieren. Das finden wir unverantwortlich! Diese Maßnahmen am heimischen Rechner einzuhalten, mag im Einzelfall gelingen, ist aber in der Masse unmöglich. Prüfen Sie erneut den Nutzen der Plattform, wenn auf den Einsatz privater Geräte verzichtet wird.

- **Verwaltungs-Apps:** Lehrkräfte greifen bei der Verwaltung von Noten und Unterricht oft zu Apps, die im PlayStore empfohlen werden. Auch hier müssen Sie die Vorschriften zur Einhaltung des Datenschutzes beachten. Wir raten dringend dazu, solchen Apps zu misstrauen, bis ihre Unbedenklichkeit garantiert werden kann. Sprechen Sie die Nutzung von guten Apps mit der Schulleitung ab, um sie ggf. in den Gesamtkontext des Medienkonzepts zu integrieren.

„Kinder und Jugendliche sind oft Profis an ihren Geräten. Doch in Bezug auf Datenschutz und die Tragweite ihres Handelns brauchen sie Unterstützung.“

Jessica Wawrzyniak, Medienpädagogin bei Digitalcourage

(Foto: William Iven via Pixabay)

Digitale Lernplattformen & Apps

- **Lernplattformen:** Bei Angeboten zur Verbreitung von Lernmaterialien, Hausaufgaben etc. ist zu prüfen, welche Daten erfasst werden und wo diese gespeichert werden. Seien Sie besonders wachsam bei cloudbasierten Lösungen und der Einbindung von Dritten (z.B. durch Werkzeuge wie Google Analytics).

- **Apps zur Lernförderung:** Besonderes Augenmerk gilt den Allgemeinen Geschäftsbedingungen: Wer stellt die App zur Verfügung? Wo werden die Daten gespeichert? Welche Zugriffsberechtigungen werden erteilt?

- **Digitale Werkzeuge:** Tools zur Erstellung von Mindmaps, Präsentationen und anderer Inhalte sind ebenfalls aus datenschutzrechtlicher Perspektive zu betrachten. Nicht jedes Werkzeug ist gut, nur weil es digital ist! Prüfen Sie jeweils den Mehrwert gegenüber analogen Varianten.

Die richtige Hardware & Software

- Verzichten Sie auf Hard- & Software-Angebote von Google/Android, Microsoft und Apple. Hier stehen wirtschaftliche Interessen und Machtspiele an erster Stelle, nicht Bildung und Datenschutz. Auch für mobile Endgeräte gibt es Alternativen.

- Überlegen Sie die Wahl des Anbieters vorher gut! Sie begeben sich ggf. in eine Lock-in-Situation (Kunden-/Produktbindung), welche den Wechsel zu anderen Anbietern erschwert (z.B. durch zeitlichen und finanziellen Aufwand).

- Windows-Rechner sind häufiger von Fremdzugriffen betroffen als andere. Linux (freies Betriebssystem) ist eine bessere Alternative.

- Wählen Sie freie Software als Arbeitswerkzeuge: Z.B. LibreOffice statt Microsoft Office, Thunderbird statt Outlook.

- Browser: Installieren Sie Firefox statt des Internet Explorers, deaktivieren Sie mögliche Tracking-Funktionen und integrieren Sie Werbeblocker.

Brauchen Sie Hilfe? Dann informieren Sie sich auf unserer Webseite oder besuchen Sie eine Crypto- oder Linux-Install-Party:

digitalcourage.de/digitale-selbstverteidigung
cryptoparty.in

Gesetzliche Vorgaben

Regelungen zum Schutz von Schüler.innendaten finden sich unter anderem in der EU-DSGVO, in den Schulgesetzen und in entsprechenden Anlagen.

Eine Übersicht:
schulsekretaerinnen.net/schulgesetze-daten-schutzverordnungen/

Ja, ich unterstütze ▶ digitalcourage!

Vorname: _____ Name: _____

Straße / Postfach: _____

Postleitzahl: _____ Ort: _____

E-Mail (für den Digitalcourage-Newsletter): _____

Ja, ich möchte Fördermitglied von Digitalcourage e.V. werden.
Mein Monatsbeitrag soll sein:
☐ Ermäßigter Beitrag (zur Zeit 2,50 Euro monatlich)
☐ **Normaler Beitrag** (zur Zeit 10 Euro monatlich)
☐ Soli-Beitrag (zur Zeit 20 Euro monatlich)
☐ Eigener Soli-Beitrag: _____

IBAN oder Kontonr.: _____

BIC oder BLZ: _____ Bank: _____

Hiermit ermächtige ich Digitalcourage e.V., die Zahlungen von meinem Konto mittels Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von Digitalcourage e.V. auf mein Konto gezogenen Lastschriften einzulösen. Die Lastschriften sind mit der Gläubiger-ID DE07ZZZ00000323047 gekennzeichnet. Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen. Der Einzug einer einmaligen Spende sowie ggf. die erstmalige Zahlung bei wiederkehrenden Spenden und Beiträgen erfolgt zum nächstmöglichen Zeitpunkt. Künftige Zahlungseinzüge erfolgen dann immer am gleichen Kalendertag.

Ort, Datum: _____ Unterschrift: _____

Digitalcourage e.V. ist gemeinnützig. Spenden und Mitgliedsbeiträge können beim Finanzamt geltend gemacht werden. Zum Beginn des nächsten Jahres versenden wir eine Bescheinigung

Bitte Formular als Brief schicken an:
Digitalcourage e.V., Marktstraße 18. 33602 Bielefeld

Oder einfach online Fördermitglied werden:
digitalcourage.de/mitglied