

KI im pädagogischen Alltag

Chancen nutzen, Grenzen erkennen,
Verantwortung beim Menschen lassen.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in Eurer Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Eine Kollegin nutzt ein frei verfügbares KI-System, um einen Entwicklungsbericht schneller zu formulieren. Dafür gibt sie Alter, familiäre Situation, Förderbedarf und auffälliges Verhalten eines Kindes ein. Gleichzeitig erzählt ein Jugendlicher stolz, dass er Hausaufgaben fast vollständig mit KI erledigt: „Warum soll ich das noch selbst machen?“ Im Team entsteht Streit: Die einen wollen KI möglichst konsequent nutzen, die anderen am liebsten ganz verbieten.

1 | Erst verstehen - noch nicht lösen / Leitfragen

- Welche zwei völlig unterschiedlichen Probleme stecken in diesem Fall?
- Wo liegen Chancen, wo konkrete Risiken - für Fachkräfte und für Kinder?
- Welche Informationen dürften aus Eurer Sicht niemals ungeprüft in ein externes KI-System gelangen?
- An welchen Stellen muss ein Mensch zwingend prüfen, entscheiden oder Verantwortung übernehmen?

2 | Die ersten 30 Minuten

- Was würdet Ihr der Kollegin unmittelbar raten?
- Wie würdet Ihr mit dem Jugendlichen sprechen, ohne KI zu verteufeln?
- Welche eine Regel braucht das Team sofort, auch wenn eine vollständige KI-Leitlinie noch fehlt?

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Welche Fähigkeiten dürfen Kinder und Jugendliche nicht an KI delegieren, wenn sie sich gesund entwickeln sollen?
- Wo könnte KI Euren pädagogischen Alltag tatsächlich sinnvoll entlasten?
- Wie gehen wir mit Ängsten im Kollegium um, ohne sie lächerlich zu machen oder zum Stillstand zu führen?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Formuliert Hinweise für eine erste KI-Leitlinie Eurer Einrichtung. Sie muss Chancen, Datenschutz, Prüfung und menschliche Verantwortung enthalten.

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot?

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

KI im pädagogischen Alltag

Chancen, Grenzen, Verantwortung

KI kann im pädagogischen Alltag entlasten, inspirieren und Struktur geben. Gleichzeitig braucht ihr Einsatz Klarheit, Haltung und Verantwortung. Kinder und Jugendliche brauchen Erwachsene, die Chancen erklären, Risiken benennen und selbst souverän bleiben.

Silke Müller

Gute
Bildung
für starke
Menschen.

*"Technik darf helfen.
Verantwortung
bleibt menschlich."*

PRAXISNAH. RELEVANT. GEMEINSAM WEITER.

1



Worum es geht

- **Ideenfindung und Vorbereitung**
Impulse für Projekte, Stunden und pädagogische Angebote.
- **Differenzierung und Sprachhilfe**
Texte anpassen, vereinfachen oder in andere Sprachen übertragen.
- **Struktur bei Dokumentation**
Formulierungsentwürfe und Gliederungen als Unterstützung.
- **Unterstützung im Alltag**
Zeit sparen, Routineaufgaben erleichtern und Freiräume schaffen.

2



Worauf wir achten müssen

- **Keine sensiblen Daten eingeben**
Personenbezogene Daten von Kindern, Jugendlichen und Kolleg:innen schützen.
- **Ergebnisse immer prüfen**
KI kann überzeugend klingen, ist aber nicht immer richtig.
- **Halluzinationen und Fehler einplanen**
Falsche oder erfundene Inhalte sind möglich und müssen erkannt werden.
- **KI ersetzt keine Beziehung und kein pädagogisches Urteil**
Die Entscheidung über den Einsatz liegt immer beim Menschen.

3



Was Kinder lernen müssen

- **KI verstehen**
Grundfunktionen, Möglichkeiten und Grenzen kennen.
- **Antworten hinterfragen**
Nicht alles glauben, sondern kritisch denken.
- **eigene Gedanken entwickeln**
Kreativität, Meinung und Urteilsfähigkeit stärken.
- **Chancen und Risiken benennen**
Sowohl Potenziale als auch mögliche Gefahren einschätzen können.

4



Drei Impulse für die Praxis

- **Klein anfangen**
Mit einem konkreten, überschaubaren Anwendungsfall starten.
- **transparent arbeiten**
Offen kommunizieren, wenn KI genutzt wird – im Team und gegenüber Kindern, Jugendlichen und Eltern.
- **menschliche Entscheidungshoheit behalten**
KI als Werkzeug nutzen – die pädagogische Verantwortung bleibt beim Menschen.

*Wissen
wirkt,
wenn wir
es gemeinsam
nutzen.*

Für Kita, Jugendhilfe, Schule und pädagogische Praxis.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

STARKE
MENSCHEN
FÜR EINE STARKE
DIGITALE
ZUKUNFT!



Cybergrooming & sexualisierte Gewalt

Beziehung schützen, Warnzeichen ernst nehmen, professionelle Hilfe früh einbinden.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in einer realen Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Ein zwölfjähriges Kind erzählt einer Erzieherin nebenbei von einem „15-Jährigen“, den es in einem Online-Spiel kennengelernt hat. Inzwischen schreiben beide auf Snapchat. Der Kontakt macht viele Komplimente, schickt gelegentlich Guthaben und bittet darum, dass „niemand von ihrer Freundschaft erfährt“. Nun fragt er nach einem privaten Bild. Das Kind möchte auf keinen Fall, dass die Eltern informiert werden, weil es Angst hat, dann sein Handy zu verlieren.

1 | Erst verstehen - noch nicht lösen/Leitfragen

- Welche Warnsignale erkennt Ihr - und welche Informationen fehlen Euch noch?
- Was braucht das Kind in diesem Moment emotional?
- Was dürft Ihr versprechen - und was gerade nicht?
- Wo liegt die Grenze zwischen vertraulichem Gespräch und Schutzauftrag?

2 | Die ersten 30 Minuten

- Welche Fragen stellt Ihr zuerst?
- Wen holt Ihr intern dazu?
- Welche Inhalte dokumentiert Ihr, ohne selbst problematische Bilder weiterzuverbreiten?
- Welche externe Beratung würdet Ihr aus dem Handout nutzen?

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Wie verhindert Ihr, dass das Kind sich schuldig fühlt?
- Wie könnte die Kommunikation mit Eltern gelingen, ohne das Vertrauen des Kindes unnötig zu zerstören?
- Was müsste präventiv passieren, damit Kinder solche Kontakte früher erkennen und Hilfe holen?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Entwerft einen einfachen Melde- und Schutzweg mit maximal 5 Stationen: Kind -> ... -> externe Hilfe.

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot? _____

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

*Das stärkste
Schutzprogramm
heißt Beziehung.*

Cybergrooming & sexualisierte Gewalt

Warnzeichen erkennen. Kinder schützen.

Cybergrooming beginnt selten mit einem Schockmoment. Es beginnt mit Aufmerksamkeit, Nähe und Vertrauen. Genau deshalb brauchen Kinder informierte Erwachsene, die Warnzeichen erkennen und ruhig handeln können.

Silke Müller

STARKE KINDER
BRAUCHEN
INFORMIERTE
ERWACHSENE.

1



Was ist Cybergrooming?

Gezielte Kontaktaufnahme im Netz mit sexueller Absicht. Häufig über Chats, Games, Social Media und Messenger.

2



Warnzeichen

- Geheimnisse mit Online-Kontakten
- Rückzug und Angst
- plötzliche Geschenke oder Guthaben
- Druck, Bilder zu schicken
- auffällige Stimmungsschwankungen

3



Was jetzt wichtig ist

- ruhig bleiben
- Kind ernst nehmen
- Beweise sichern
- nicht selbst mit Tätern diskutieren
- Hilfe holen

4



Anlaufstellen

- Polizei in akuten Fällen (Notruf 110)
- Jugendamt (vor Ort)
- Hilfe-Telefon Sexueller Missbrauch (0800 22 55 530, kostenfrei)
- Nummer gegen Kummer (116 111, kostenfrei)
- JUUUPORT (www.juuuport.de)

*Hinsehen.
Zuhören.
Handeln.*

Für sichere Aufwachsorte – online und offline. Mit Wissen, Achtsamkeit und einer starken Gemeinschaft können wir Kinder wirksam schützen.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

SICHERE
KINDER.
STARKE
GESELLSCHAFT.



Cybermobbing, Klassenchats & Deepfakes

Digitale Gewalt ernst nehmen, Verbreitung
stoppen, Schutz und Aufarbeitung verbinden.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in einer realen Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Montagsmorgen kommt eine 13-Jährige weinend in die Einrichtung. Seit dem Wochenende kursiert in einem Klassenchat ein KI-generiertes Nacktbild von ihr. Mehrere Jugendliche haben es weitergeleitet. Ein Kollege schlägt vor, sich das Bild „zur Beweissicherung“ schicken zu lassen. Das Mädchen möchte auf keinen Fall, dass jetzt „alle davon erfahren“. Später stellt sich heraus: Ein anderer Jugendlicher aus der Gruppe hat das Bild erstellt.

1 | Erst verstehen - noch nicht lösen/ Leitfragen

- Wer braucht jetzt zuerst Schutz - und warum?
- Welche Fehler könnten Erwachsene aus gutem Willen machen?
- Was muss dokumentiert werden, ohne die Darstellung weiterzuverbreiten?
- Wie trennt Ihr Schutz des betroffenen Kindes, rechtliche Klärung und pädagogische Aufarbeitung?

2 | Die ersten 30 Minuten

- Was sagt Ihr dem betroffenen Mädchen?
- Was tut Ihr mit dem Chat / den beteiligten Accounts?
- Wen informiert Ihr intern und extern?
- Was geschieht mit dem Jugendlichen, der das Bild erstellt hat?

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Wie verhindert Ihr, dass aus dem Fall ein öffentliches Tribunal wird?
- Welche Verantwortung tragen Weiterleitende und Zuschauende?
- Wie arbeitet Ihr mit der Gruppe weiter, wenn die akute Krise vorbei ist?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Schreibt eine 6-Zeilen-Notfallkarte für Mitarbeitende: „Wenn ein sexualisierter Deepfake auftaucht, dann ...“

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot? _____

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

Kinder und Jugendliche brauchen keine perfekten Antworten, sondern erwachsene Menschen die drankleben.

Cybermobbing, Klassenchats & Deepfakes

Wenn digitale Gewalt Alltag wird

Digitale Verletzungen verschwinden nicht mit dem Klingeln zur nächsten Stunde. Cybermobbing, entgleisende Klassenchats und KI-generierte Deepfakes treffen Kinder und Jugendliche oft mitten ins Herz und mitten in den Alltag.

Silke Müller

„Digitale Gewalt ist echte Gewalt.“

1

Woran wir Cybermobbing erkennen



- Beleidigung und Bloßstellung
- Ausschluss aus Gruppen
- Gerüchte und Fake-Profile
- Verbreitung peinlicher oder intimer Inhalte

2

Was Deepfakes so gefährlich macht



- Bilder oder Videos wirken echt
- Scham und Angst steigen
- sexualisierte Darstellungen können schnell verbreitet werden
- Betroffene fühlen sich ausgeliefert

3

Was Einrichtungen tun sollten



- klare Zuständigkeiten
- Vorfall dokumentieren
- Betroffene schützen
- Eltern einbeziehen
- externe Hilfe nutzen

4

Was Kinder hören müssen



- Du bist nicht schuld
- Hilfe holen ist kein Verrat
- nichts allein klären müssen
- wir stehen an deiner Seite

Wissen wirkt, wenn wir ins Handeln kommen.

Für starke Kinder. Für eine informierte, handlungsfähige und zugewandte pädagogische Praxis. Heute und morgen.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

SCHÜTZEN
STATT
BAGATELLISIEREN.



Fake News, Extremismus & Manipulation

Im Gespräch bleiben, Quellen prüfen, klare Grenzen setzen.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in einer realen Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Ein 15-Jähriger zeigt in der Gruppe immer wieder stark zugespitzte politische Videos. Einige Behauptungen sind nachweislich falsch, andere arbeiten mit Angst, Feindbildern und Entmenschlichung. Zwei weitere Jugendliche beginnen, die Inhalte zu teilen. Auf Widerspruch reagiert er mit: „Ihr glaubt halt alles, was die Mainstream-Medien euch erzählen.“ Im Team herrscht Unsicherheit: diskutieren, ignorieren oder sofort sanktionieren?

1 | Erst verstehen - noch nicht lösen/Leifragen

- Was ist hier pädagogische Herausforderung, was möglicherweise schon ein Schutz- oder Beratungsfall?
 - Wie bleibt Ihr im Gespräch, ohne menschenfeindliche Aussagen stehen zu lassen?
 - Welche Rolle spielen Emotion, Zugehörigkeit und algorithmische Verstärkung?
 - Wie unterscheidet Ihr Meinung, Desinformation und extremistische Ansprache?
-
-
-

2 | Die ersten 30 Minuten

- Welche Fragen würdet Ihr dem Jugendlichen stellen?
 - Welche Aussagen brauchen sofort Widerspruch oder Grenzsetzung?
 - Welche Fakten würdet Ihr gemeinsam prüfen - und wie?
 - Ab wann holt Ihr externe Fachberatung hinzu?
-
-
-

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Wie verhindert Ihr, dass ein Faktencheck zum Machtkampf wird?
- Welche Medienrituale könnten präventiv helfen?
- Wie schaffen wir Räume, in denen Jugendliche Widerspruch aushalten und ihre Position überprüfen können?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Entwickelt eine Mini-Routine für Quellenprüfung mit höchstens 5 Fragen, die Jugendliche selbst anwenden können.

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot?

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

Demokratie beginnt
auch dort, wo wir
lernen zu widersprechen.

Fake News, Extremismus & Manipulation

Orientierung im Informationsdschungel

Für viele Kinder und Jugendliche sind Social Media längst Nachrichtenquelle, Unterhaltungsraum und Weltdeuter zugleich. Umso wichtiger ist es, Manipulation zu erkennen, Widerspruch auszuhalten und Orientierung zu geben.

Silke Müller

KRITISCH DENKEN.
MENSCHLICH BLEIBEN.
GEMEINSAM
ZUKUNFT GESTALTEN.

1



Was junge Menschen heute erleben

- Emotionale Inhalte, die stark wirken
- Algorithmische Verstärkung
- Desinformation
- Extreme Positionen
- KI-generierte Bilder und Videos

2



Worauf wir achten müssen

- Wer sagt das?
- Woher kommt die Information?
- Wem nützt es?
- Was fehlt?
- Wie prüfe ich es?

3



Was Kinder und Jugendliche brauchen

- Gespräch
- Einordnung
- Widerspruch
- Faktencheck
- Erwachsene, die erreichbar bleiben.

4



Was Einrichtungen tun können

- Medienbildung fest verankern
- Über Propaganda sprechen
- Quellen prüfen üben
- Räume für Diskussion schaffen

Wissen
wirkt,
wenn wir
ins Handeln
kommen.

Für starke Kinder. Für informierte, selbstbewusste junge Menschen. Für eine offene und demokratische Gesellschaft. Heute und morgen.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

AUFKLÄREN
STATT
ÜBERLASSEN.

Recht, Abos & Haftung

Klare Zuständigkeiten schaffen, bevor aus einem Klick ein Konflikt wird.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in einer realen Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Ein 13-Jähriger nutzt in einer Jugendhilfeeinrichtung ein Tablet. Über eine App schließt er ein kostenpflichtiges Abo ab. Die Zahlung läuft über einen hinterlegten Account. Zwei Wochen später kommt die Rechnung. Niemand weiß genau, wer Apps installieren durfte, ob eine Kaufbestätigung aktiviert war und wer für das Gerät zuständig ist. Im Team fällt schnell der Satz: „Dann haftet eben die Einrichtung.“

1 | Erst verstehen - noch nicht lösen/Leitfragen

- Welche Tatsachen müsst Ihr zuerst klären, bevor Ihr irgendeine Haftung behauptet?
- Welche Rolle spielen Alter, Zustimmung, Account, Zahlungsmittel und interne Regeln?
- Welche Unterlagen oder Einstellungen würdet Ihr prüfen?
- Wo endet pädagogische Einschätzung und wo braucht es rechtliche Beratung?

2 | Die ersten 30 Minuten

- Wie stoppt Ihr weitere Kosten?
- Wer spricht mit dem Anbieter / Zahlungsdienst?
- Welche Stelle aus dem Handout könnte beraten?
- Wie sprecht Ihr mit dem Jugendlichen, ohne nur Schuld zu verteilen?

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Welche technischen Voreinstellungen hätten geholfen?
- Welche Regeln müssen Mitarbeitende kennen?
- Welche Situationen sollten dokumentiert werden?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Formuliert 5 klare Regeln für digitale Käufe, Apps und Zahlungsmittel in Eurer Einrichtung.

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot?

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

Verstehen.
Orientieren.
Gemeinsam
sicher handeln.

Recht, Abos & Haftung

Was Minderjährige dürfen – und wo Risiken liegen

Digitale Käufe, In-App-Angebote und Abos wirken harmlos und sind im Alltag schnell abgeschlossen. Umso wichtiger ist es, die rechtlichen Grundlagen zu kennen und in Einrichtungen klare Regeln zu haben.

Silke Müller

„Aufklärung
schützt oft früher
als der Streit im
Nachhinein.“

Die wichtigsten Aspekte im Überblick

PRAXISNAH. RELEVANT. GEMEINSAM WEITER.

1



Typische Risiken

- Ungewollte Abos
- In-App-Käufe
- Kostenpflichtige Dienste
- Nutzung fremder Accounts oder Zahlungsmittel

2



Rechtliche Orientierung

- Minderjährige sind nicht in jedem Fall voll geschäftsfähig.
- Zustimmung der Sorgeberechtigten kann nötig sein.
- Der Taschengeldparagraph greift nicht immer.
- Einzelfälle genau prüfen.

3



Was Einrichtungen klären sollten

- Zuständigkeiten
- Freigaben
- Geräteverwaltung
- Kommunikation mit Eltern
- Dokumentation

4



Wenn etwas passiert

- Ruhe bewahren
- Vorgang sichern
- Vertrag prüfen
- Verbraucherzentrale oder Rechtsberatung einbeziehen
- Gemeinsam Lösungen finden.

Wissen
wirkt,
wenn wir
ins Handeln
kommen.

Für starke Kinder. Für eine informierte, handlungsfähige und zugewandte pädagogische Praxis. Heute und morgen.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

KLARHEIT
SCHAFFT
SICHERHEIT.

Hacking, Phishing & Identitätsdiebstahl

Digitale Sicherheit als pädagogische Alltagsroutine verstehen.

**SILKE
MÜLLER**

VERSTEHEN.
HANDELN.
VERANKERN.

Euer Auftrag: Arbeitet nicht auf eine perfekte Musterlösung hin. Einigt Euch auf ein Vorgehen, das in einer realen Einrichtung funktionieren würde. Nutzt das Handout als Wissensquelle.

Der Fall

Ein Jugendlicher lädt einen vermeintlichen Key Generator herunter, um kostenlos an ein Spiel zu kommen. Kurz danach wird sein Account übernommen. Über sein Profil gehen Nachrichten an Freunde, ein Passwort funktioniert plötzlich nicht mehr und auf dem Gerät sind weitere Zugangsdaten gespeichert. Der Jugendliche schämt sich und bittet: „Bitte sagt niemandem, wie blöd ich war.“

1 | Erst verstehen - noch nicht lösen/Leitfragen

- Welche Schäden könnten bereits entstanden sein?
- Welche Konten, Geräte oder Personen könnten noch betroffen sein?
- Wie verhindert Ihr, dass Scham die Hilfe verzögert?
- Welche Informationen müssen zuerst gesichert bzw. geändert werden?

2 | Die ersten 30 Minuten

- Welche Passwörter ändern?
- Wo Zwei-Faktor-Authentifizierung aktivieren?
- Welche Geräte prüfen lassen?
- Welche Kontakte informieren?
- Wann braucht es IT-Fachhilfe, Plattform-Support oder Polizei?

Was nehmen wir mit - und was ändern wir?

Wichtig: Ihr müsst nicht alles lösen. Entscheidend ist, dass Ihr Zuständigkeiten, Grenzen und nächste Schritte klar benennen könnt.

3 | Jetzt wird es schwieriger

- Welche typischen Versprechen („kostenlos“, „Hack“, „Cheat“, „Key“) machen Jugendliche anfällig?
- Welche Sicherheitsroutinen können pädagogische Teams vermitteln, ohne Technikunterricht zu halten?
- Was müsste bei einem kompromittierten Einrichtungsgerät zusätzlich passieren?

4 | Transfer in Eure eigene Einrichtung

Hätten wir heute einen klaren Ablauf?

Wer wäre bei uns die erste Ansprechperson?

Wo endet unsere Kompetenz?

Welche externe Hilfe muss griffbereit sein?

Konkrete Gruppenaufgabe: Erstellt eine 5-Punkte-Notfallroutine „Account gehackt - was jetzt?“ für Jugendliche und Mitarbeitende.

Unser Ergebnis für die Praxis

Eure Aufgabe für diese Seite: Verdichtet Eure Diskussion. Diese Seite ist Euer gemeinsames Ergebnis und die Grundlage für die 3-Minuten-Präsentation im Plenum.

5 | Unsere drei Take-Home-Punkte

Das müssen wir wissen.

Das müssen wir können.

Das sollten wir in unserer Einrichtung verändern.

Wenn wir nur eine Sache morgen ändern könnten, wäre es:

Wer muss dafür bei uns ins Boot?

Für die Präsentation im Plenum:

3 Minuten: 1 Aha-Moment - 1 Handlungsschritt - 1 Veränderungspunkt.



SILKE MÜLLER

MENSCHEN STÄRKEN.
DIGITALE WELTEN GESTALTEN.
GEMEINSAM VERANTWORTUNG ÜBERNEHMEN.

Wissen
schützt.
Gemeinsam
mehr erreichen.

Hacking, Phishing & Identitätsdiebstahl

Digitale Sicherheit praktisch erklärt

Manchmal beginnt ein Vorfall mit einer kleinen Unachtsamkeit: einem falschen Link, einem geteilten Passwort oder einem vermeintlich kostenlosen Download. Für Kinder, Jugendliche und Einrichtungen kann das schnell große Folgen haben.

Silke Müller

„Digitale Sicherheit
ist kein Technikthema allein.
Sie ist Beziehung,
Aufklärung und Routine.“

1 Typische Gefahren



- Phishing-Nachrichten
- schwache Passwörter
- fremde Zugriffe auf Accounts
- dubiose Downloads und Key Generatoren

2 Warnzeichen



- unbekannte Login-Meldungen
- seltsame Nachrichten an Kontakte
- plötzlich veränderte Kontodaten
- gesperrte Zugänge
- ungewöhnliche Käufe

3 Sofortmaßnahmen



- Passwörter ändern
- Zwei-Faktor-Authentifizierung aktivieren
- Gerät prüfen
- betroffene Kontakte informieren
- Hilfe holen

4 Was wir vorbeugend tun können



- sichere Passwörter
- keine Zugangsdaten teilen
- Updates ernst nehmen
- Downloads prüfen
- ruhig über Fehler sprechen

*Sicherheit
beginnt
im Alltag.*

Für starke Kinder. Für eine informierte, handlungsfähige und zugewandte pädagogische Praxis. Heute und morgen.



VERSTEHEN



HANDELN



GEMEINSAM MEHR ERREICHEN

STARKE
MENSCHEN
FÜR EINE STARKE
DIGITALE
ZUKUNFT.