

RATGEBER - TIPPS UND TOOLS

IM DIGITALEN ZEITALTER

EIN VORBILD SEIN

FÜR LEHRKRÄFTE



BEE
SECURE

INHALTSVERZEICHNIS

EINLEITUNG	3
1. VERHALTENSREGELN IM SCHULISCHEN KONTEXT	4
1.1 Das Recht am eigenen Bild: das Verbreiten von Bildern der Schüler	4
1.2 DSGVO: Speichern und Teilen von Daten oder Fotos	6
1.3 Benutzung von Werken Dritter: Urheberrecht (Copyright ©)	8
1.4 Regeln für die Nutzung von Bildschirmen durch Kinder: sicheres Lernen	10
2. EINRICHTUNG UND SCHUTZ DER GERÄTE	12
2.1 Elektronische Geräte sichern	12
2.2 Vertraulichkeit und Schutz der Privatsphäre	16
3. NUTZUNG DER SOZIALEN NETZWERKE	19
3.1 Die eigene Darstellung im Internet	19
3.2 Die Klasse in den sozialen Netzwerken	21
3.3 Gefahren: Hacking und Identitätsdiebstahl	22
4. VORBEUGUNG UND VORGEHEN	24
4.1 Vorbeugung	24
4.2 Vorgehen bei Zwischenfällen	26
4.3 Die Grenzen Ihrer Verantwortung	31
BIBLIOGRAFIE	34

Um die Lesbarkeit dieser Publikation zu erleichtern, wurde die männliche Form als neutrales Geschlecht verwendet, um die gesamte Bevölkerung zu bezeichnen.



EINLEITUNG

Im digitalen Zeitalter nehmen vernetzte Technologien einen zentralen Platz im Alltag der Schüler sowie dem Lehrpersonal ein. Diese Tools bieten immense pädagogische Möglichkeiten, werfen aber auch neue ethische und rechtliche Fragen auf und stellen die Pädagogik vor neue Anforderungen. In einem Umfeld, in dem die Grenzen zwischen Privat- und Berufsleben verschwimmen, ist es für Lehrpersonen unerlässlich, bewährte Praktiken zu kennen, um die Sicherheit, den Schutz und das Wohlergehen aller Akteure der Schulgemeinschaft zu gewährleisten.

Dieser Ratgeber wurde als praktisches und konkretes Hilfsmittel konzipiert, um Lehrkräfte in ihrer Vorbildfunktion im digitalen Zeitalter zu unterstützen. Er enthält Tipps, rechtliche Hinweise und Empfehlungen aus offiziellen Quellen, um einen verantwortungsvollen und sicheren Umgang mit digitalen Tools – sowohl im privaten als auch im beruflichen Bereich – zu unterstützen. Ziel ist, den Lehrkräften dabei zu helfen, präventives Verhalten zu entwickeln, und zu vermitteln, wie sie mit problematischen Situationen umgehen können.

Im ersten Kapitel geht es um die im schulischen Kontext zu beachtenden Verhaltensregeln, anschließend wird die Konfiguration und Sicherung digitaler Tools besprochen. Die Nutzung sozialer Netzwerke ist Thema des dritten Kapitels, während sich der vierte Teil der Prävention und dem Umgang mit Störfällen widmet, konkrete Hilfestellungen bietet und nützliche Quellen angibt. Ergänzt wird der Ratgeber durch kleine Memos für Lehrkräfte (Post-its), eine Checkliste für die Nutzung sozialer Netzwerke und Anhänge, beispielsweise eine Vorlage für einen Verhaltenskodex.

Der Ratgeber und die dazugehörigen Tools sollen Lehrkräfte bei ihrer pädagogischen Arbeit unterstützen und einen bewussten, sicheren und verantwortungsvollen Umgang mit digitalen Medien in der Schule fördern.

1. VERHALTENSGESETZEN IM SCHULISCHEN KONTEXT



Digitale Geräte gehören sowohl für Lehrkräfte als auch für Schüler zum Alltag. Um die Integrität und das Wohlergehen aller zu gewährleisten, ist es wichtig, bestimmte Verhaltensregeln zu kennen und einzuhalten.

1.1 Das Recht am eigenen Bild: das Verbreiten von Bildern der Schüler

Im schulischen Kontext

Fotos und Videoaufnahmen haben durchaus ihren Platz im schulischen Alltag, z. B. als Erinnerung an Besichtigungen oder zur Dokumentation bei Projekten. Gleichzeitig hat jede Person das Recht, sich der Aufnahme und Veröffentlichung ihres Bildes zu widersetzen. Dies gilt auch für Kinder. Lehrkräfte müssen also ein ausgewogenes Verhältnis zwischen Dokumentation und Achtung des Rechts am eigenen Bild bzw. Schutz der Privatsphäre der Schüler finden.



Aus rechtlicher Sicht

Das Recht am eigenen Bild gründet auf verschiedenen Gesetzen zum **Schutz der Privatsphäre**¹ (S.35), auf europäischer und nationaler Ebene. Es ist laut Gesetz vom 11. August 1982 über den Schutz der Privatsphäre verboten, mit einem beliebigen Apparat von einer Person, die sich an einem nicht öffentlich zugänglichen Ort befindet, ohne deren Zustimmung Aufnahmen zu machen. Eine Zustimmung kann jederzeit widerrufen werden. Verstöße gegen diese Bestimmungen können strafrechtlich und zivilrechtlich verfolgt werden.



WICHTIG

Sich fotografieren zu lassen bedeutet nicht, dass man der Veröffentlichung des Fotos zustimmt!

Die **Einwilligung Minderjähriger** in Bezug auf das Recht am eigenen Bild wirft mehrere rechtliche und ethische Fragen auf. Kinder können vor Vollendung des 18. Lebensjahres keine rechtsverbindlichen Verträge abschließen (Artikel 1124 des Code Civil – Zivilgesetzbuch). Deshalb muss die Zustimmung von ihren gesetzlichen Vertretern eingeholt werden. Bei Kindern ab dreizehn Jahren ist es jedoch ratsam, auch deren Meinung zu berücksichtigen. Es wird davon ausgegangen, dass Kinder ab diesem Alter urteilsfähig sind, d. h. dass sie in der Lage sind, Wesen und Folgen ihrer Handlungen, z. B. wenn sie der Verwendung ihres Bildes zustimmen, zu verstehen.

RECHTE DER KINDER

Das „**Recht auf Rechte**“ von Kindern ist in der seit Juli 2023 geltenden luxemburgischen Verfassung verankert. Die Teilnahme von Kindern gehört somit zu den Grundprinzipien der luxemburgischen Gesellschaft.

Die Internationale Kinderrechtskonvention (IKRK) legt die Grundrechte von Kindern fest. Als Unterzeichnerstaat hat sich Luxemburg zum Respekt der dort aufgeführten Rechte verpflichtet. Artikel 16 der IKRK garantiert die Achtung der Privatsphäre von Kindern und Artikel 17 ihr Recht auf Information und Teilnahme.



Empfehlungen

Um die Vorschriften zum Recht am eigenen Bild einzuhalten und Kindern den richtigen Umgang mit Fotos und Videos beizubringen,

- **bitten Sie um die ausdrückliche schriftliche** Zustimmung der gesetzlichen Vertreter, bevor Sie Aufnahmen von Kindern machen oder veröffentlichen. Im Anhang finden Sie ein Muster von BEE SECURE, um die Zustimmung einzuholen, die Sie nach Bedarf verwenden oder anpassen können;
- reden Sie mit den Kindern und Eltern über **das Recht am eigenen Bild und die Zustimmung zur Benutzung**;
- **erklären Sie den Kindern, warum Sie Fotos machen**, und bitten Sie sie um ihre Zustimmung, bevor Sie Fotos machen, damit sie diesen Reflex erlernen. Beachten Sie, dass die Erlaubnis zum Fotografieren nicht automatisch auch eine Erlaubnis zur Veröffentlichung der Aufnahme bedeutet.
- Wenn keine Einigung erzielt werden kann, **besteht eine Lösung darin, die Bilder unscharf zu machen**, damit die Kinder nicht identifizierbar sind.

ZUSAMMENGEFASST

- Bitten Sie die gesetzlichen Vertreter um deren schriftliche Zustimmung.
- Bitten Sie auch die Kinder immer um deren Erlaubnis, damit sie diesen Reflex lernen.
- Erklären Sie den Kindern, warum Sie Bilder machen möchten und was Sie mit den Bildern vorhaben.


1.2 DSGVO: Speichern und Teilen von Daten oder Fotos


Im schulischen Kontext


Als Lehrkraft haben Sie Zugang zu einer Vielzahl an Daten über die Schüler und ihre Eltern, Daten, die Sie auch benutzen: Informationen über etwaige Allergien der Kinder, Kontaktdaten der Eltern, Name und Adresse der Schüler. Um den Schutz der Daten der Kinder und Eltern zu gewährleisten, ist es wichtig, verantwortungsbewusst damit umzugehen, sowohl bei der Sicherung als auch bei der Nutzung dieser Daten.

Aus rechtlicher Sicht

Das Speichern und die Nutzung von Daten oder Fotos unterliegen der Datenschutz-Grundverordnung (DSGVO), die seit 2018 für alle Akteure im europäischen Raum gilt. Jede Verarbeitung personenbezogener Daten muss **sechs Grundsätze** berücksichtigen:


- 

Nur die Daten dürfen erhoben werden, die für **den betreffenden Zweck** unbedingt erforderlich sind.
- 

Vor der **Datenverarbeitung** müssen die **Zielsetzungen präzise** definiert sein.
- 

Bei der Verarbeitung von Daten oder Bildern ist ein **transparentes Vorgehen** erforderlich.
- 

Es müssen Prozeduren vorgesehen sein, damit **die Betroffenen ihre Daten einsehen, berichtigen oder löschen können**.
- 

Die Dauer der Speicherung der Daten und Bilder muss **begrenzt sein**.
- 

Die Daten müssen gesichert und vor **unbefugtem Zugriff geschützt** sein.



Empfehlungen

Indem Sie die Grundsätze der DSGVO in Ihre tägliche Praxis integrieren, können Sie zum Schutz der personenbezogenen Daten von Schülern und ihren gesetzlichen Vertretern beitragen und ein schulisches Umfeld schaffen, das die Privatsphäre respektiert. Für eine sichere Datenverwaltung ist es vor allem wichtig zu wissen, wo die Daten gespeichert sind, und sie nur über sichere Kanäle zu übertragen.

Daten, die in bestimmten Cloud-Diensten wie Dropbox oder Messaging-Diensten wie WhatsApp gespeichert sind, könnten auf externen Servern landen, die keinerlei Garantie für Sicherheit und Transparenz bieten.

Daraus ergeben sich folgende Empfehlungen:

- **physische Speichermedien und lokale Server** zur Sicherung von Daten oder Fotos verwenden
- **vermeiden, Daten oder Fotos per E-Mail** zu versenden oder in Clouds oder Chatgruppen zu teilen
- die gesetzlichen Vertreter der Schüler über **die Speicherung und Verarbeitung der Daten und Fotos** ihres Kindes informieren
- eine **Vorgehensweise zur systematischen Überprüfung und Löschung nicht mehr benötigter Daten**, beispielsweise am Ende des Trimesters oder des Schuljahres, festlegen

ZUSAMMENGEFASST

- Seien Sie präzise und transparent, wenn es um die Speicherung und Benutzung von Fotos und Dokumenten geht.
- Löschen Sie Fotos und Daten, sobald Sie sie nicht mehr benötigen.
- Speichern Sie die Daten nur auf Medien, deren Zugriff Sie kontrollieren.
- Benutzen Sie sichere Übertragungskanäle (Rubrik 2.1 Elektronische Geräte sichern).



1.3 Benutzung von Werken Dritter: Urheberrecht (Copyright ©)

Im schulischen Kontext

Es kann vorkommen, dass Sie als Lehrkraft zusätzlich zu den vom Ministerium für Bildung, Kinder und Jugend (MENJE) vorgesehenen Unterlagen weiteres pädagogisches Material benötigen. Bilder, Videos und Texte, die benutzt werden, um ein Thema zu illustrieren oder zu vertiefen, sind wichtige Hilfsmittel, um aktuell zu sein und für die Kinder angepasste Kurse zu gestalten. Es ist jedoch wichtig zu wissen, wie man sich dieses Material legal und unter Einhaltung der Urheberrechte beschaffen kann.

Aus rechtlicher Sicht: Ausnahme für pädagogische Zwecke und Lizenzen

Das **Urheberrecht**, auf Englisch „copyright“, gehört zur Gruppe der Rechte an geistigem Eigentum. Sie schützen literarische und künstlerische Werke ab ihrer Entstehung, ohne dass dazu Registrierungsformalitäten nötig sind. Sie geben dem Urheber oder Autor das ausschließliche

Recht, sein Werk zu nutzen und daraus finanzielle Vorteile zu ziehen. Sie schützen also ein Werk vor unbefugter Weitergabe, Vervielfältigung und Verkauf durch Dritte.

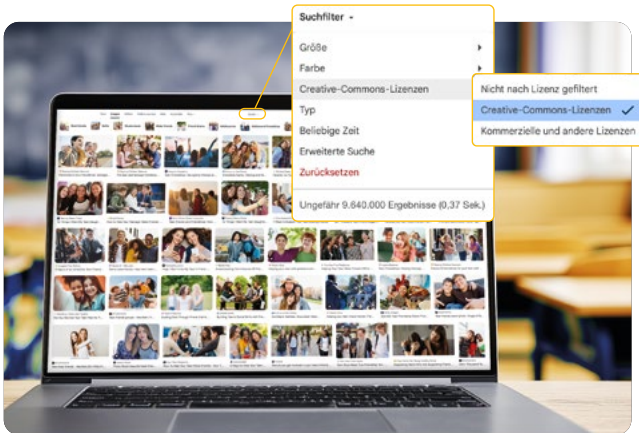
Ausnahme für pädagogische Zwecke: In Luxemburg sieht Artikel 10 des Gesetzes über die Urheberrechte eine Ausnahme vor, wenn es um die pädagogische Nutzung künstlerischer Werke geht. Laut dieser Ausnahme ist es erlaubt, Auszüge aus urheberrechtlich geschützten Werken ohne Genehmigung zu kopieren, solange die Quelle angegeben wird.

Public Domain: Ein Werk gehört zum Gemeingut, wenn es nicht unter das geistige Eigentumsrecht fällt oder der Urheberschutz abgelaufen ist. Diese Werke können frei benutzt werden, ohne jegliche Genehmigung.

Creative Commons: Werke unter einer „Creative Commons“-Lizenz können gratis benutzt werden. Der Autor des Werkes kann jedoch die Bedingungen festlegen, unter denen er sein Werk zur Verfügung stellt. Folglich gibt es unterschiedliche Varianten dieses Lizenztyps: Muss man den Autor erwähnen? Hat man das Recht, das Werk zu bearbeiten oder zu verändern?

Empfehlungen

- Die Angabe der Quellen, die als Grundlagen oder Inspiration benutzt wurden, sollten aus Gründen des Berufsethos und der Transparenz stets angegeben werden (z. B. am unteren Rand von Kopien oder PowerPoint-Folien).
- Bevorzugen Sie frei verfügbare „Public Domain“ und „Creative Commons“-Ressourcen. Fügen Sie bei der Suche „free to use“ hinzu oder benutzen Sie Filter, damit nur Bilder unter einer „Creative Commons“-Lizenz angezeigt werden.



URheberRECHT UND KÜNSTLICHE INTELLIGENZ

Die künstliche Intelligenz (KI) stellt die bisherigen Regeln der Kreativität und damit auch die des Urheberrechts auf den Kopf. Die KI kann eigenständig Werke generieren, aber müssen diese behandelt werden wie von Menschen erzeugte Werke? Im engeren Sinne: Nein, es bedarf eines menschlichen Kuschaffenden, um ein Urheberrecht zu haben. Die Frage wird aber komplizierter, wenn KI als Assistent im kreativen Prozess eingesetzt wird. Ein weiterer kritischer Punkt hinsichtlich der Vereinbarkeit von Urheberrecht und KI sind die Daten, die zum Trainieren der KI-Modelle verwendet werden. Zu diesen Daten können tatsächlich – je nach KI Tool – einige urheberrechtlich geschützte Werke gehören, die ohne Zustimmung der Autoren benutzt wurden.

Bis auf Weiteres weist BEE SECURE darauf hin, dass Transparenz Pflicht ist. Nicht nur, dass Sie den Schülern mit gutem Beispiel vorangehen, Sie vermeiden auch unangemessene urheberrechtliche Forderungen und tragen gleichzeitig dazu bei, die Vergütung von Kuschaffenden hinsichtlich computergenerierter Werke zu schützen. Greifen Sie außerdem auf die im KI Kompass empfohlenen KI-Tools zurück.

Gehen Sie mit gutem Beispiel voran: Erwähnen Sie es, wenn Sie KI benutzen.

ZUSAMMENGEFASST

- Stellen Sie sicher, dass sie das Recht haben, ein Bild oder ein anderes Werk zu verwenden, und geben Sie den Autor an.
- Sprechen Sie mit den Schülern über das Thema Urheberrecht und erklären Sie ihnen, wie sie Plagiate vermeiden können.
- Geben Sie immer an, wenn eine KI zur Erstellung von Inhalten benutzt wurde.

1.4 Regeln für die Nutzung von Bildschirmen durch Kinder: sicheres Lernen

Im schulischen Kontext

Digitale Medien bieten neue Lernmöglichkeiten, bringen aber auch neue Herausforderungen mit sich. Übermäßiger Bildschirmkonsum birgt unterschiedliche Risiken, so kann er zum Beispiel das Schlafverhalten beeinflussen oder zu Übergewicht führen. Kinder sollen einen verantwortungsvollen und bewussten Umgang mit digitalen Medien lernen; gleichzeitig müssen sie vor deren negativen Auswirkungen geschützt werden.

Aus rechtlicher Sicht:

Handyverbot in der Schule

Seit 2025 sind an allen Grundschulen und in allen Betreuungsstrukturen (Maisons relais) Handys und andere netzwerkfähige Geräte verboten. Dieser Entschluss des Ministeriums für Bildung, Kinder und Jugend wurde gefasst mit dem Ziel, die Zeit, die die Kinder vor dem Bildschirm verbringen, zu reduzieren und analoge Aktivitäten zu fördern.

Netzwerkfähige Geräte dürfen nach wie vor zu pädagogischen Zwecken benutzt werden, allerdings unter der Aufsicht der Lehrkräfte. Ausnahmen werden gemacht, wenn ärztlich attestierte medizinische Bedürfnisse des Kindes vorliegen.

Empfehlungen

Die Fähigkeiten und Fertigkeiten zum Umgang mit netzwerkfähigen Geräten und zur Aufnahme digitaler Inhalte sind nicht angeboren. Die Kinder erlernen sie im Lauf ihrer Entwicklung. Die vom Psychiater und Psychoanalytiker Serge Tisseron vorgeschlagene **Regel 3-6-9-12** gibt Richtlinien für die Nutzung von Bildschirmen je nach Alter des Kindes.

6 bis 9 Jahre



DIE NUTZUNG DIGITALER GERÄTE BEGLEITEN

Zu Beginn des Zyklus 2 der Grundschule benötigen Kinder noch Unterstützung beim Umgang mit digitalen Geräten. Mit der Zeit werden sie jedoch selbstständiger und beherrschen diese Umgebung immer besser.

9 bis 12 Jahre



DIE RISIKEN IM INTERNET ERKLÄREN

In diesem Alter sind die Schüler besser in der Lage, selbstständig zu handeln und ihre Aktivitäten auszuwählen, aber sie sind noch nicht reif genug, um die Gefahren des Internets selbst einzuschätzen. Dies ist der richtige Zeitpunkt, um ihnen zu erklären, dass alles, was online gestellt wird, von jedem gesehen werden kann, und dass sogar gelöschte Informationen oder Fotos weiterhin im Umlauf bleiben können. Sensibilisieren Sie die Kinder auch für Falschinformationen: **Nur weil etwas irgendwo geschrieben steht, muss es noch lange nicht wahr sein!**

ZUSAMMENGEFASST

- Verbot von Smartphones in der Schule seit April 2025.
- Die Benutzung digitaler Tools dem Alter der Kinder anpassen (Regel 3-6-9-12).
- Betreute digitale Aktivitäten planen und vorbereiten, um einen größtmöglichen didaktischen Nutzen zu erzielen.
- Analoge Aktivitäten planen (erliewen.snj.lu).

2. EINRICHTUNG

UND SCHUTZ DER GERÄTE



Um die Schüler anzuleiten und zu inspirieren, sollten Lehrer die Werte und Verhaltensweisen verkörpern, die sie ihren Schülern vermitteln möchten. Lehrkräfte sollten sich der tiefgreifenden Auswirkungen ihres Einflusses bewusst sein und daher wissen, wie sie ihre elektronischen Geräte im Unterricht sicher konfigurieren und verwenden können.

2.1 Elektronische Geräte sichern

Privat und beruflich genutzte elektronische Geräte trennen

Die Nutzung privater Geräte und Dienste wie WhatsApp mag für die Organisation des Schulalltags praktisch erscheinen, doch sie birgt Risiken für den Schutz der Daten von Lehrkräften und Schülern. Es wird daher dringend empfohlen, keine privaten netzwerkfähigen Geräte wie Smartphones, Tablets oder Computer im schulischen Kontext zu verwenden und nur die vom Ministerium für Bildung, Kinder und Jugend empfohlenen Dienste zu nutzen (siehe nächsten Punkt).

Die von kompetenten Stellen empfohlenen Dienste benutzen

Die Schulen stellen oft Systeme und spezifische Softwareprogramme zur Verfügung, um ihre pädagogischen Ressourcen zu verwalten, mit den Schülern und den Eltern zu kommunizieren und die Fortschritte der Schüler zu verfolgen. Professionelle Tools sind bereits so vorkonfiguriert, dass sie eine maximale Sicherheit gewährleisten. Diese Systeme haben außerdem den Vorteil, dass sie das Risiko der Ablenkung verringern (kein Zugang zu sozialen Netzwerken oder Spielen).

Vom Ministerium für Bildung, Kinder und Jugend empfohlenen, bzw. zur Verfügung gestellten Dienste und Softwareprogramme, wie beispielsweise aktuell:



Microsoft Teams/OneDrive
für den Austausch von Dokumenten



Der **KI Kompass** für Informationen zur KI und den empfohlenen KI-Tools



LuxChat oder **Signal** für die Kommunikation mit den Schülern

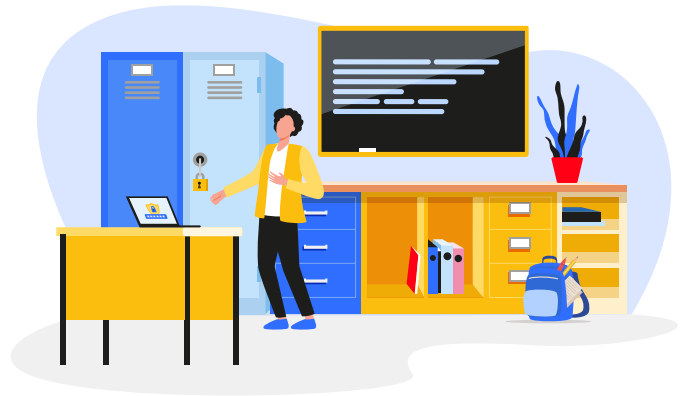


Luxchat4Gov „Bildung“ für die Kommunikation mit den Eltern der Schüler

Im Klassenzimmer



Windows+L oder Cmd+Q: Sperren Sie den Bildschirm mit der Tastenkombination Windows + „L“ oder Cmd + „Q“ für Mac, sobald Sie das Klassenzimmer oder Ihr Büro verlassen.



Sichere Aufbewahrung: Nutzen Sie sichere Aufbewahrungsmöglichkeiten wie abschließbare Schränke oder Schubladen für Ihre persönlichen Geräte während des Unterrichts, damit sie nicht leicht zugänglich sind oder beschädigt werden können.

Schutz des Displays und Schutzhüllen: Verwenden Sie stabile Schutzfolien und Hüllen, damit die Geräte bei einem Sturz oder beim Transport ins Klassenzimmer gut geschützt sind.

Maßnahmen zur Sicherung Ihrer privaten Geräte

Sorgen Sie immer für den bestmöglichen Schutz Ihrer Tools und Daten. Dies ist umso wichtiger, wenn Sie Ihren Computer, Ihr Smartphone oder ein anderes privates netzwerkfähiges Gerät im schulischen Kontext verwenden müssen.



Sperrung durch PIN-Code oder Passwort

Benutzen Sie einen PIN-Code oder ein sicheres Passwort, so schützen Sie Ihr Gerät vor unbefugtem Zugriff und verringern das Risiko eines Datendiebstahls.



Passwortmanager

Benutzen Sie diese Software, um starke und einzigartige Passwörter zu erstellen und diese sicher zu speichern. So müssen Sie sich keine Vielzahl von Passwörtern merken, sondern nur das Hauptpasswort Ihres Passwortmanagers.



Software-Updates

Stellen Sie sicher, dass alle verwendeten Softwareprogramme und Anwendungen regelmäßig aktualisiert werden, um den neuesten Schutz vor Online-Bedrohungen zu haben.



Regelmäßige Backups

Sichern Sie wichtige Daten und Dateien regelmäßig (z. B. einmal pro Woche) auf einem externen Datenträger oder einem sicheren Cloud-Dienst oder richten Sie automatische Backups ein, um Datenverluste durch Beschädigungen oder Fehlfunktionen zu vermeiden.



Öffentliche WiFi-Netze (WLAN-Netze)

Um Passwörter einzugeben oder Zahlungen zu tätigen, sollten Sie das mobile Internet gegenüber öffentlichen Netzwerken bevorzugen.



Nicht genutzte Funktionen deaktivieren

Deaktivieren Sie Bluetooth, NFC oder Ortungsdienste und aktivieren Sie sie nur bei Bedarf.



Maßnahmen bei Diebstahl oder Verlust des Gerätes

Informieren Sie sich über Maßnahmen, die Sie im Fall des Verlusts oder Diebstahls Ihres Geräts ergreifen sollten, um mögliche negative Folgen zu minimieren.



PASSWÖRTER FÜR SCHÜLER

Die **Wahl des Passworts** ist ein guter Zeitpunkt, um den Schülern die Begriffe Verantwortung und Recht auf Privatsphäre näherzubringen. Lassen Sie die Kinder ihr eigenes Passwort wählen, nachdem Sie ihnen erklärt haben, wie man ein sicheres Passwort erstellt.

Wie erstellt man ein sicheres Passwort?

MÖGLICHKEIT 1

Wählen Sie einen Satz, der Ihnen gefällt, der leicht zu merken ist und der keine persönlichen Informationen enthält.

BEISPIEL

Heute esse ich 1 Apfel aus dem Garten meiner Eltern!

ERWEITERTE OPTION

Ersetzen Sie die Leerzeichen durch ein Sonderzeichen.

BEISPIEL

Heute!esse!ich!1!Apfel!aus!dem!Garten!meiner Eltern!

MÖGLICHKEIT 2

Sie können auch lediglich die Anfangsbuchstaben der Wörter des Satzes benutzen.

EXEMPLE

Hei1AadGmE!

Erstellen Sie verschiedene Passwörter: Personalisieren Sie Ihr Passwort je nach Anwendung oder Website, die Sie benutzen. Zum Beispiel: Fügen Sie für TikTok „tt“ am Ende hinzu, das ergibt dann:

BEISPIEL

Hei1AadGmE!tt

Um die Sicherheit Ihres Passworts zu überprüfen, gehen Sie auf die Website von **BEE SECURE**, wählen Sie „Interaktive Tools“ im Menü, anschließend „Die Güte eines Passworts testen“.

Bewahren Sie Ihr Passwort an einem sicheren Ort auf



Sobald die Schüler ein sicheres Passwort erstellt haben, schreiben sie es auf einen Zettel, stecken diesen in einen Umschlag, der fest zugeklebt wird. Die Umschläge werden dann an einem Ort aufbewahrt, der nicht für Dritte zugänglich ist. Hat ein Schüler sein Passwort vergessen, kann er im Umschlag nachsehen. Es ist wichtig, dass die Schüler lernen, dass Passwörter wie Zahnbürsten sind: Man teilt sie nicht mit anderen!

2.2 Vertraulichkeit und Schutz der Privatsphäre

Als Lehrkraft kommunizieren Sie mit den Kindern, den Eltern, den Arbeitskollegen, den Fachkräften für besondere Bedürfnisse und anderen Personen. Oft geht es bei diesen Gesprächen um sensible Daten wie Informationen über die Gesundheit des Kindes oder persönliche Daten wie Name und Adresse des Kindes. Gehen Sie verantwortungsbewusst mit diesen Daten um und gewährleisten Sie das Recht der Kinder auf Privatsphäre.



PERSÖNLICHE DATEN ODER SENSIBLE DATEN?

Persönliche Daten ermöglichen die Identifizierung einer Person anhand einer Information oder einer Kombination von Informationen. Beispiel: Name, Adresse, Alter, Telefonnummer. Die Verarbeitung dieser Daten unterliegt der DSGVO.

Sensible Daten ermöglichen nicht nur die Identifizierung einer Person, sondern können auch zu Diskriminierung oder einer Verletzung der Grundrechte der Person führen. Die Weitergabe dieser Daten ist gemäß DSGVO verboten, außer in einigen sehr spezifischen Ausnahmefällen, wie zum Beispiel zum Schutz des Lebens oder mit ausdrücklicher Zustimmung der betroffenen Person. Beispiele: Rasse oder ethnische Herkunft, Religion, medizinische Daten, Daten über die sexuelle Orientierung.

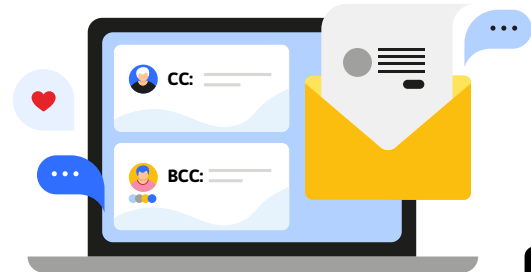


Maßnahmen für sichere Kommunikation und Datenübertragung

Versenden von Mitteilungen und E-Mails: Vom Versenden persönlicher Daten über WhatsApp oder via E-Mail wird abgeraten, da es sich hierbei um nicht sichere Verbindungen handelt. Um die Privatsphäre der Kinder und Eltern zu schützen, sollten gesicherte Verbindungen wie Luxchat und die von CGIE/Restena/der Schule vorgeschlagenen Plattformen für den Datenaustausch bevorzugt werden (Rubrik 2.1 Elektronische Geräte sichern).

DIE RICHTIGEN REFLEXE, UM ZU VERHINDERN, DASS EINE E-MAIL IN DIE FALSCHEN HÄNDE GERÄT

- Überprüfen Sie den Empfänger: Ist es der richtige Elternteil oder gesetzliche Vertreter, dem Sie die E-Mail schicken?
- Überprüfen Sie die Felder Cc und Bcc (leer, mit Ausnahme der gewählten Empfänger natürlich).
- Wenn Sie eine E-Mail weiterleiten, gibt es in den zuvor gesendeten E-Mails Informationen, die den Empfänger nichts angehen?
- Überprüfen Sie, ob Sie „antworten“ oder „allen antworten“ ausgewählt haben.



CC UND BCC, WAS BEDEUTET DAS?

„**Cc**“, Abkürzung für „carbon copy“. Dieses Feld fügt zu den „primären“ Empfängern weitere Empfänger hinzu, von denen nicht unbedingt eine Antwort erwartet wird, die jedoch in eine Angelegenheit einbezogen oder über ein Thema informiert werden sollen. Die elektronischen Adressen der Personen unter „Cc“ sind für die primären Empfänger sichtbar.

„**Bcc**“, Abkürzung für „blind carbon copy“. Die Empfänger der E-Mail können die anderen Empfänger nicht sehen. Eine Möglichkeit, keine Empfänger preiszugeben – und somit deren Kontaktdaten zu schützen – besteht darin, die E-Mail an die eigene Adresse zu senden und alle Empfänger im Feld Bcc einzugeben.

Online Datenverarbeitungstools: Online Datenverarbeitungstools wie kollaborative online Texteditoren können Sicherheitsrisiken bergen. Lehrkräfte sollten sich über die Datenschutzrichtlinien der von ihnen verwendeten Tools im Klaren sein und sicherstellen, dass die Daten ethisch einwandfrei und sicher verarbeitet werden. Es wird empfohlen, sich auf die vom Ministerium für Bildung, Kinder und Jugend angebotenen Programme und Tools zu beschränken. Dies gilt ebenso für KI-Programme.



MIT KÜNSTLICHER INTELLIGENZ ARBEITEN

Künstliche Intelligenz hat Einzug in unser Leben gehalten und ihre immer leistungsfähigeren Funktionen entwickeln sich in rasendem Tempo weiter. Es ist zwar völlig legitim, sich von einer KI unterstützen zu lassen, doch sollte man gegenüber den Antworten der KI **wachsam und kritisch** bleiben:

- Die Antworten können sehr überzeugend, aber falsch sein.
- Die Antworten können unvollständig sein und einige Aspekte nicht beinhalten.
- Die Antworten können verfälscht sein und Stereotypen verstärken.

Ein anderer Punkt, den es zu beachten gilt, ist der **Datenschutz**: Es ist schwierig zu wissen, wie die Tools mit den Daten umgehen und wie sie später benutzt werden. Wenn ein Dienst (mit oder ohne KI) gratis angeboten wird, bezahlt man wahrscheinlich mit seinen persönlichen Daten. **Geben Sie bei Kontakt mit einem KI-unterstützten Chatbot keine persönlichen Daten oder andere Informationen ein, die Sie oder Ihre Schüler identifizieren könnten (Vornamen, Namen, Geburtstage, Adressen, Name der Schule usw.).**

Gefahren im Internet vorbeugen

Internetinhalte filtern: Filterprogramme analysieren den Inhalt von Webseiten in Echtzeit und schränken die Inhalte ein, die angezeigt werden. Sie können individuell angepasst werden und blockieren den Zugriff auf unangemessene oder gefährliche Websites, beispielsweise solche mit Gewaltdarstellungen, Pornografie oder Hassreden.

Zwei-Faktor-Authentifizierung: Die Aktivierung der Zwei-Faktor-Authentifizierung für Online-Konten sorgt für zusätzliche Sicherheit beim Einloggen. Diese Maßnahme verringert das Risiko, dass sich Dritte in ein Konto (z. B. ein soziales Netzwerk) einloggen, selbst wenn sie sich das Passwort beschafft haben.

Phishing-Versuche erkennen (Rubrik 3. Nutzung der sozialen Netzwerke):

- Überprüfen Sie die Echtheit von E-Mails oder Websites, bevor Sie auf Links klicken.
- Überprüfen Sie die Domain der URL, um sicherzustellen, dass sie mit der Website übereinstimmt, auf die Sie zugreifen möchten. Phishing-Websites verwenden oft Domains, die denen seriöser Websites ähneln, enthalten jedoch minimale Abweichungen oder Tippfehler.
- Überprüfen Sie die Syntax der URL. Fehler oder ungewöhnliche Zeichen könnten auf einen Betrugsversuch hindeuten.
- Sicherheitsprotokoll: Überprüfen Sie, ob die URL mit „https://“ beginnt und nicht nur mit „http://“. Ein „https://“ zeigt an, dass die Verbindung sicher und verschlüsselt ist.

Phishing-Versuche melden: Melden Sie der Schulverwaltung oder der Informatikabteilung jeden Phishing-Versuch, damit geeignete Maßnahmen ergriffen werden können und das gesamte Schulpersonal informiert wird.

3. NUTZUNG DER SOZIALEN NETZWERKE



Die sozialen Netzwerke sind heute Teil des digitalen sozialen Lebens und die Verhaltensregeln unterscheiden sich nicht wesentlich von denen im analogen sozialen Leben. Wenn die Lehrkräfte sich der Risiken bewusst sind, können sie nicht nur ihr öffentliches Image schützen, sondern auch Kinder vor Online-Bedrohungen schützen.

3.1 Die eigene Darstellung im Internet

Im schulischen Kontext

Als Lehrkraft und Beamter vertreten Sie den Staat und die Schule als öffentliche Einrichtung, weshalb Sie verpflichtet sind, Vorsicht walten zu lassen bei allem, was Sie ins Netz stellen. Während sich Posts über sportliche Erfolge oder ehrenamtliches Engagement positiv auf das öffentliche Image auswirken, können Fotos von wilden Partys oder andere zweifelhafte Inhalte Fragen hinsichtlich Ihrer Eignung als Lehrkraft aufwerfen.

Die sozialen Netzwerke sind a priori öffentliche Plattformen: Ihre Kollegen, Ihre Vorgesetzten, die Schüler und deren Eltern haben Zugriff darauf und können Ihre Beiträge sehen.

- Auch Inhalte, die nur für Freunde bestimmt sind, können für andere sichtbar werden, wenn sie geteilt werden oder wenn Ihre Freunde oder das soziale Netzwerk Opfer einer Datenschutzverletzung wurden.
- Sogar ein simples „Like“ bei einem Beitrag ist keine Privatangelegenheit, es ist eine für andere sichtbare öffentliche Handlung.

Aus rechtlicher Sicht

(Art. 10 Abs.1 des Gesetzes vom 16. April 1979 in seiner geänderten Form)
Angemessenes Verhalten

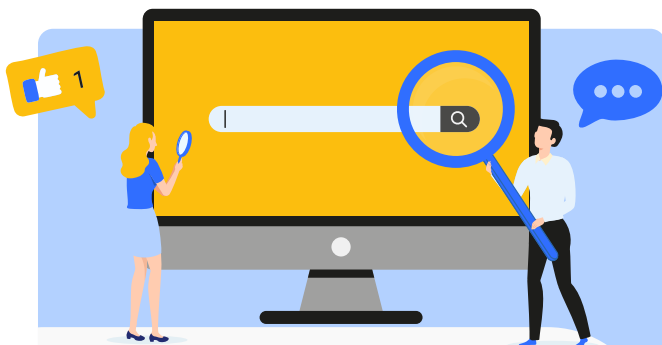
Der Beamte muss, **bei der Ausübung des Dienstes oder außerhalb der Ausübung seines Amtes**, alles vermeiden, was die Würde dieser Funktionen oder die Fähigkeit, sie auszuüben, beeinträchtigen, einen Skandal verursachen oder die Interessen des öffentlichen Dienstes gefährden könnte.

Ihr berufliches Ansehen dient der Wahrung des Vertrauens in den Lehrerberuf und in das Bildungswesen. Die Untergrabung der Glaubwürdigkeit der Schule oder des Berufs kann zu Disziplinarmaßnahmen oder, im Extremfall, zur Entlassung führen.



Empfehlungen

Überprüfen Sie, welches Bild von Ihnen online zu finden ist, wählen Sie die richtigen Privatsphäre-Einstellungen und achten Sie auf Ihre Darstellung in den sozialen Netzwerken.



SO ÜBERPRÜFEN SIE IHRE ONLINE-DARSTELLUNG:

- Geben Sie Ihren Namen in eine Suchmaschine ein und analysieren Sie die Ergebnisse: Welche Informationen, Fotos und Beiträge finden Sie? Welche Schlussfolgerungen ziehen Sie daraus?
- Melden Sie sich bei Ihren sozialen Netzwerken ab oder bitten Sie jemanden, sich Ihr Profil auf seinem Handy ansehen zu dürfen. So erfahren Sie, wie Ihr Profil aus der Perspektive anderer Nutzer aussieht.
- Verwenden Sie die von BEE SECURE erstellte Checkliste (im Anhang).



HANDHABUNG DER EIGENEN DARSTELLUNG IN SOZIALEN NETZWERKEN:

- Räumen Sie auf: Löschen Sie rufschädigende Beiträge und Fotos, misten Sie Ihre Freundeslisten aus.
- Aktualisieren Sie die für Ihr Profil geltenden Privatsphäre-Einstellungen, um die Sichtbarkeit und Reichweite Ihrer Beiträge einzuschränken.
- Legen Sie für jedes soziale Netzwerk das Nutzungsziel fest (mit wem kommuniziere ich wie worüber?).
- Verwenden Sie je nach Plattform unterschiedliche Profilfotos und Pseudonyme, trennen Sie nach privater und beruflicher Nutzung.



3.2 Die Klasse in den sozialen Netzwerken

Im schulischen Kontext

Lehrkräfte können eine wichtige Rolle dabei spielen, Schüler für bewährte Praktiken und Risiken im Zusammenhang mit der Nutzung sozialer Netzwerke zu sensibilisieren. Im Allgemeinen haben nur wenige Kinder unter zwölf Jahren ein Benutzerkonto in sozialen Netzwerken; soziale Netzwerke sind ohnehin für Kinder unter fünfzehn Jahren nicht zu empfehlen (Strategie „sécher.digital“ des MENJE). Dennoch ist es wichtig, die bestehenden Mechanismen und Praktiken zu verstehen, um die Probleme, mit denen Kinder konfrontiert werden können, besser zu begreifen.

Möglicherweise möchten Sie mit Ihrer Klasse auch an einem Projekt teilnehmen, das eine Präsenz in sozialen Netzwerken erfordert, um Stimmen zu sammeln oder Sponsoren zu finden, oder Sie müssen Fotos von Projekten in einem sozialen Netzwerk veröffentlichen. In diesem Fall müssen Sie den Nutzen des Projekts, die Vor- und Nachteile, ein breiteres Publikum anzusprechen, und die Rechte der Kinder auf Privatsphäre gegeneinander abwägen.

Aus rechtlicher Sicht

Aufgrund der Kinderschutzgesetze in den USA verlangen die meisten sozialen Netzwerke und Messaging-Dienste, dass die Nutzer mindestens dreizehn Jahre alt sind. In Luxemburg, wie im übrigen Europa, legt die DSGVO das Mindestalter für Nutzer fest. Jugendliche und Kinder zwischen dreizehn und sechzehn Jahren benötigen die Zustimmung ihrer Eltern, um Messaging-Dienste nutzen zu dürfen. In der Praxis hat sich jedoch gezeigt, dass die Altersüberprüfung relativ leicht zu umgehen ist.

Fotos, die im Unterricht gemacht wurden, dürfen nicht benutzt werden, um für Unterrichtsmaterialien zu werben, da es sich hierbei um einen Erwerbszweck handelt.

Empfehlungen

- Vermeiden Sie „Freundschaften“ mit Eltern oder Schülern: Erklären Sie den Schülern, dass Sie keine „Freundschaftsanfragen“ von Schülern annehmen, um klarzustellen, dass es sich nicht um persönliche Zurückweisungen handelt.
- Trennen Sie Ihr persönliches Profil von Veröffentlichungen von Schulprojekten.
- Bitten Sie um die ausdrückliche Erlaubnis der Eltern für die Art des Inhalts (z. B.: Fotos der von den Kindern geschaffenen Produkte), die Art der benutzten Plattform und die Dauer der Sichtbarkeit.
- Veröffentlichen Sie die Fotos ohne die persönlichen Daten der Kinder (also ohne Namen usw.).
- Denken Sie an die Vorgaben bezüglich des Rechts am eigenen Bild (Rubrik 1.1).
- Konfigurieren Sie die Privatsphäre-Einstellungen (Rubrik 3.1).



ZUSAMMENGEFASST

- Pflegen Sie Ihre Online-Präsenz und achten Sie auf Ihr berufliches Ansehen.
- Bitten Sie die Eltern um deren ausdrückliche Zustimmung, bevor Sie Bilder oder andere Informationen von Schulprojekten ins Netz stellen.

3.3 Gefahren: Hacking und Identitätsdiebstahl

Im schulischen Kontext

Jeder kann Ziel oder sogar Opfer von Cyberkriminellen werden. Diese missbrauchen die Identität des Nutzers, um an sensible Informationen zu gelangen oder Daten zu manipulieren. Für Lehrkräfte in einer Autoritäts- und

Vertrauensposition sind die Risiken dieser Bedrohung erheblich. Die Vorsichtsmaßnahmen zum Schutz Ihrer Identität tragen auch dazu bei, Schüler vor unangemessenen Inhalten oder schädlichem Verhalten zu schützen.



VERSCHIEDENE ARTEN VON CYBERKIRMINALITÄT

Phishing ist eine Technik, die Cyberkriminelle einsetzen, um Nutzer zu täuschen und sie so dazu zu bringen, sensible Informationen wie Passwörter, Kreditkartennummern oder andere persönliche Daten preiszugeben. Durch die Erstellung eines „gefälschten Profils“ (auf Englisch „fake profile“) bauen Cyberkriminelle Vertrauen zu ihren Opfern auf, um sie anschließend um persönliche oder sensible Informationen zu bitten.

Grooming bezeichnet einen Vorgang, bei dem ein Erwachsener ein Vertrauensverhältnis zu einem Kind oder Minderjährigen im Internet aufbaut, mit dem Ziel, es/ihn sexuell auszubeuten. Die Lehrkräfte sind besonders gefährdet gegenüber dieser Bedrohung, wenn ihre Identität missbraucht wird. Die Folgen für die Kinder und ihr Umfeld sind verheerend.

Fotomontagen und Deep-Fake-Videos verwenden vorhandene Bilder des Gesichts oder Körpers, setzen sie in kompromittierende Kontexte oder manipulieren sie derart, dass die Person Dinge tut oder sagt, die sie nie gesagt oder getan hat. Ein Beispiel hierfür sind pornografische Videos. Obwohl die Opfer absolut nichts mit diesen Bildern zu tun haben, macht die Verbreitung im Internet es sehr schwer, die Wahrheit wiederzugeben und das Ansehen wiederherzustellen.

Aus rechtlicher Sicht

Die DSGVO verpflichtet Sie dazu, Daten von Kindern verantwortungsbewusst, transparent und sicher zu verarbeiten (Rubrik 1.2). Wenn vertrauliche Informationen über Schüler aufgrund des fahrlässigen Verhaltens einer Lehrkraft öffentlich werden, kann dies rechtliche Konsequenzen für die Lehrkraft haben.

Empfehlungen: Sich vor Identitätsdiebstahl schützen und dagegen vorgehen

- Überprüfen Sie regelmäßig, ob Ihr Name, Ihre Identität oder Fotos nicht missbraucht werden.
- Schützen Sie Ihr Profil mit einzigartigen, sicheren Passwörtern.
- Erstellen Sie für die sozialen Netzwerke eine getrennte E-Mail-Adresse.
- Bei Missbrauch: Melden Sie gefälschte Profile oder den Missbrauch Ihrer Daten beim Netzbetreiber / Serviceanbieter.
- Benachrichtigen Sie Ihre Kollegen, damit sie sich vor dem gefälschten Profil in Acht nehmen.



4. VORBEUGUNG UND VORGEHEN BEI ZWISCHENFÄLLEN



Ob online oder im persönlichen Umgang, Respekt gegenüber anderen ist wichtig und muss unter allen Umständen gepflegt werden. In der digitalen Welt fördern Anonymität und Distanz manchmal respektloses Verhalten. Als vorbeugende Maßnahme hilft ein zu Beginn des Schuljahres gemeinsam mit den Schülern erstellter Verhaltenskodex, die Risiken zu erkennen, denen sie ausgesetzt sein können, und ermöglicht es, in kritischen Situationen im Unterricht angemessen zu reagieren.

4.1 Vorbeugung

Erstellen eines Verhaltenskodex

Zu Beginn des Schuljahres ist es sinnvoll, mit den Schülern das Thema des respektvollen Umgangs miteinander zu besprechen. Allgemeine Regeln für den Umgang mit anderen im Unterricht und im Internet können diskutiert und anschließend in einem Verhaltenskodex festgehalten werden. Es ist wichtig, über die Konsequenzen zu sprechen und Verfahren für den Fall von Regelverstößen festzulegen. Der von allen Beteiligten – Lehrern, Schülern und Eltern – unterzeichnete und gut sichtbar im Klassenzimmer ausgehängte Verhaltenskodex ist ein Instrument zur Prävention von respektlosem Verhalten.

BEE SECURE stellt ein Muster für einen solchen Verhaltenskodex im Anhang zur Verfügung.

Regeln für den Klassenchat festlegen

Da viele Klassen einen Chat für den Austausch zwischen allen Klassenmitgliedern nutzen, ist es ratsam, auch Regeln für den Chat festzulegen. Wenn viele Personen in der Chatgruppe sind, können Probleme auftreten, wie z. B. Belästigungen in den Mitteilungen, Spam, irrelevante Inhalte oder Kettenbriefe. Überlegen Sie sich auch Konsequenzen und Sanktionen bei Nichteinhaltung der Regeln.



Mit gutem Beispiel vorangehen

Ihr eigenes Verhalten im Unterricht kann das Verhalten Ihrer Schüler beeinflussen. Nutzen Sie diese Gelegenheit, um ihnen ein gutes Beispiel zu geben, indem Sie die Rechte des Kindes, die Datenschutz-Grundverordnung, die Schulordnung, aber auch den Verhaltenskodex einhalten, den Sie gemeinsam mit Ihren Schülern erstellt haben!

Im Dialog mit den Kindern bleiben

- Halten Sie sich über die Kommunikationspräferenzen Ihrer Schüler auf dem Laufenden: Trends, Spiele, genutzte Plattformen und Herausforderungen ändern sich ständig und variieren je nach Altersgruppe. Tauchen Sie in ihre Welt ein und informieren Sie sich ständig, damit Sie sie besser verstehen.
- Weiterbildungen sind ebenfalls eine hervorragende Möglichkeit, um über neue Trends auf dem Laufenden zu bleiben. Informieren Sie sich über die verfügbaren Trainings und Kurse – insbesondere über die BEE SECURE-Trainings für Fachkräfte aus dem Bildungsbereich.

Schüler und Schulgemeinschaft sensibilisieren

- Das Thema mit der Klasse besprechen, um den Schülern die Risiken dieser Plattformen aufzuzeigen, vor allem, wenn viele Schüler in der Klasse Plattformen nutzen, die für ihr Alter nicht geeignet sind.

- Eine weitere Möglichkeit besteht darin, ein präventives Training von BEE SECURE zu buchen, um das Thema auf spielerische Weise mit einem Trainer im Unterricht zu behandeln („Cyber-Mobbing: Mit Detektiv Shadow auf Mission“ für den Zyklus 3.2).
- Eine Informationsveranstaltung für die Eltern zu den Risiken und Gefahren im Netz organisieren.

Den Zugang zu Hilfe erleichtern

Stellen Sie sicher, dass die Kinder die Telefonnummern und Adressen kennen, wo sie sich Hilfe holen können, anonym, vertraulich und gratis, für den Fall, dass sie sich nicht an eine Vertrauensperson wenden möchten.



BEE SECURE Helpline
8002 1234



KJT
1 1 6 1 1 1



Online help: Schriftliche Online-Beratung für Kinder und Jugendliche

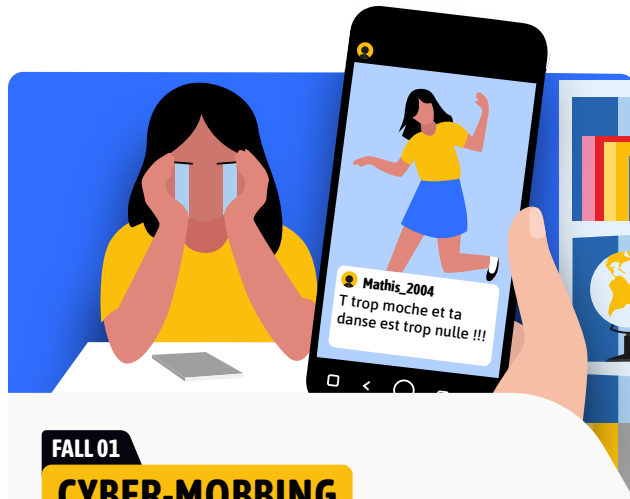


Chatberodung: Beratung in Form eines Live-Chats, für Kinder und Jugendliche

4.2 Vorgehen bei Zwischenfällen

Das Internet ist Teil des Alltags von Schülern und Lehrkräften. Die Gefahren für Schüler sind vielfältig: Cyber-Mobbing, die Konfrontation mit ungeeigneten Inhalten, Verletzungen der Privatsphäre, unrechtmäßige Weitergabe von Daten oder Inhalten machen auch vor Klassenzimmern nicht Halt. Wenn man die Risiken kennt, denen Kinder ausgesetzt sein können, und weiß, wie man darauf reagieren soll, kann man sie besser schützen und ihnen eine verantwortungsvolle und sichere Nutzung des Internets vermitteln.

In den folgenden Abschnitten finden Sie Beispielfälle, Fragen, die Sie sich vor einer Reaktion stellen sollten, und Maßnahmen, die Sie anschließend ergreifen können.



FALL 01

CYBER-MOBGING

Jacky ist acht Jahre alt. Sie kommt zu Ihnen und erzählt, dass ein anderer Schüler der Schule ihr auf TikTok einen Kommentar geschickt hat mit dem Inhalt, es sei dämlich, wie sie tanze.

GLEICHES RECHT FÜR ALLE

Art. 2 der Kinderrechtskonvention besagt, dass jedes Kind Rechte hat, „ohne Unterschied“, das heißt, jedes Kind hat ein Recht auf Nicht-Diskriminierung.



Bevor Sie reagieren



Wurde der Kommentar während der Schulzeit geschickt?

Achten Sie darauf, Ihre Handlungskompetenz nicht zu überschreiten; neben der Verantwortung der Lehrkräfte gibt es auch die Verantwortung der Eltern.



Ist die Plattform, auf der die Nachricht oder der Kommentar gepostet wurde, für Kinder im Alter des Opfers bestimmt?

Es ist wichtig, sich klarzumachen, dass soziale Medien wie TikTok, Instagram und Co nicht für Kinder unter dreizehn Jahren gedacht sind.



Hat das Opfer mehrere solcher Nachrichten erhalten oder handelt es sich um eine einzige Nachricht?

Unter Cyber-Mobbing versteht man das vorsätzliche Beleidigen, Bedrohen, Verspotten oder Belästigen anderer Personen über einen längeren Zeitraum online oder über Telefon.

Vorgehensweise

1. Dem betroffenen Schüler zuhören und ihn unterstützen

- Nehmen Sie dem Kind die Schuldgefühle. Versichern Sie ihm, dass es nicht seine Schuld ist und dass es sich nichts vorzuwerfen hat.
- Greifen Sie als Erwachsener ein und versichern Sie dem Kind, dass Sie reagieren werden. Kinder sind nicht in der Lage, Probleme mit Cyber-Mobbing selbst zu lösen, daher ist das Eingreifen eines Erwachsenen unerlässlich.
- Raten Sie dem Kind, nicht auf solche Nachrichten oder Beiträge zu reagieren.
- Notieren Sie sich alles, was der Schüler erklärt, um den Fall weiterverfolgen zu können, und helfen Sie ihm gegebenenfalls dabei, Beweise zu sichern.

2. Die Schulleitung informieren

- Wenden Sie sich an Ihre Kollegen und, wenn nötig, an die Regionaldirektion und die Eltern, um die Situation zu evaluieren, und stimmen Sie sich untereinander über das weitere Vorgehen ab.

3. Die Schulgemeinschaft sensibilisieren

- Wenden Sie sich an die Arbeitsgruppe „Stop Mobbing“, eine Initiative des Ministeriums für Bildung, Kinder und Jugend, die in Klassen interveniert, Opfer unterstützt und mit Lehrern spricht.
- S-Team des Service national de la jeunesse: Das Projekt umfasst Sensibilisierungsaktivitäten und Präventionsmaßnahmen gegen Gewalt in den Schulen/ Maisons relais. Ziel ist, den Kindern und Jugendlichen

bewusst zu machen, dass sie eine Verantwortung tragen, wenn es um die Prävention von Gewalt geht, und ihnen Wege aufzuzeigen, wie sie zu einem besseren Miteinander beitragen können. Die „Peer-Mediation“ ist ein fester Bestandteil des Projekts „S-Team“.

- BEE SECURE – Training „Cyber-Mobbing: Mit Detektiv Shadow auf Mission“ für die Schüler des Zyklus 3.2.
- BEE SECURE – Training für Lehrkräfte und Erzieher zum Thema Internetnutzung durch Kinder und Jugendliche und die damit verbundenen Risiken.

4. Sich über die Rechtsgrundlage informieren

- Informieren Sie sich über die Einreichung einer Klage und das richtige Verhalten bei Konfrontationen im BEE SECURE Leitfaden zum Thema Cyber-Mobbing, den Sie auf der Website unter der Rubrik „Veröffentlichungen“ finden.

Externe Hilfe



BEE SECURE Helpline
8002 1234



KJT
1 1 6 1 1 1





FALL 02

DEEP FAKES

Sie wurden darüber informiert, dass ein Deep Fake eines Ihrer Schüler in der Schule im Umlauf ist. Das gefälschte Video, das den Schüler in einer kompromittierenden Situation zeigt, wurde von mehreren Schülern geteilt.

Vorgehensweise

1. Dem betroffenen Schüler zuhören und ihn unterstützen

- Es ist wichtig, den Schüler, der Opfer eines Deep Fakes wurde, emotional und psychologisch zu unterstützen.
- Falls noch nicht geschehen, raten Sie dem Schüler, Beweise (Screenshots) zu sichern.

2. Die Schulleitung informieren

- Melden Sie den Vorfall der Schulleitung, damit geeignete Maßnahmen ergriffen werden können.
- Ermitteln Sie die Quelle der Verbreitung: In Zusammenarbeit mit der Schulleitung muss unbedingt festgestellt werden, wie der Deep Fake erstellt und verbreitet wurde und wer daran beteiligt war.

ARTIKEL 16- SCHUTZ AUF PRIVATSPHÄRE

Garantiert jedem Kind das Recht auf Schutz der Privatsphäre, Familie, Wohnung und Korrespondenz sowie auf Schutz vor rechtswidrigen Angriffen auf seine Ehre und seinen Ruf.



3. Die Eltern informieren und einbeziehen

- Die Eltern des betroffenen Schülers müssen über den Vorfall informiert werden. Die Zusammenarbeit mit den Eltern ist entscheidend, um den Schüler zu unterstützen und ein kohärentes Vorgehen sicherzustellen.

4. Geeignete Maßnahmen ergreifen

- **Angemessene disziplinarische Maßnahmen:** Wurden die für die Erstellung und Verbreitung des Deep Fakes verantwortlichen Schüler identifiziert, müssen Disziplinarmaßnahmen gemäß den Richtlinien der Schule in Betracht gezogen werden.

5. Die Schulgemeinschaft informieren

- Organisieren Sie Sensibilisierungssitzungen, um die Schüler und Lehrkräfte über die Gefahren von Deep Fakes zu informieren und ein digitales Umfeld zu schaffen, das den gegenseitigen Respekt fördert.

6. Die rechtlichen Aspekte in Betracht ziehen

- Das luxemburgische Gesetz vom 21. Mai 2024 hat das Strafgesetz angepasst und Deep Fakes als Straftaten eingestuft.

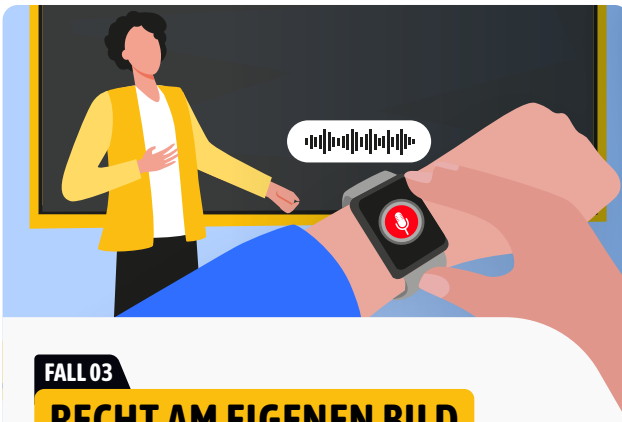
Externe Hilfe



BEE SECURE Helpline
8002 1234



KJT
116111



FALL 03

RECHT AM EIGENEN BILD

UND SCHUTZ DER PRIVATSPHÄRE

Während des Unterrichts hat Alex seine Smartwatch benutzt, um ein Video seiner Lehrkraft aufzunehmen sowie die Unterhaltung seiner Mitschüler aufzuzeichnen, ohne sie um Erlaubnis zu fragen. Er wurde von einem seiner Klassenkameraden gemeldet.

Vorgehensweise

1. Mit dem betroffenen Schüler reden

- Fordern Sie den Schüler auf, das Video und die Audioaufzeichnung sofort zu löschen.
- Erklären Sie ihm, dass ohne Zustimmung des Betroffenen ein Video die Privatsphäre verletzt und es bei den anderen Unbehagen auslösen kann.

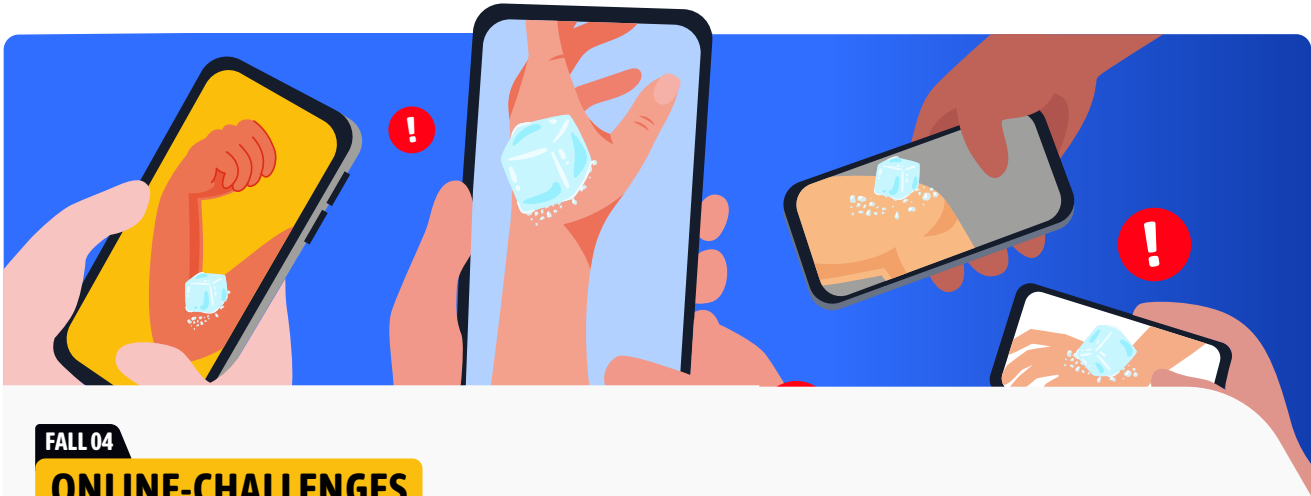
2. Wenn nötig, Schulleitung und Eltern informieren

- Informieren Sie die Eltern des betroffenen Kindes.
- Informieren Sie die Schulleitung, um etwaige Disziplinar- oder Präventionsmaßnahmen zu ergreifen.

3. Die Schulgemeinschaft sensibilisieren

- Behandeln Sie das Thema des Rechtes am eigenen Bild und der Rechte der Kinder im Unterricht.
- Informieren Sie die Eltern, um über die Bedeutung des Schutzes der Privatsphäre und das Verbot von netzfähigen Geräten im Unterricht zu reden.
- Erstellen Sie einen Verhaltenskodex (Rubrik 4.1 Vorbeugung).

4. Wenn es die Schwere des Falles erfordert, informieren Sie sich über mögliche rechtliche Schritte.



FALL 04

ONLINE-CHALLENGES

Ein Schüler startet ein gefährliches Online-Challenge, das sich schnell in der Klasse verbreitet. Der Lehrer erfährt davon.

Bevor Sie etwas unternehmen

- Stellen Sie fest, um welche Art von Challenge es sich handelt: Ist sie harmlos, riskant oder sogar gefährlich?
- Wenn die Schüler Ihnen von Challenges berichten, hören Sie ihnen zu und erklären Sie ihnen die Risiken. Vermeiden Sie es, Challenges zu erwähnen, die noch nicht im Umlauf sind, um sie nicht zu verbreiten.

Vorgehensweise

1. Mit den betroffenen Schülern reden.

- Versuchen Sie, den Sinn der Challenge zu verstehen.
- Erklären Sie die Risiken.

2. Wenn nötig, Schulleitung und Eltern informieren

- Informieren Sie die Eltern der betroffenen Kinder.
- Informieren Sie die Schulleitung, um etwaige Disziplinar- oder Präventionsmaßnahmen zu ergreifen.

3. Die Schulgemeinschaft sensibilisieren

- Machen Sie auf potenzielle Risiken aufmerksam und besprechen Sie das Thema Respekt und Sicherheit im Unterricht und erklären Sie, wie man Challenges, die Schaden anrichten können, erkennt und sie ablehnt.
- Reden Sie mit den Eltern über die Bedeutung des Schutzes der Privatsphäre und das Verbot von netzwerkfähigen Geräten im Unterricht
- Erstellen Sie einen Verhaltenskodex (Rubrik 4.1 Vorbeugung).

4. Wenn es die Schwere des Falles erfordert, informieren Sie sich über mögliche rechtliche Schritte.

4.3 Die Grenzen Ihrer Verantwortung

Entdecken Sie die verschiedenen Dienste, die Sie bei Bedarf kontaktieren können.



BEE SECURE Helpline

Hotline bietet Kindern, Jugendlichen, Eltern, Erwachsenen sowie Lehrkräften und Erziehern, die mit Problemen im Zusammenhang mit der Online-Sicherheit konfrontiert sind, praktische Ratschläge und Unterstützung. Sie hilft dabei, digitale Risiken zu verstehen und zu bewältigen..

→ bee-secure.lu/de/helpline



BEE SECURE Stopline

Eine Plattform zur Meldung illegaler Online-Inhalte (wie Kinderpornografie oder Ausbeutung). Die Meldungen werden in Zusammenarbeit mit den zuständigen Behörden und Partnern auf nationaler und internationaler Ebene bearbeitet.

→ stopline.bee-secure.lu



KJT – KannerJugendTelefon 1 1 6 1 1 1

Der Hilfsdienst für Kinder und Jugendliche bietet auch Unterstützung für Personen, die sich um sie kümmern. Die Beratung erfolgt per Telefon, E-Mail oder Chat.

→ kjt.lu



CEPAS – Centre psycho-social et d'accompagnement scolaires

Das CePAS setzt sich in Zusammenarbeit mit den Akteuren der Schulgemeinschaft für die Entfaltung und das Wohlbefinden der Jugendlichen in der Schule ein. Das Ressourcenzentrum des CePAS unterstützt das pädagogische und psychosoziale Personal der Dienste für schulpsychologische Beratung und Schulorientierung (SePAS), der sozialpädagogischen Dienste (SSE) und der Internate und begleitet sie bei der Umsetzung in der beruflichen Praxis.

→ cepas.public.lu



CESAS – Centre national de référence pour la promotion de la santé affective

Cesas unterstützt das Netzwerk der Akteure, die sich zum Ziel gesetzt haben, die affektive und sexuelle Gesundheit durch Information, Sensibilisierung und Schulung zu fördern. Besonderes Augenmerk wird dabei auf Fachkräfte im Bereich Kinder- und Jugendarbeit gelegt.

→ cesas.lu



CNAPA – Centre national de prévention des addictions

Aufgabe des CNAPA ist die Sensibilisierung für einen gesunden Lebensstil. Neben Information werden auch Fortbildungen für Fachleute aus dem pädagogischen Bereich angeboten.

→ cnapa.lu



CNPD – Commission nationale pour la protection des données

Die Nationale Kommission für den Datenschutz ist der Garant für den Schutz der Privatsphäre und die rechtmäßige Verarbeitung personenbezogener Daten. Sie berät, kontrolliert und kann bei Verstößen Sanktionen verhängen.

→ cnpd.public.lu



OKAJU – Ombudsman fir Kanner a Jugendlecher

Diese unabhängige Institution hat die Aufgabe, die Rechte des Kindes, wie sie in der Internationalen Kinderrechtskonvention (KRK) definiert sind, zu fördern, zu wahren und zu schützen.

→ okaju.lu



ONE – Office national de l'enfance

Das Office national de l'enfance (ONE) ist eine öffentliche Verwaltung unter der Aufsicht des Ministeriums für Bildung, Kinder und Jugend und bietet Unterstützung für Kinder, Jugendliche, junge Erwachsene und Familien, die Hilfe benötigen.

→ officenationaleenfance.lu



Police Lëtzebuerg

Polizei ist zuständig für Prävention, Ermittlungen und Interventionen bei Verstößen gegen das Gesetz oder bei unmittelbarer Gefahr und nimmt Meldungen entgegen, die ein polizeiliches Eingreifen erfordern.

→ police.public.lu



Planning Familial

Die vom Ministerium für Gesundheit und soziale Sicherheit anerkannte gemeinnützige Organisation möchte den Zugang zu Informationen, Aufklärung und Dienstleistungen im Bereich der affektiven, sexuellen und reproduktiven Gesundheit erleichtern. Sie hat Dienststellen in Luxemburg-Stadt, Esch-sur-Alzette und Ettelbrück.

→ pfl.lu



Respect.lu

Ein Dienst, der Menschen, die in irgendeiner Weise mit Extremismus und gewalttätiger Radikalisierung konfrontiert sind, zuhört und sie begleitet; er bietet Ressourcen, Beratung und pädagogische Hilfsmittel an.

→ respect.lu



CGIE – Centre de gestion informatique de l'éducation

Das CGIE des Ministeriums für Bildung, Kinder und Jugend ist für alle Informations- und Kommunikationstechnologien der Verwaltungen des Bildungsministeriums zuständig. Das CGIE fördert den Umgang mit der digitalen Technik durch eine Reihe von Projekten.

→ zesummendigital.lu



SCRIPT – Service de Coordination de la Recherche et de l'Innovation pédagogiques et technologiques

Als einer der wichtigsten Motoren für die Entwicklung des Bildungswesens in Luxemburg ist der SCRIPT dafür zuständig, die Prioritäten der Bildungspolitik umzusetzen und so zur Verbesserung der Schulqualität beizutragen.

→ script.lu



GOVCERT

Zentrale Anlaufstelle für alle Arten von IT-Vorfällen, die eine Bedrohung für die Informationssysteme der nationalen Regierung und anderer Betreiber kritischer öffentlicher oder privater Infrastrukturen darstellen könnten.

→ govcert.lu

BIBLIOGRAFIE

- **BEE SECURE.** Unterrichtseinheit zum Video „Sharen“
bee-secure.lu/de/publikation/unterrichtseinheit-sexting-zum-video-sharen
- **BEE SECURE.** Das PEGI-Label für Videospiele
bee-secure.lu/de/publikation/das-pegι-label-fuer-videospiele-schutz-fuer-kinder-vor-unangemessenen-inhalten
- **BEE SECURE.** Recht am eigenen Bild
bee-secure.lu/de/publikation/recht-am-eigenen-bild
- **BEE SECURE.** Bildschirme in der Familie: einstellen, aufklären, begleiten
bee-secure.lu/de/publikation/bildschirme-in-der-familie-einstellen-aufklaeren-begleiten
- **BEE SECURE.** Das Smartphone sichern
bee-secure.lu/wp-content/uploads/2023/11/securisez-votre-smartphone-fr.pdf
- **BEE SECURE.** Risiken im Netz
bee-secure.lu/de/publikation/risiken-im-netz
- **BEE SECURE.** Bist du Opfer von Cyber-Mobbing?
bee-secure.lu/de/publikation/bist-du-opfer-von-cybermobbing
- **BEE SECURE.** Radar 2025
bee-secure.lu/de/publikation/bee-secure-radar
- **BEE SECURE.** Mindestalter: Ab wann dürfen Kinder WhatsApp, Instagram & Co. nutzen?
bee-secure.lu/de/news/mindestalter-ab-wann-duerfen-kinder-whatsapp-instagram-co-nutzen
- **CGID.** Devoirs du fonctionnaire
cgid.gouvernement.lu/fr/legislation/devoirs-fonctionnaire.html
- **Childfocus.** De mots à maux : comprendre, reconnaître et agir sur le cyberharcèlement.
childfocus-webshop.be/products/dossier-pedagogique-stop-au-cyber-harcelement
- **Unicef.** Texte de la Convention relative aux droits de l'enfant
unicef.org/fr/convention-droits-enfant/texte-convention
- **Commission européenne.** Public domain
https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/public-domain-2020-11-19_en
- **CNIL.** Grands principes du RGPD
cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd
cnil.fr/fr/identifier-les-donnees-personnelles
cnil.fr/fr/definition/donnee-sensible
- **CNPD .** Droit à l'image.
cnpd.public.lu/fr/dossiers-thematiques/droit-image.html
cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/droit-image/CNPD-fiche-edusphere-milieu-scolaire.pdf
- **GDPR.eu.** What is GDPR, the EU's new data protection law?
<https://gdpr.eu/what-is-gdpr>

- **KI Kompass.** Orientierung, Praxis & Austausch zu Künstlicher Intelligenz für Schulen in Luxemburg ki-kompass.lu
- **Klicksafe.** Mediennutzungsvertrag. mediennutzungsvertrag.de
- **Klicksafe.** Klassenchat-Regeln. klicksafe.de/printmaterialien/unsere-regeln-fuer-den-klassenchat-unterrichtseinheit
- **Legilux.** Droits d'auteur legilux.public.lu/eli/etat/leg/loi/2001/04/18/n2/consolide/20220409
- **Ministère de la culture.** Droits d'auteur mcult.gouvernement.lu/dam-assets/publications/guide-manuel/minist-culture/guide-droit-auteur/droits-auteur-droits-voisins-et-autres-droits-numerique.pdf
- **Saferinternet.at.** Sichere Internet-und Handynutzung macht Schule! saferinternet.at/wie-koennen-regeln-fuer-die-handynutzung-in-der-schule-aussehen
- **Saferinternet.at.** Tipps für Lehrende. saferinternet.at/zielgruppen/lehrende
- **Sécher.Digital** secher.digital/fr/utilisation-smartphone
- **SNJ.** Activités analogiques erliewen.snj.lu
- **TISSERON, S.** Grandir avec les écrans « La règle 3-6-9-12 ». Bruxelles : Yapaka, 2013. (Temps d'arrêt lectures) 57 Pages. Document PDF yapaka.be/livre/livre-grandir-avec-les-ecrans-la-regle-3-6-9-12

FUSSNOTE

¹Das Recht am eigenen Bild gründet auf verschiedenen Gesetzen zum **Schutz der Privatsphäre**.

Zum Beispiel:

- Europäische Menschenrechtskonvention, Artikel 8;
- Gesetz vom 8. Juni 2004 über die Meinungsfreiheit in den Medien, in seiner geänderten Fassung. Artikel 14.(1) besagt, dass jeder Recht auf Achtung seiner Privatsphäre hat;
- Gesetz vom 11. August 1982 über den Schutz der Privatsphäre, das jede vorsätzliche Verletzung der Privatsphäre anderer verbietet, indem mit einem beliebigen Apparat Aufnahmen von einer Person gemacht werden, die sich an einem nicht öffentlich zugänglichen Ort befindet, ohne deren Zustimmung. Dieses Gesetz untersagt auch die Veröffentlichung solcher Bilder.



Herausgeber: Service national de la jeunesse (SNJ)

Service national de la jeunesse - B.P. 707 L-2017 Luxembourg

www.snj.lu | www.bee-secure.lu



© 2025 Service national de la jeunesse (SNJ) – Initiative BEE SECURE

Die Creative-Commons-Lizenz dieser Publikation nachlesen :

www.creativecommons.org/licenses/by-nc-sa/4.0/deed.de

Ratgeber - Tipps und Tools

Im digitalen Zeitalter ein Vorbild sein

Für Lehrkräfte

01.2026

ISBN 978-2-919828-93-7

Elektronische Ressource

Initiiert von:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Durchgeführt von:



Service national
de la jeunesse



Kofinanziert von:



Kofinanziert von der
Europäischen Union