Leitfaden Datensicherheit BSB

Datenschutz und Datensicherheit (Begriffsdefinition)

Datensicherheit ist im Wesentlichen durch die Aspekte «Zutrittsschutz» (Schloss an der Tür), «Zugangsschutz» (Passwort) und «Zugriffsschutz» (Berechtigung, eine Datei öffnen zu dürfen) definiert. Weiterhin gehört die Transportsicherung (Verschlüsselung) dazu.

Datenschutz hingegen ist primär der Schutz der Persönlichkeit in Bezug auf den Umgang mit deren persönlichen bzw. personenbezogenen Daten. Voraussetzung für einen funktionierenden Datenschutz ist neben organisatorischen Aspekten auch die Datensicherheit.

Datensicherheit im Lehrberuf

Lehrerinnen und Lehrer hatten immer schon besondere Sorgfaltspflichten zu beachten, zum Beispiel:

– bei Lernendenakten und Zeugnissen,
– beim Austausch mit Kollegen,
– bei Eltern- oder Lehrbetriebsanfragen zu ihrem Lernenden,
– bei Datenanfragen von Behörden oder Fachstellen
– bei der Verwendung von Unterrichtsmaterial.

Mit der elektronischen Kommunikation akzentuieren sich die Sorgfaltspflichten, weil Datenlecks rasch sehr gravierende Auswirkungen haben können.

Die gesamte Kommunikation von Lehrpersonen mit Lernenden, Lehrbetrieben, Eltern, Fachstellen und Behörden sowie zwischen dem schulischen Personal soll ausschliesslich nur über die von der Schule dafür vorgesehenen sicherheitstauglichen Systeme z.B. mit E-Mail-Verschlüsselungen und die dafür zugelassene Software erfolgen.

Aus diesem Grunde ist von einer Kommunikation via Facebook oder WhatsApp bzw. ähnlichen kommerziellen Diensten abzuraten. Ausnahmen bilden hier allenfalls die zurzeit sicheren Dienste wie SIMSme, Threema oder bleep (SMS-Dienst).

Verhalten von Lehrpersonen im Internet

Für die gesamte Kommunikation von Lehrpersonen im Internet empfiehlt sich folgender Verhaltenskodex:

– So wie Sie sich auch im täglichen beruflichen Leben als Lehrperson geben, so sollten Sie auch online kommunizieren – nicht zu persönlich und freundschaftlich. Lehrpersonen werden in Social Media nie nur privat, sondern immer auch als öffentliche Berufsperson mit einer gewissen Vorbildfunktion wahrgenommen, sobald ihre Identität bekannt ist. Sie stehen mit ihrem Erziehungsauftrag in einer besonderen (auch dienstrechtlichen) Verantwortung. Lernende (inklusive deren Eltern) stehen in einem Abhängigkeitsverhältnis zu Lehrpersonen.
– Bei jedem Auftritt ist der Grundsatz der Datensparsamkeit zu beachten. Datenschutz für Fotos oder persönliche Daten gilt besonders auch im Internet. Das heisst: Persönliche Daten sind unbedingt mit ausreichenden Passwörtern zu schützen. Zur Publikation von Fotos und persönlichen Angaben auf öffentlich einsehbaren Seiten (z.B. Schulwebseiten, Social-Media-Plattformen) ist vorgängig die ausdrückliche Einwilligung der Betroffenen (inkl. der Erziehungsbevollmächtigten) einzuholen.

Verfasser: M. Woog
Genehmigt: J. Coviello

- Seien Sie zurückhaltend mit allzu schnellen Aktivitäten. Ein «Zurückholen» von Geschriebenem oder von Fotos und Videos aus dem Internet ist kaum mehr möglich. Die Konsequenzen können schlimmstenfalls bis zum Verlust der Anstellung und zur völligen sozialen Ausgrenzung führen.
- Das Internet vergisst nicht! Beachten Sie, dass auch viele Jahre zurückliegende Einträge in den Netzwerken oder gar in Suchmaschinen sichtbar sein können. Die eigenen Profile sollten also von Zeit zu Zeit aufgeräumt werden.
- Thematisieren Sie die Verwendung von sozialen Netzwerken im Unterricht. Klären Sie Lernende darüber auf, wie Sie den Umgang mit Netzwerken pflegen und warum Sie möglicherweise online keine Einzelkontakte mit Lernenden (oder Eltern) pflegen wollen. Machen Sie auf die rechtlichen Konsequenzen von Missbräuchen aufmerksam.
- Weil selten alle Lernende auf ungeschützten Plattformen kommunizieren (dürfen) oder von zu Hause gar keinen Zugang haben, sind öffentlich zugängliche Social Media auch für «private» Inhalte nicht zu empfehlen. Behandeln Sie alle Kontaktanfragen Ihrer (ehemaligen) Lernenden gleich. Entweder Sie nehmen diese an oder lehnen diese ausnahmslos ab.
- Da es nach wie vor Lernende ohne privaten PC oder Internetzugang gibt, sollten Sie sich, bevor Sie soziale Netzwerke in Ihren Unterricht einbauen, sich über allfällige Regelungen an Ihrer Schule informieren. Insbesondere welche Plattformen werden von staatlichen Einrichtungen für Bildungszwecke zur Verfügung gestellt?

Lehrperson als Privatperson im Internet

Wie sollte ich mich als Privatperson im Internet verhalten?

Wenn man einige Verhaltensregeln beherzigt, ist der Umgang mit dem «privaten» Internet relativ unkompliziert.

- Keine Lernenden als Freunde hinzufügen bzw. sich nicht von ihnen als Freund hinzufügen lassen, sofern nicht alle Lernenden einer Klasse diese Möglichkeit haben.
- Keine Teilnahme an Social-Media-Gruppen, insbesondere nicht von Lernenden aus der eigenen Schule, besser generell nicht von Lernenden.
- Kein Austausch von privaten Informationen mit einzelnen Lernenden via kommerzielle Internetplattformen, insbesondere auch nicht von Fotos.

Persönliche Verantwortung/rechtliche Risiken für Lehrpersonen

Für eine urheberrechtskonforme Mediennutzung im «normalen» Unterricht und das entsprechende Beschaffen von Material, Bildern etc. trägt jede Lehrperson die persönliche Verantwortung. Die Schule stellt zur Verfügung: geschützte dienstliche E-Mail-Adressen, der geschützte Zugang auf dienstliche Online-Plattformen sowie einen regelmässiger IT-Support für die Schule, um die sensiblen Schuldaten vor jeglichem Fremdzugriff zu schützen.

Einhalten des Urheberrechts

Grundsätzlich sind bei jeglicher Nutzung von medialen Inhalten im Unterricht bzw. in schulischen Veranstaltungen die geltenden urheberrechtlichen Bestimmungen einzuhalten.

Der Einsatz digitaler Schulbücher setzt eine entsprechende Lizenz voraus. Ebenso gilt dies für digitale Arbeitsbögen und andere Arbeitsmaterialien für den Unterricht, wenn diese auf Verlagsplattformen oder Lernplattformen zur Verfügung gestellt werden. Zu beachten ist, dass auch Lernmaterialien mit offenen Lizenzen die Arbeit des Autors/der Autoren urheberrechtlich schützen, aber offen sind für eine Bearbeitung durch weitere Nutzer. Die entsprechenden Dokumente dürfen zwar frei verwendet werden, die Autoren verlangen aber, dass deren Namen genannt werden.

Begrenztes Kopieren und Scannen von Büchern, Fachartikeln, etc. ist urheberrechtlich zulässig, wenn die nationalen Regelungen eingehalten werden. In der Schweiz dürfen veröffentlichte Werke zum Eigengebrauch verwendet werden. Als Eigengebrauch gilt jede Werkverwendung von Lehrpersonen für den Unterricht in der Klasse. Sobald jedoch eine Vorführung nicht mehr zur Schulung, sondern vielmehr zur Unterhaltung erfolgen soll oder sofern ein Werk wie beispielsweise ein Theaterstück gegenüber Dritten vorgeführt werden soll, ist das Urheberrecht des Autors strikt zu beachten.

Vorsicht ist auch bei der Nutzung von Videos auf Plattformen wie Youtube im Unterricht geboten. Zulässig ist hier der Klick auf den jeweiligen Link, um das gewählte «Medium» im Unterricht einzusetzen, vorausgesetzt das Video ist nicht rechtswidrig. Hier ist davon auszugehen, dass der Schulungszweck überwiegt. Nicht zulässig ist es jedoch, eine Kopie des gesamten Werkes anzufertigen und diese im Unterricht zu nutzen, da hier davon ausgegangen werden muss, dass dann der Unterhaltungszweck überwiegt.

Es empfiehlt sich, vorher bei den Verlagen und Online-Plattformen über die AGB zu informieren, damit Lehrpersonen nicht unvermutet mit einer Klage eingedeckt werden.

Sorgfaltspflichten bei Recherchen durch Lernende im Internet

Eine Aufforderung an die Lernenden, für schulische Aufgaben im Internet zu recherchieren, sollte von den notwendigen Informationen begleitet sein: Persönlichkeitsrechte, das Urheberrecht, AGB und datenschutzrechtliche Zusammenhänge sollten den Lernenden bekannt gemacht werden und auch, wo ethische Grenzen gesetzt sind. Die Lernenden sind dazu anzuleiten, keine Plagiate zu erstellen, sondern die Quellen genau anzugeben. Eins-zu-eins-Kopien aus dem Internet sollen thematisiert werden. Neben den gesetzlichen Schranken sollen mit den Lernenden auch die moralischen und ethischen Grenzen von Internetinhalten thematisiert und erarbeitet werden. Dazu gehört das Wissen, welche Grenzen die Schule für den Einsatz privater mobiler Geräte insbesondere auch in Prüfungssituationen zieht.

Rechtsverstösse in der digitalen Welt, ob in Unkenntnis oder aus Leichtfertigkeit, können im schlimmsten Falle zu rechtlichen Klagen führen und sehr teuer werden. Hier ist es auch wichtig, im Blick zu haben, dass der Urheber seinen Sitz nicht immer im gleichen Land wie die Schule hat und deshalb schwierig zu klärende Fragen auftauchen können, da in Ländern unterschiedliche Rechtssysteme gelten und die ausländischen Bestimmungen gestützt auf das internationale Privatrecht bei der Verwendung des Internets auch bei uns zur Anwendung gelangen können.

D5.6-02B
Erstellung 13.08.2020
Revision –

Cybermobbing

In aller Regel schreiten staatliche Stellen nicht von sich aus ein, wenn Lernende oder Lehrpersonen Opfer von Cybermobbing oder auch Hacking bzw. Datenverlust werden. Die Strafverfolgungsbehörden haben nämlich in den seltensten Fällen Kenntnis von diesen Delikten. Das Opfer oder eine für das Opfer zuständige Person muss zuerst selber aktiv werden, um so eine straf- und/oder zivilrechtliche Verfolgung in Gang zu setzen. Betroffenen ist zu empfehlen, unverzüglich die Beweise mittels Bildschirmfoto oder eines Ausdrucks zu sichern. Einen garantierten Rechtsschutz durch den Arbeitgeber gibt es nicht.

Zum Cybermobbing gehört u.a. auch das ungefragte Aufschalten von Bildern oder Filmen zum Beispiel aus dem Unterricht, die andere Menschen der Lächerlichkeit preisgeben. Genauso sind beleidigende oder blossstellende Kommentare und Ratings Formen des Cybermobbings.

Für den Fall, dass Lernende oder schulisches Personal auf öffentlich zugänglichen Internetplattformen andere Mitglieder der Schulgemeinschaft oder andere Menschen beleidigen oder anderweitig angreifen, empfehlen sich folgende Vorgehensweisen:

Sofortmassnahmen

– Überlegen Sie zuerst und handeln Sie dann rasch.
– Notieren Sie sich die entsprechenden Links und Internetadressen, machen Sie ein Bildschirmfoto, dokumentieren Sie alles.
– Löschen Sie mögliche anfeindende Kommentare oder Bilder aus Ihrem eigenen Profil, um Trittbrettfahrer abzuhalten, in die Diskussion einzusteigen. Blockieren Sie nach Möglichkeit Nutzer, die Ihnen in den Netzwerken zu nahe treten.

Information

– Informieren Sie die Schulleitung und als Fachlehrperson die Klassenlehrperson.
– Fragen Sie nach Beratung durch externe Fachstellen.
– Bitten Sie um eine sofortige Besprechung des weiteren Vorgehens mit der Schulleitung.

Problemlösung

– Suchen Sie mit Unterstützung einer Drittperson (Schulleitung, Beratungsstelle, Mediation) das direkte, persönliche Gespräch mit den betreffenden Lernenden (und deren Eltern).
– Versuchen Sie, den Grund des Ärgers aufzuspüren. Machen Sie die rechtlichen Konsequenzen klar.
– Verlangen Sie die Löschung der Einträge, sofern das technisch möglich ist.
– Vereinbaren Sie das zukünftige Verhalten bei Unzufriedenheit.
– Erstatten Sie in Absprache mit der Schulleitung Anzeige bei der Polizei.

Anzeigepflicht

In der Schweiz eine Pflicht zur Gefährdungsmeldung bei der Kinder- und Erwachsenenschutzbehörde (KESB) und in einzelnen Kantonen bei der Jugendanwaltschaft, wenn Lernende von Übergriffen oder Versuchen dazu betroffen sind. Bei Cybermobbing gegen Lehrpersonen besteht für Zeugen keine Meldepflicht.

Auf keinen Fall tun

– Sich schämen und niemandem etwas sagen.
– Direkt im Internet reagieren.
– Allein das Gespräch suchen und Druck ausüben.

– Bagatellisieren, wegschauen und ausharren.
– Freunde für einen «Shitstorm» gegen die betreffende Person mobilisieren, um viele negative Bemerkungen auf der Seite des Täters einzutragen.
– Eine Lehrperson darf ihre persönlichen Rechte selbstständig wahrnehmen. Trotzdem empfiehlt sich vor einer Anzeige bei der Polizei eine Rücksprache mit der Schulleitung.

Datenschutz, Datensicherheit

Informationen über Lernende unterliegen auch auf Schulservern der Vertraulichkeit. Bei interdisziplinären Teams ist zur eigenen Entlastung darauf zu achten, dass nicht immer alle über alles informiert werden. Insbesondere in schwierigen Situationen, u.a. bei Meldungen wegen Integritätsverletzungen in Familien, ist der Kreis von Mitwissenden klein zu halten. Allenfalls sind die Daten wie in Fallbesprechungen zu anonymisieren. Die Datenaufbewahrung auf Schulservern sollte deshalb eine Differenzierung der Nutzungsberechtigungen erfolgen.

Für die Zusammenarbeit mit externen Fachstellen oder speziellen Einrichtungen (Heime o. ä.) sollten der Datenaustausch und allfällige Zugriffsmöglichkeiten genau geregelt sein.

Lagern und Nutzen von Medien oder Lernmaterial von Verlagen auf schulischen Servern

Das Kopieren und Nutzen von urheberrechtlich relevantem Material unterliegt urheberrechtlich strengen Regeln. Die jeweiligen nationalen Regelungen sind jedoch so gestaltet, dass Lehrpersonen einen praktikablen Spielraum haben, um Auszüge aus Schulbüchern und anderen Lernmaterialien für den Einsatz in ihrem Unterricht zu kopieren – auch digital. Nicht zulässig ist allerdings, auf schulischen Servern urheberrechtlich geschütztes Material zum Beispiel aus Verlagen in grossem Umfang abzulegen.

Clouds und Server

Eine Schule kann das Speichern von Informationen Dritten übertragen, also auslagern – aber nur unter Berücksichtigung der datenschutzrechtlichen Anforderungen. Solange keine personenbezogenen oder sonst zu schützenden Daten abgelegt werden, ist gegen Cloud-Lösungen grundsätzlich nichts einzuwenden. Je nach gesetzlicher Regelung können allenfalls Cloud-Lösungen verwendet werden, sofern mit dem Anbieter ein datenschutzkonformer Vertrag abgeschlossen wird oder datenschutzkonforme allgemeine Geschäftsbedingungen vereinbart werden. Zuvor gilt es zu klären, welche Anbieter vom Arbeitgeber zugelassen sind.

Sind sensible Personendaten wie Informationen über Zeugnisnoten oder die Gesundheit betroffen, sind besondere Sicherheitsmassnahmen erforderlich, namentlich die Verschlüsselung dieser Daten (gilt auch für E-Mails). Von einer Auslagerung auf im Ausland stationierte Server sollte in diesen Fällen abgesehen werden.

Geräte zu Hause und unterwegs

Bei der Nutzung des Privat-PCs zur Verarbeitung von schulischen Daten gelten grundsätzlich die gleichen Standards wie an der Schule. Im Wesentlichen beinhalten diese einen sicheren und vor fremden Zugriffen geschützten PC. Folgende Aspekte sind in jedem Fall dabei zu berücksichtigen:

– Verschlüsselter Datenträger, um den Zugriff wie auch den Zugang zu sensiblen Daten zu verhindern.
– Antivirenprogramm, um den Angriff von Viren und im begrenzten Umfang von Trojanern abfangen bzw. abwehren zu können.
– Sicheres Passwort, denn ausser den berechtigten Lehrpersonen darf niemand Zugang zu diesen Daten erlangen.
– Sicherer Zugang zum Schulserver.
– Sicherer USB-Stick, um Daten gegebenenfalls vom Schulsystem zum Privatsystem transportieren zu können.

Im Umgang insbesondere mit sensiblen Schuldaten nicht geeignet bzw. nicht zulässig sind:

– Kommunikation via WhatsApp oder ähnlichen Programmen.
– Ablage von sensiblen Daten in der Dropbox oder anderen von der Schule nicht freigegebenen Cloud-Systemen.
– Standard-E-Mail ohne Verschlüsselung.
– Unverschlüsselte Festplatten (Zugangssicherung, Reparaturen). Zu beachten ist, dass auch eine verschlüsselte Festplatte nach dem Hochfahren während des gesamten Betriebs des Computers sichtbar ist!
– Automatische Anmeldung am PC oder Notebook ohne Eingabe eines Passwortes.

Reparatur von PC-Systemen

Ein Computersystem mit Schülerdaten darf nicht ohne weiteres bei dem örtlichen PC-Händler zur Reparatur gegeben werden, sofern keine zusätzlichen Massnahmen und Vereinbarungen bezüglich Datensicherheit getroffen worden sind. Einem IT-Experten ist es fast immer möglich, direkt auf alle Daten zuzugreifen. Dies gilt für alle Geräte, also sowohl für beruflich genutzte Privat-PCs von Lehrpersonen als auch für dienstliche Geräte.

Für eine Reparatur gibt es somit drei Möglichkeiten:

– Während des gesamten externen Reparaturvorgangs anwesend bleiben (nur computerkundige Personen).
– PC zu Hause/in der Schule reparieren lassen, Passwörter selber eingeben und darauf achten, dass der PC nicht manipuliert wird (Keylogger, Datenversand etc.).
– Die Festplatte ist mit einer separaten und komplett verschlüsselten Datenpartition ausgerüstet und das Passwort ist dem Dienstleister nicht bekannt.

D5.6-02B
Erstellung 13.08.2020
Revision –

Private E-Mail-Accounts von Lehrpersonen

Wenn Lehrpersonen oder Mitglieder von Schulbehörden Informationen aus eigenem Entscheid von ihrer schulischen an ihre private E-Mail-Adresse weiterleiten, sind diese Personen für die Datensicherheit haftbar.

Insbesondere ist sicherzustellen, dass keine automatische Weiterleitung der Schuladressen zu privaten E-Mail-Konten erfolgen, da die Absender im falschen Glauben gelassen würden, ihre E-Mail werde nur über eine sichere Umgebung geleitet. Sobald jedoch eine E-Mail unverschlüsselt über einen privaten Mailserver (gmx, gmail etc.) geleitet wird, ist diese in den Zugriff Dritter gelangt, was nicht erlaubt ist.

Quellenangabe: Dieser Leitfaden besteht aus relevanten Abschnitten aus dem "Leitfaden Daten-Sicherheit Für Lehrpersonen und Schulleitungen" (VBE, GÖD, LCH) (https://www.vbe.de/service/leitfaden-social-media/)