LEITFADEN DATEN-SICHERHEIT

FÜR LEHRPERSONEN UND SCHULLEITUNGEN

VBE
Verband Bildung und Erziehung
Deutschland
www.vbe.de

GÖD
Gewerkschaft Öffentlicher Dienst
Österreich
www.goed.at

LCH
Dachverband Lehrerinnen
und Lehrer Schweiz
www.lch.ch

www.medien-datensicherheit-schulen.info

Herausgeber:

**Gewerkschaft Öffentlicher Dienst –
Gewerkschaft Pflichtschullehrerinnen
und Pflichtschullehrer (göd aps)
Schenkenstraße 4/5
A-1010 Wien
T. +43 153 45 44 35
F. +43 153 45 44 52
kontakt@pflichtschullehrer.at
www.pflichtschullehrer.at**

**Dachverband Lehrerinnen
und Lehrer Schweiz (LCH)
Kulturpark
Pfingstweidstrasse 16
CH-8005 Zürich
T. +41 44 315 54 54
F. +41 44 311 83 15
www.lch.ch**

**Verband Bildung und Erziehung (VBE)
Behrenstraße 23/24
D-10117 Berlin
T. +49 30 726 19 66 0
F. +49 726 19 66 19
bundesverband@vbe.de
www.vbe.de**

**Redaktion:
Jürg Brühlmann, Rolf Busch, Mira Futász,
Martin Höflehner**

**Beratung und Mitarbeit:
Peter Hofmann, Geschäftsführer
Fachstelle Schulrecht, Goldach (Schweiz),
www.schulrecht.ch
Thomas Merz, Medienpädagoge,
Prorektor, Pädagogische Hochschule
Thurgau (Schweiz)
Fritz Tanner, Datenschutzbeauftragter
Kanton Thurgau (Schweiz)
Thomas Floß, Berater für Datenschutz
und Informationssicherheit (Deutschland)**

**Gestaltung:
Integral Lars Müller, Zürich**

**Realisation:
Peter Waeger, Baden**

**Druck:
dbb verlag**

**Stand:
November 2015**

1. Auflage

DATENSICHERHEIT: SICHERHEIT UND SCHUTZ FÜR LEHRPERSONEN UND SCHULEN GEWÄHRLEISTEN!

Die stürmische Entwicklung der Informationstechnologien und die rasante Einbindung aller Lebensbereiche ins Internet machen um die Schule keinen Bogen. Dem Bildungs- und Erziehungsauftrag gerecht zu werden, schließt daher ein, auch die entstehenden digitalen Daten über Schülerinnen und Schüler, über Lernergebnisse, über Ereignisse in der Schule sensibel zu behandeln und dem berechtigten Schutzbedürfnis aller an Schule Beteiligten zu entsprechen.

GÖD-APS, LCH und VBE sind beunruhigt, dass Lehrpersonen und Schulleitungen von den Arbeitgebern keine ausreichenden Voraussetzungen zu Datensicherheit und Datenschutz in der schulischen Arbeit erhalten. Eine erfolgreiche Schule muss eine datensichere, datengeschützte Schule sein. Daraus folgen klare Verantwortlichkeiten insbesondere für Arbeitgeber und Schulträger/Schulerhalter, damit Schulleitungen und Lehrpersonen ihrer Verantwortung nachkommen können.

GÖD-APS, LCH und VBE legen daher diesen Leitfaden zugleich als Hausaufgabe für die Arbeitgeber und Schulträger/Schulerhalter vor. Weder die «Hardware» Schule noch die «Software» Schule passen aktuell zu den Erwartungen der Politik, dass Schule kompetente Medienerziehung, digitales Lernen und die Einbindung in digitales Verwaltungshandeln zu meistern hat. Mehrheitlich ist die IT-Ausstattung der Schulen der Zeit hinterher. Den Lehrpersonen werden nicht nur zeitgemäße Hardware und die notwendige Fort- und -weiterbildung verweigert. Dass überdies von den Lehrpersonen erwartet wird, mit Privatgeräten den dienstlichen Auftrag zu erfüllen und das volle Risiko selbst zu tragen, ist vollkommen inakzeptabel.

GÖD-APS, LCH und VBE fordern:

1. Arbeitgeber und Schulträger/Schulerhalter müssen allen Schulen eine zeitgemäße IT-Ausstattung bereitstellen. Jede Schule – unabhängig von ihrem sozialen Umfeld – muss den «digitalen» Bildungs- und Erziehungsauftrag ausfüllen können.

2. Arbeitgeber und Schulträger/Schulerhalter müssen allen Schulen den Zugang zum schnellen Internet ermöglichen, einen grundsätzlich geschützten dienstlichen Datenverkehr, Datensicherung und Datenschutz gewährleisten und IT-Support als Selbstverständlichkeit für alle Schulen bereitstellen.

3. Lehrpersonen müssen zur Erfüllung ihres dienstlichen Auftrags über die notwendige Hard- und Software verfügen und diese sind von Arbeitgeber sowie Schulträger/Schulerhalter bereitzustellen.

4. Der Arbeitgeber muss systematische und passgenaue Lehreraus-, -fort- und -weiterbildung in ausreichendem Maße anbieten und die kostenfreie Teilnahme daran ermöglichen.

5. Der Arbeitgeber muss den Lehrpersonen finanzielle und zeitliche Ressourcen für Weiterbildung und Beratung für digital basiertes Unterrichten zur Verfügung stellen.

VBE
Verband Bildung und Erziehung
Deutschland
www.vbe.de

GÖD
Gewerkschaft Öffentlicher Dienst
Österreich
www.goed.at

LCH
Dachverband Lehrerinnen
und Lehrer Schweiz
www.lch.ch

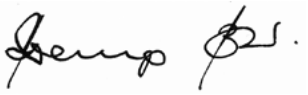
6. Der Arbeitgeber muss klare gesetzliche Grundlagen entwickeln, damit Lehrpersonen ihrem «digitalen» Bildungs- und Erziehungsauftrag geschützt nachkommen können.

7. Der Arbeitgeber muss Ressourcen und Beispiele zur Verfügung stellen, damit an jeder Schule ein Datensicherheitskonzept entwickelt werden kann, das gemeinsam von der gesamten Schulgemeinde getragen und umgesetzt wird.

Berlin, Wien, Zürich im Oktober 2015

Udo Beckmann, Bundesvorsitzender VBE

Paul Kimberger, Vorsitzender Pflichtschullehrer/innengewerkschaft GÖD



Beat W. Zemp, Zentralpräsident LCH

VORWORT

Mit der Bildungs- und Erziehungsarbeit an Schulen werden laufend Daten erzeugt. In Vor-IT-Zeiten wurden diese Daten in Klassenbüchern, Notizheften, Protokollen, Beurteilungen und Zeugnissen handschriftlich oder per Schreibmaschine festgehalten. Es wurden vielleicht einige Kopien angefertigt und irgendwann wurde alles in Schränken, im Schulkeller oder im Schulamt archiviert. Einblick durfte nur per Antrag erfolgen. Doch nun werden in der schulischen Arbeit Daten zunehmend digital erzeugt, abgespeichert, transportiert und aufbewahrt. Die bisher nur in Papierform erstellten Daten sind durch die Digitalisierung viel umfassender und untereinander verknüpfbar. Zudem sind sie nun sehr viel mehr Personen zugänglich und dadurch viel schwieriger zu kontrollieren. Mit diesen Tatsachen und den möglichen Konsequenzen müssen sich alle Beteiligten befassen. Die kleinste Fahrlässigkeit oder auch unzureichende Sicherheitsstandards der eingesetzten Hard- und Software können unabsehbare Folgen haben, sowohl für betroffene Schüler/innen, Eltern und Familien als auch für die Lehrpersonen.

Appelle der Politik an Schulen, sich für den Einsatz von IT zu öffnen, sind nur die eine Seite der Medaille. Mangels staatlicher Finanzierung übernehmen immer häufiger Sponsoren teilweise oder ganz die IT-Ausstattung von Schulen. Damit geht einher, dass die zu schützenden Schuldaten durch private Unternehmen «übernommen» und mit zweifelhafter Sicherheit irgendwo im Ausland in einer privaten Cloud gespeichert werden können. Unternehmen mit Niederlassung in den USA können von ihren Behörden gezwungen werden, Daten offenzulegen, auch wenn sie außerhalb der USA gelagert werden.

Dass Daten einen großen Wert haben können, zeigt das Bonmot, wonach Daten das Erdöl des 21. Jahrhunderts seien. Es genügt ein Blick in die AGB von Internetunternehmen, um aufzuzeigen, welches starke Interesse an der Weiternutzung etwaiger Daten der Nutzer besteht und welcher Druck mit immer wieder wechselnden Geschäftsbedingungen ausgeübt wird, um über die eingesetzten Tools von den Nutzern, ohne dass sie es wirklich merken, möglichst viele Daten zu erhalten. Die sich stetig wandelnde Technologie birgt für die Schülerinnen und Schüler, die Lehrpersonen und die Eltern die große Gefahr, dass deren Persönlichkeitsrechte massiv verletzt werden – mit unabsehbaren Folgen.

Sichere Daten und einen sichereren Umgang mit Daten wollen alle, die an Schulen arbeiten oder mit Schulen zu tun haben. Doch ist das bloße Wollen eindeutig zu wenig, um tatsächlich mit den hochsensiblen Daten – und das gilt ausnahmslos für alle anfallenden schulischen Daten – verantwortungsbewusst umzugehen. Mit der Einforderung des Engagements von Lehrpersonen und Schulleitungen ist es nicht getan. Auch die Schulträger/Schulerhalter müssen für Datenschutz und Datensicherheit aktiv Verantwortung übernehmen und notwendige Rahmenbedingungen schaffen.

Betonen möchten wir, dass Schulen im pädagogischen Sinne offene und professionell kommunizierende Organisationen bleiben sollen. Dafür nötig sind differenzierte Konzepte zur internen und externen Information mit geregelten Zugängen und sicherem Umgang mit Daten. Eine panikartige totale Abschottung wäre kontraproduktiv. Dieser Leitfaden möchte für die Problematik sensibilisieren und dazu allen Beteiligten konkrete Hinweise geben: In einem ersten Teil geht es um die beim pädagogischen Auftrag anfallenden Herausforderungen und im zweiten Teil werden Hinweise für die Verantwortlichen auf der Ebene Schuleinheit genannt. Im Anhang sind Hinweise auf Ratgeber und juristische Bestimmungen angeführt.

1 DATENSICHERHEIT UND DATENSCHUTZ FÜR DEN PÄDAGOGISCHEN AUFTRAG (UNTERRICHT, SCHÜLER/INNEN UND LEHRER/INNEN)

Die Rahmenbedingungen zur Ausübung des pädagogischen Auftrags müssen Datenschutz gewährleisten und Datensicherheit garantieren

1.1 Einleitung

In den ersten Jahren der Digitalisierung standen die Chancen und Möglichkeiten für den Unterricht und die Anwenderkompetenz im Zentrum des Interesses. Bald wurde auch über die Gefahren für die Kinder und Jugendlichen und deren Mediennutzung insbesondere im Internet diskutiert. Damit rückte das persönliche Verhalten von Lehrpersonen in der öffentlichen sozialen Kommunikation ins Zentrum. Vor zwei Jahren haben die gleichen Herausgeber den Leitfaden Social Media für Lehrpersonen und Schulleitungen publiziert. Heute stehen wir auch vor der Herausforderung, den Unterricht, also das Kerngeschäft der Schulen sicher zu gestalten.

Lehrpersonen müssen sich mit der Digitalisierung auf verschiedenen Ebenen auseinander setzen:

1. Schülerinnen und Schüler nutzen persönliche und schuleigene digitale Geräte, nutzen Apps und Programme und kommunizieren mit diesen Geräten (u.a. Fotos, Filme, Texte).
2. Schulen digitalisieren ihre Dokumentation (lokale und vernetzte PCs, Schulserver, Datenbanken, Clouds etc.) sowie ihre interne und externe Kommunikation (Mails, SMS, Webseiten, Newsletter, Social Media u.a.).
3. Lehrpersonen nutzen im Unterricht und für Vorbereitung und Dokumentation sowie für die Kommunikation mit Schüler/innen, im Team und mit Eltern digitale Geräte und Daten (USB-Sticks, lokale, verkabelte und mobile Geräte, Server, SMS, Social Media, E-Mails etc.).
4. Lehrpersonen bleiben auch als Privatpersonen im Internet und in der digitalen Kommunikation mit Fotos und Texten als Berufspersonen meist erkennbar.
5. Die Rahmenbedingungen zur Ausübung des pädagogischen Auftrags sind bisher vielerorts bezüglich Datenschutz und Datensicherheit alles andere als überzeugend. Was Datenschutzbeauftragte im Soft- und Hardwarebereich bemängeln, sind primär folgende Punkte:
   Datenablage: Cloud-Lösungen und externe Server ohne genügende Sicherheiten, interne oder private Server und mobile Speicher ohne hinreichenden Schutz, zu wenig differenzierte Dateneinsicht;
   Kommunikation: Mails und andere Kommunikation über ungesicherte Geräte, Mailserver und Kommunikationswege;
   Webseiten und Social Media: Fotos, Adressen und Material ohne Schutz der Persönlichkeitsrechte, zugänglich für Manipulationen von außen; Nutzung von Programmen und Apps, die parallel zur Nutzung Daten der Nutzer sammeln und weiterleiten.

Dazu kommt eine bisher vernachlässigte Weiterbildung des Schulpersonals über Persönlichkeitsrechte, Datenschutz und Datensicherheit, oft auch zu nur grundlegender medienpädagogischer Kompetenz.

Dieser erste Teil des Leitfadens möchte einige Aspekte der Datensicherheit und des Datenschutzes im pädagogischen Kerngeschäft thematisieren. Der Bogen reicht von der persönlichen Medienkompetenz von Lehrpersonen über die Nutzung von Medien durch Kinder und Jugendliche im Unterricht bis zur Bewältigung von Krisen. Die persönliche Verantwortung von Lehrerinnen und Lehrern zeigt sich u. a. in der sicheren und regelkonformen Nutzung von Geräten und im verantwortungsvollen Umgang mit

digitalen Daten, deren Kontrolle heute nicht mehr mit einem abgeschlossenen Pult und gut bewachter Ledermappe sichergestellt werden kann.

1.2 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.

1.3 Datensicherheit im Lehrberuf

Die Einhaltung der Sorgfaltspflichten bei Schülerbewertungen, beim Zeugnisschreiben, beim Austausch mit Kollegen, bei der Unterrichtsvorbereitung, bei Elternanfragen zum eigenen Kind, bei Datenanforderungen von Schulgremien und Fachstellen bedingt eine Kommunikation über sicherheitstaugliche Systeme.

Lehrerinnen und Lehrer hatten immer schon besondere Sorgfaltspflichten bei Schülerakten und Zeugnissen, beim Austausch mit Kollegen, bei Elternanfragen zu ihrem Kind, bei Datenanfragen von Behörden oder Fachstellen oder bei der Verwendung von Unterrichtsmaterial zu beachten. Mit der elektronischen Kommunikation akzentuieren sich die Sorgfaltspflichten, weil Datenlecks rasch sehr gravierende Auswirkungen haben können.
Die gesamte Kommunikation von Lehrpersonen mit Schüler/innen, 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 Schulen von einer Kommunikation via Facebook oder WhatsApp bzw. ähnlichen kommerziellen Diensten dringend abzuraten, in Deutschland ist sie gar nicht zulässig. Ausnahmen bilden hier allenfalls die zurzeit sicheren Dienste wie SIMSme, Threema oder bleep (SMS-Dienst).
Hinweis: Mehr zu Kommunikationsdiensten, Servern und zur sicheren Datenaufbewahrung finden Sie im Teil 2 betreffend Anforderungen an die Schulen.

1.4 Medienkompetenz der Lehrperson

Medienkompetenz definiert sich nicht allein durch die Kenntnis von Produkten wie Word, WhatsApp oder Plattformen wie Facebook (vgl. Anhang). Das Erkennen von sensiblen Daten und Texten sowie das sichere Aufbewahren und Übermitteln von Daten gehören zu den Grundkenntnissen einer Lehrperson.

Lehrpersonen sollten also wissen, wer welche schulisch sensiblen Daten gegebenenfalls ebenfalls einsehen und auch weiter kombinieren kann und welche Daten öffentlich gestellt oder im Unterricht genutzt werden dürfen und welche nicht. Weiter gehört das Verständnis dazu, mit welchen Gegengeschäften gewisse Softwarelösungen und Plattformen für Kunden kostenfrei angeboten werden und wie die Nutzungsbedingungen für den Gebrauch dieser Systeme bzw. Plattformen formuliert sind.
Notwendig ist, dass solche Kenntnisse nicht nur in der Ausbildung vermittelt werden, sondern auch bereits aktive Lehrpersonen erreichen. Dies liegt in der Verantwortung von Arbeitgebern, welche an ihren Schulen digitale Technologien einführen.

1.5 Verhalten von Lehrpersonen im Internet

Lehrpersonen bewegen sich als Berufsleute 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. Schülerinnen und Schüler 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.
- 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 und am Elternabend. Klären Sie Schülerinnen, Schüler und Eltern darüber auf, wie Sie den Umgang mit Netzwerken pflegen und warum Sie möglicherweise online keine Einzelkontakte mit Schüler/innen oder Eltern pflegen wollen. Machen Sie auf die rechtlichen Konsequenzen von Missbräuchen aufmerksam.
- Weil selten alle Eltern bzw. deren Kinder und Jugendliche 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) Schülerinnen und Schüler oder deren Eltern gleich. Entweder Sie nehmen diese an oder lehnen diese ausnahmslos ab.
- Da es nach wie vor Schülerinnen und Schüler ohne privaten PC oder Internetzugang gibt, sollten Sie sich, bevor Sie soziale Netzwerke in Ihren Unterricht einbauen, sich über allfällige Regelungen an Ihrer Schule und im Land informieren. Weitere zu klärende Fragen wären: Darf ich Social-Media-Plattformen für den Unterricht benutzen? Auf welche Plattformen darf ich Kinder verpflichten – auf welche nicht? Welche Plattformen werden von staatlichen Einrichtungen für Bildungszwecke zur Verfügung gestellt?

Eine Lehrperson kann privat in Facebook, Twitter oder WhatsApp unterwegs sein.

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

1.7 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. Für das Festlegen von Grundsätzen zur Datensicherheit und zum Datenschutz sowie für eine sichere Infrastruktur ist die Schule zuständig. Dazu gehören geschützte dienstliche E-Mail-Adressen, der geschützte Zugang auf dienstliche Online-Plattformen sowie ein regelmäßiger IT-Support für die Schule, um die sensiblen Schuldaten vor jeglichem Fremdzugriff zu schützen. Wenn Lehrpersonen oder auch Schüler/innen den schulischen IT-Support übernehmen, ist es notwendig, diese Aufgabe vertraglich festzulegen, um Risiken zu vermeiden. Es ist ratsam, dieses Thema gegenüber der Schulleitung und Personalvertretungen anzusprechen. Auf keinen Fall sollte von Lehrpersonen stillschweigend eine Vernachlässigung dieser Sicherheitsaspekte hingenommen werden.
Hinweis: Vgl. auch Teil 2. Im Anhang gibt es einen Link zu einem Muster-Auftragsdatenvertrag.

1.8 Lehrperson und Arbeitsrecht

Im Umgang mit sensiblen Daten sind keine Kompromisse zulässig.

Das Einhalten von auferlegter Datensicherheit kann aufgrund mangelhafter Ausstattung mit Hard- und Software sowie unzureichendem IT-Support zum Problem für Schulleitung und Lehrpersonen werden. Zudem gibt es noch nicht überall genügend finanzierte Fortbildungsangebote und Zeitressourcen für regelmäßige schulinterne Weiterbildung.

Da jedoch die gesetzlichen Bestimmungen im Umgang mit sensiblen schulischen Daten gewahrt werden müssen, sind Kompromisse, die auf eine Verletzung dieser Vorschriften hinauslaufen würden, nicht zulässig. Auf diese Problematik müssen die Betroffenen daher die Vorgesetzten aufmerksam machen – die Lehrperson gegenüber der Schulleitung, die Schulleitung gegenüber dem Arbeitgeber. Auch sollten Ombudsstellen bzw. Personalvertretungen auf das Problem angesprochen werden. Es empfiehlt sich, die vor Ort geltenden Bestimmungen einzuholen.

1.9 Einhalten des Urheberrechts

Grundsätzlich sind bei jeglicher Nutzung von medialen Inhalten im Unterricht bzw. in schulischen Veranstaltungen die geltenden urheberrechtlichen Bestimmungen einzuhalten. Einerseits soll geistiges Eigentum geschützt werden können, andererseits brauchen öffentliche Schulen und Lehrpersonen in ihrem Alltag möglichst einfache Regelungen.

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. An Schulen ist manchmal unklar, wem die von Lehrpersonen erarbeiteten Unterlagen für Unterrichtslektionen gehören und ob sie kostenlos auch von anderen Lehrpersonen dieser Schule genutzt werden dürfen.

Begrenztes Kopieren und Scannen von Büchern, Fachartikeln oder Musiknoten ist urheberrechtlich zulässig, wenn die nationalen Regelungen eingehalten werden. In Deutschland ist das begrenzte Scannen und Speichern von Dateien zulässig, wenn das Werk nach 2005 erschienen ist und der Zugriff nur durch die Lehrperson selbst erfolgen kann. In Österreich dürfen Bildungseinrichtungen veröffentlichte Werke für einen bestimmten abge-

grenzten Kreis von Lernenden vervielfältigen und zur Verfügung stellen (dies gilt allerdings nicht für explizite Schul- oder Lehrbücher!). 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 mit den zuständigen Rechtsdiensten der Schulbehörde Rücksprache zu nehmen bzw. sich bei den Verlagen und Online-Plattformen über die AGB zu informieren, damit Lehrpersonen nicht unvermutet mit einer Klage eingedeckt werden.

Ein «Digital-Kodex» an der Schule ist Einzelregelungen durch die Lehrperson vorzuziehen.

1.10 Sorgfaltspflichten bei Recherchen durch Schüler/innen im Internet

Eine Aufforderung an die Schüler/innen, für schulische Aufgaben im Internet zu recherchieren, sollte von den notwendigen Informationen begleitet sein: Persönlichkeitsrechte, das Urheberrecht, AGB und datenschutzrechtliche Zusammenhänge sollten den Schüler/innen bekannt gemacht werden und auch, wo ethische Grenzen gesetzt sind. Die Schüler/innen 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 Schüler/innen 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.

Ein schulischer «Digital-Kodex», der einvernehmlich von den Schulgremien erarbeitet wird, ist auf jeden Fall Einzelregelungen durch die Lehrperson vorzuziehen. Ebenso ist es empfehlenswert, rechtliche und ethische Fragen rund um die Mediennutzung in Elternveranstaltungen aufzugreifen. 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.

1.11 Datenverlust

Bei Datenverlust bzw. Datendiebstahl ist unmittelbar nach Bekanntwerden bzw. Erkennen des Problems zu handeln. Zum einen ist die Schulleitung zu informieren und zum anderen ist eine Beweissicherung einzuleiten. Für die Beweissicherung sollte ein Experte zu Rate gezogen werden, um den möglichen Datenverlust einzuschränken und die daraus entstehenden Konsequenzen so weit wie möglich klären zu können. Spätestens nach der genauen Analyse sind die Ermittlungsbehörden und/oder die Polizei einzuschalten, weil möglicherweise strafrechtlich relevante Sachverhalte abgeklärt werden müssen, die anzeigepflichtig sind oder weil Persönlichkeitsrechte betroffen sind.

Neben den zivil- und strafrechtlichen Maßnahmen sind bei Delikten oder bei fahrlässigem und schädigendem Umgang mit Daten für Lehrpersonen arbeitsrechtliche Maßnahmen und je nach Schultyp für Jugendliche auch schulische Disziplinarmaßnahmen bis zum Schulausschluss möglich. Hier sind die rechtlichen Bestimmungen vor Ort zu beachten.

1.12 Cybermobbing

In Krisensituationen muss seitens der Lehrperson generell mit sehr viel Bedacht und Vorausschau gehandelt werden.

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 Schülerinnen und Schüler, Eltern oder schulisches Personal auf öffentlich zugänglichen Internetplattformen andere Mitglieder der Schulgemeinschaft oder andere Menschen beleidigen oder anderweitig angreifen, empfehlen sich folgende Vorgehensweisen:

Prävention:
- Erarbeiten und vermitteln Sie einen Ethik-Kodex (Klasse, Schule, Eltern).
- Informieren Sie sich über Ihren Dienstweg, über die Pflichten des Arbeitgebers, Ihre rechtlichen Möglichkeiten und über Beratungsstellen.

Sofortmaßnahmen:
- Überlegen Sie zuerst und handeln Sie dann rasch.
- Notieren Sie sich die entsprechenden Links und Internetadressen, machen Sie ein Bildschirmfoto[1], 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 nahetreten.

Information:
- Informieren Sie die vorgesetzte Stelle (Schulleitung, Arbeitgeber) und als Fachlehrperson die Klassenlehrperson.
- Fragen Sie nach Beratung durch externe Fachstellen.
- Bitten Sie um eine sofortige Besprechung des weiteren Vorgehens mit der Schulleitung.

Auf keinen Fall tun: Sich schämen und niemandem etwas sagen.

Problemlösung:
- Suchen Sie mit Unterstützung einer Drittperson (Schulleitung, Beratungsstelle, Mediation) das direkte, persönliche Gespräch mit den betreffenden Schülerinnen und Schülern 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.

[1] Bildschirmfoto der Seite:
Strg + Print/Druck gemeinsam drücken und dann in ein leeres Dokument einfügen (Strg + V).

- Vereinbaren Sie das zukünftige Verhalten bei Unzufriedenheit.
- Erstatten Sie in Absprache mit Ihren Vorgesetzten Anzeige bei der Polizei.

Anzeigepflicht:
In Österreich besteht Anzeigepflicht und in der Schweiz eine Pflicht zur Gefährdungsmeldung bei der Kinder- und Erwachsenenschutzbehörde (KESB) und in einzelnen Kantonen bei der Jugendanwaltschaft, wenn Schüler oder Schülerinnen von Übergriffen oder Versuchen dazu betroffen sind. Bei Cybermobbing gegen Lehrpersonen besteht für Zeugen keine Meldepflicht. In Deutschland müssen Vorfälle gegen Schülerinnen und Schüler der Schulleitung gemeldet werden.

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.

2 DATENSCHUTZ UND DATENSICHERHEIT FÜR DEN SCHULISCHEN AUFTRAG (SCHULLEITUNG, SCHULTRÄGER/SCHULERHALTER)

2.1 Einleitung

Die Verantwortung für Datensicherheit und Datenschutz wird zu einer wesentlichen Führungs- und Finanzierungsaufgabe für Schulleitungen und Schulträger/Schulerhalter.

Mit der Ablage von teilweise sensiblen Schuldaten (Prüfungs- und Zeugnisnoten, Beobachtungen, Gesprächsnotizen etc.) auf öffentlich oder schulintern genutzten Servern und Clouds, aber auch mit der Kommunikation über teilweise offene Kanäle steigt der Handlungsbedarf an Schulen. Die Verantwortung für Datensicherheit und Datenschutz kann nicht an die Lehrpersonen delegiert werden, sie wird zu einer wesentlichen Führungs- und Finanzierungsaufgabe für Schulleitungen und Schulbetreiber.

Schulen sind pädagogische Einrichtungen mit einem hohen Bedarf an interner und externer Kommunikation. Unzureichende Ausstattung und mangelhafte oder aus mangelnder Zeit und anderen Prioritäten nicht nutzbare Weiterbildungsangebote behindern sie im Ausbau einer zeitgerechten Kommunikation. Das Bewusstsein für die Verantwortung und den daraus resultierenden Handlungsbedarf ist in vielen Bereichen noch zu wenig entwickelt.

Folgende Herausforderungen für Schulverantwortliche stehen dabei im Vordergrund:

1. Datenablage: Sichere Server und Clouds in der eigenen Computerumgebung inkl. sicherer externer Zugänge, rechtlich sichere Verträge, nachhaltig geregelte finanzielle Verbindlichkeiten, mögliche Differenzierung der Zugänge und Einsichtsrechte, Klärung der Verantwortlichkeiten.
2. Kommunikationskonzepte: Klärung der Erwartungen, Zuständigkeiten und Verantwortungen für alle Beteiligten, Regelung der internen und externen Kommunikation auf allen Kanälen (Kommunikationswege, -mittel und -inhalte).
3. Hard- und Software: Differenzierte Logins und Möglichkeiten für limitierte Zugänge, technische Sicherheit, genügende Vernetzung, Ausrüstung mit schulischen Geräten oder persönliche Ausrüstung mit Sicherheiten, Unterstützung für das Alltagsgeschäft ohne Überkomplizierung.
4. Persönliche Kompetenzen und Krisenbewältigung: Gewähr für sicheren Umgang mit Geräten und Datenbearbeitung, Krisenkonzepte erstellen, Aufklärung über rechtliche Aspekte gewährleisten.

Dieser zweite Teil thematisiert u.a. Passwortschutz, Aktenaufbewahrung, Einsichtsrechte, Netzwerke, Umgang mit Bildmaterial, IT-Support bis hin zur sicheren Entsorgung von Geräten.

2.2 Datensichere Schule

Die Schule muss ihre Informationen gemäß aktuellem Stand der Technik mit organisatorischen und technischen Sicherheitsmaßnahmen schützen. Die Maßnahmen sind darauf auszurichten, dass sie die Vertraulichkeit, Integrität, Verfügbarkeit, Zumutbarkeit und Nachvollziehbarkeit gewährleisten.

Beispiele von Maßnahmen sind die Installation von Virenschutzprogrammen, Firewall, Backup-Systemen, Passwortschutz, differenzierte Zugangsmöglichkeiten, Protokollierung von Vorgängen, Nutzungsregelungen usw.

Auf das schuleigene Intranet hat nur ein beschränkter Personenkreis Zugriff. Vor-, Nachnamen, Stundenpläne und Klassenlisten ohne persönliche

Informationen können deshalb im Intranet verbreitet werden. Für die interne Offenlegung von privaten Telefonnummern von Schüler/innen und Lehrpersonen, von privaten Postadressen und E-Mail-Adressen oder Fotos braucht es jedoch eine Einwilligung der Betroffenen. Lehrpersonen haben einen Anspruch, dass ihnen eine geschäftliche E-Mail-Adresse zugeteilt wird. Gleiches gilt für die Schülerinnen und Schüler, wenn die Lehrpersonen oder Schulführung mit diesen per E-Mail kommuniziert. Insbesondere Führungsdaten, aber auch vertrauliche Daten zu Kindern und Eltern dürfen nur einem beschränkten Personenkreis bekannt gemacht werden.

Folgende Punkte sind somit bei der Umsetzung des Datenschutzes im Schulumfeld zu beachten:

- Zentrale Datenablage (Server, Speichersystem etc.) mit einem definierten und schriftlich fixierten Berechtigungskonzept.
- Eigene Bereiche für jede Lehrperson, auf welche andere Personen nicht zugreifen können.
- Spezielle Bereiche nur für die Schulleitung, für Klassenteams, Fachgruppen und weitere Gruppen.
- Sichere Arbeitsplätze mit verschlüsselten Festplatten und insbesondere mit sicheren Passwörtern.
- Verwaltungs- und Schulnetz sind physisch getrennt. Aus dem Verwaltungsnetz kann es einen transparent geregelten Zugriff auf das Schulnetz geben.
- Sicheres WLAN, wobei der WLAN-Schlüssel an niemanden weitergegeben wird.
- Cloud-Lösungen sind rechtlich umfassend abzuklären und müssen vom Schulträger/Schulerhalter bewilligt sein.
- Abklärung der Rechtssituation beim Arbeitgeber/Schulträger/Schulerhalter bezüglich Speicherung von Daten außerhalb des Landes oder der Europäischen Union (in Deutschland: nicht erlaubt).
- Erstellung von Richtlinien für die Nutzung der IT-Systeme durch die Lehrpersonen.
- Haftbarkeitsvereinbarungen mit den Verantwortlichen für externe Server sowie für die externe und interne IT-Wartung.
- Auf externe Cloud-Lösungen mit privaten Unternehmen sollte verzichtet werden, da die Besitzverhältnisse jederzeit wechseln können (Konkurs, Verkauf ins Ausland) und damit die Sicherheit von zu schützenden Daten nicht gewährleistet ist.
- Sicherung des E-Mail-Verkehrs und Backup der Daten, allenfalls nur nachvollziehbare Veränderungen an Datensätzen (Log-System).

2.3 Datensicherer persönlicher Arbeitsplatz an der Schule

Ein datensicherer Arbeitsplatz für Lehrpersonen definiert sich im Wesentlichen dadurch, dass jede Person von intern und extern den geschützten Zugriff auf die Daten hat, die sie für ihr tägliches Arbeitsumfeld benötigt. Es empfiehlt sich ein bereits im Serverumfeld entsprechend administriertes Berechtigungskonzept. Ein sicherer Arbeitsplatz für Lehrpersonen definiert sich im Wesentlichen durch folgende Faktoren:

- Sichere Zugriffe von intern und extern von allen verwendeten Geräten aus.
- Verschlüsselter Zugriff für die verwendeten Geräte.
- Regelmäßige Updates der Software und insbesondere des Virenschutzes.
- Einsatz von sicheren Passwörtern in Kombination mit automatisch einschaltenden Bildschirmschonern.
- Regelmäßige Information und Sensibilisierung der Lehrpersonen.

Als sicher gelten zurzeit die SMS-Dienste SIMSme und Threema sowie schuleigene und somit interne Systeme wie z.B. iServe oder Moodle.

2.4 Datenschutz, Datensicherheit in der inklusiven Schule

Informationen über eine Schülerin, einen Schüler unterliegen der Vertraulichkeit, auch wenn diese auf dem Schulserver gespeichert sind.

Informationen über eine Schülerin, einen Schüler 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 ermöglichen.

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

2.5 Datenzugriff aus der Verwaltung

Schulen mit direkten Zugriffsmöglichkeiten aus anderen Verwaltungsabteilungen oder von vorgesetzten Stellen sollten die Einsichtsmöglichkeiten genau kennen und regeln. Unsinnig und in der Regel auch ein Verstoss gegen die jeweilige Datenschutzgesetzgebung wäre, wenn Gemeinden oder Kreise/Kantone ungehindert Zugriff auf schulische Server hätten.

Schülerdaten dürfen nur an Dritte übermittelt (weitergegeben) werden, wenn entweder eine Einwilligung der Schüler/innen bzw. der Eltern vorliegt oder eine gesetzliche Grundlage existiert. Dies gilt auch für die Nennung von realen Schülernamen in Online-Medien ohne vertragliche Zusicherung von Anonymität (z.B. Online-Arbeitsbögen, Prüfungen).

Bei Fahndungen oder sonstigen Ermittlungen der Strafbehörden an Schulen findet sich die gesetzliche Grundlage in der Strafprozessordnung. Allenfalls bestehen weitere gesetzliche Grundlagen bei Ermittlungen durch die Schluntersuchungsbehörden. Bevor jedoch Daten von Schüler/innen an die Behörden herausgegeben werden, empfiehlt sich eine umgehende Rücksprache mit der Schulleitung oder mit dem zuständigen Datenschutzbeauftragten. Werden die Daten zu früh herausgegeben, sind sie nicht mehr zurückholbar.

Auch Datenanforderungen von sonstigen Behörden wie z.B. Jugendämtern, Sozialämtern etc. bedürfen ebenfalls immer einer gesetzlichen Grundlage. Im Allgemeinen wird man diese in den Sozialgesetzbüchern finden. Vor jeglicher Übermittlung ist hier immer die Gesetzesgrundlage seitens der Schulleitung zu prüfen bzw. mit den Datenschutzbehörden Rücksprache zu halten. Unabhängig davon, wer diese Daten erhält, verantwortlich für die Übermittlung ist immer der Absender.

Auch mit kooperierenden Fachstellen und Heimen sind gegenseitige Zugriffe oder das Zur-Verfügung-Stellen von Daten vorab genau zu prüfen.

2.6 Recht auf Einsicht in Daten

Eltern und Schülerinnen oder Schüler haben ein Einsichtsrecht in amtlich abgelegte Daten zu ihrer Person. Dies gilt auch für digitalisierte Daten an Schulen über Schülerinnen und Schüler.
Es braucht Regelungen, welche Daten wie aufbewahrt werden müssen und bei welchen Daten auf Ansuchen hin Einsicht gewährt werden muss. Beispiele: Name, Adresse, Noten, Stütz- und Fördermaßnahmen.

2.7 Aufbewahrung und Vernichtung von Akten

Die Schule darf ihre Akten solange in einer laufenden Datenablage aufbewahren, wie sie diese für das Erfüllen ihrer Aufgaben benötigt. Die Daten sollen maximal während der gesetzlich vorgegebenen oder an den Schulen definierten Fristen aufbewahrt werden. Anschließend müssen die für das Archiv bestimmten Akten aussortiert und archiviert werden. Die Aufbewahrungsfristen variieren je nach Land und Kanton. Nicht ins Archiv überführte Akten und Dateien sind so zu vernichten, dass sie nicht wiederhergestellt werden können. Dies gilt insbesondere für nicht mehr gebrauchte PCs, Laptops, Tablets und andere Festplatten. Für Archive gelten weitere Bestimmungen.

2.8 Problem Passwörter

Initial vergebene Passwörter (z.B. durch das IT-System oder die Schulleitung) müssen nach der ersten Systemanmeldung geändert werden. Vorgaben seitens der Schulleitung, die einmal vergebenen Passwörter nicht zu verändern, sind grundsätzlich unzulässig.

Passwörter sollte man sich merken können. Ein Passwort, welches an einem Bildschirm klebt oder unter der Schreibtischunterlage liegt, erfüllt seine Funktion nicht wirksam.
Hinweis: Mehr dazu, wie man sich Passwörter merken kann, im Anhang.

Machen Sie sich pro Jahr einen entsprechenden Unterordner für Ihre Dokumente oder stellen Sie ein Datum vom Typ Jahr-Monat-Tag vor den Dokumentennamen.

2.9 Löschen von Dokumenten und E-Mails

Je nach Inhalt gelten E-Mails und ihre Anhänge (PDF-, Word-Dateien etc.) ebenfalls als Urkunden mit Aufbewahrungspflicht und sind daher gleichzusetzen mit Schriftstücken, die mit normaler Post versendet werden. Für den Versand von Dokumenten, die in Office-Programmen hergestellt wurden, empfiehlt sich die Umwandlung in eine PDF-Datei. Die dafür notwendige Software ist an den Arbeitsplätzen zur Verfügung zu stellen.

Alle relevanten Schriftstücke haben sogenannte Aufbewahrungsfristen, die je nach Land und Kanton bei zwei bis über zehn Jahren liegen können. Gewisse Daten dürfen z.B. gar nicht gelöscht werden und sind zu archivieren. Die Speicher- bzw. Aufbewahrungsfrist selber ist abhängig von der Art des Dokuments. Dokumente sollen so lange aufbewahrt werden, wie diese zum Beweis von rechtlichen Gegebenheiten erforderlich sind. Allenfalls müssen auch buchhalterische Grundlagen beachtet werden (keine Buchung ohne Beleg).

2.10 Bekanntgabe von Informationen von allgemeinem Interesse

Die Schule kann von Amtes wegen über Tätigkeiten von allgemeinem Interesse wie Anlässe, Neuigkeiten, Schulprogramme usw. informieren. Aufbau, Zuständigkeit und Ansprechpersonen können ebenso veröffentlicht werden. Dazu gehören beispielsweise die Namen, Funktionen und dienstliche E-Mail-Adressen der Lehrpersonen und die der anderen Mitarbeitenden, soweit diese Funktionen für die Schule ausüben, die von allgemeinem Interesse sind. Auch die Namen der Mitglieder der Schulbehörde können veröffentlicht werden.

Fotos von Mitarbeitenden sollten nur mit Einwilligung der Betroffenen freigestellt werden. Durch Automaten kopierbare Mailadressen (@) sollten zur Vermeidung unliebsamer Spam-Werbung beispielsweise mit [at] unleserlich gemacht werden.

Als Medium für diese Informationen kommen hauptsächlich die Schulhomepage, das Intranet oder Printmedien in Frage.

2.11 Schul- und Klassenwebseiten, Netzwerke

Jegliche Auftritte der Schule im Internet müssen rechtskonform gestaltet sein. Jedes eingestellte Element muss das Urheberrecht, das Recht auf Schutz der Persönlichkeit und weitere datenschutzrechtliche Bestimmungen wahren. Dies ist insbesondere zu beachten bei vorgesehener Nutzung von Zitaten aus Politik, Kultur oder Wissenschaft bzw. aus Presseveröffentlichungen, bei Nutzung von Bildern, Fotos, Filmzitaten, Videos oder Audiodateien. Besondere Beachtung gilt auch dem Erstellen von Links, die zu Fremdseiten führen, da der Betreiber der Schulhomepage dafür eine begrenzte Haftung übernimmt. Ebenso muss jede Schulhomepage über ein rechtskonformes Impressum verfügen.
Hinweis: Siehe dazu im Anhang ein Musterimpressum.

Mit großer Zurückhaltung sollte auch das Einstellen von Aufnahmen aus dem Unterricht bzw. von anderen Schulveranstaltungen erfolgen. Grundsätzlich muss dafür das Einverständnis der dargestellten Personen bzw. der Erziehungsberechtigten vorliegen. Dies gilt ebenso für Namensnennungen auf der Schulhomepage.

2.12 Networking mit Schulen im In- und Ausland

Hier gelten ebenso die gesetzlichen Regelungen für Urheberrecht, Persönlichkeitsrecht und Datenschutz. Die Sorgfaltspflichten für Daten aus dem Unterricht, aus Schulbüchern sowie für Bild- und Audiodateien sind auch hier zu beachten. Dies gilt insbesondere, wenn der Austausch zwischen Schulen in Ländern mit unterschiedlichen Rechtssystemen stattfindet.

2.13 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.

2.14 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.

Deutschland: Anbieter mit Servern außerhalb der EU sind nicht zugelassen. Die Nutzung von Clouds unterliegt strengen Regeln.

Österreich: Microsoft Office 365 kann durch die Schulen datenschutzkonform genutzt werden, wenn die Zusatzvereinbarung, welche auf österreichische Rechtsverhältnisse zugeschnitten ist, abgeschlossen wird. Weitere Maßnahmen wie das Verschlüsseln von besonderen Personendaten sind bei der konkreten Anwendung zu berücksichtigen.

In der Schweiz konnte mit Microsoft eine Regelung getroffen werden, wonach bei der Benutzung von Microsoft Office 365 die Schweizer Gerichte zuständig und Schweizer Recht anzuwenden sei. Gestützt auf den USA Patriot Act (bzw. neu: US Freedom Act) wurde Microsoft aber erstinstanzlich von einem New Yorker Bezirksgericht verpflichtet, die auf einem europäischen Server sich befindenden Daten der eigenen Cloud-Kunden an die amerikanischen Behörden herauszugeben. Als US-Gesellschaft unterliegt Microsoft ausschließlich den dortigen Gesetzen. Es empfiehlt sich deshalb, im Schulbereich auf die Verwendung von Cloud-Systemen zu verzichten, solange diese nicht auf dem eigenen Server betrieben werden. Auch wenn die Vereinigung der Schweizer Datenschutzbeauftragten «Privatim» die Verwendung von Microsoft Office 365 grundsätzlich zulässt, wird von diversen kantonalen Datenschutzbeauftragten klar festgehalten, dass Microsoft Office 365, welches auf Cloud-Diensten basiert, nicht für personenbezogene Daten eingesetzt werden darf.

Vor der Veröffentlichung von Personenfotos sollte die Einwilligung der Betroffenen eingeholt werden.

2.15 Fotos und Videos

Fotos von Schülerinnen und Schülern dürfen nur mit deren Einwilligung aufgenommen und veröffentlicht werden. Es gilt das Recht am eigenen Bild. Urteilsfähige und rechtlich mündige Schülerinnen und Schüler erteilen die Einwilligung selbst. Da der Begriff der Urteilsfähigkeit nicht altersmäßig fixiert ist, empfiehlt es sich, zusätzlich die Einwilligung der Erziehungsberechtigten einzuholen. Bei nicht urteilsfähigen Kindern erteilt diese der gesetzliche Vertreter, im Normalfall die Eltern.

Anmerkung Schweiz: Als urteilsfähig gilt ein Kind, wenn es das Ausmaß und die Folgen seiner Einwilligung abschätzen kann, wobei die individuelle Entwicklung des Kindes zu berücksichtigen ist. Es gibt keine absolute Altersangabe. Die Einwilligung kann formlos oder durch konkludentes Verhalten erfolgen. Konkludentes Verhalten bedeutet, dass der Betroffene sich so verhält, dass man daraus schließen kann, dass er nichts gegen das Fotografieren einzuwenden hat. Auch ein «Opt-out» ist möglich. Das heißt beispielsweise, dass die Lehrpersonen informieren, dass an einem Anlass fotografiert wird und dass sich diejenigen Personen melden sollen, welche nicht auf Bildern erscheinen wollen. Die Regelungen sind an Elternabenden und für Lehrpersonen transparent zu machen. Aus Beweisgründen ist es jedoch zu empfehlen, eine schriftliche Einwilligung einzuholen. Ein einzelner Schüler bzw. Elternteil kann gestützt auf Art. 28 ZGB die Verletzung des Persönlichkeitsrechts gerichtlich einklagen. Das können auch Hausregeln nicht verhindern!
Im Rahmen des Unterrichts dürfen Lehrpersonen fotografieren, wenn die Fotos nur zu Schulungszwecken gebraucht und keinen weiteren Personen zugänglich gemacht werden. Sobald Dritte Kenntnis der Daten erlangen, sind die Voraussetzungen der Datenbekanntgabe (gesetzliche Grundlage, Einwilligung) zu beachten. Das Material ist zu vernichten, sobald es für den ursprünglichen Zweck nicht mehr benötigt wird.

Fotografieren Medienvertreterinnen und -vertreter während des Unterrichts, an internen Schulanlässen oder auf dem Schulareal, müssen die Schülerinnen und Schüler respektive deren Eltern vorgängig informiert werden und in die Aufnahmen einwilligen. Die Fotos dürfen nur im Rahmen dieser Berichterstattung verwendet werden.

Fotografieren Eltern ihre Kinder mit anderen Kindern im Unterricht, an internen Schulanlässen oder auf dem Schulareal, so ist dies grundsätzlich erlaubt, wenn

- die Fotos nur zum persönlichen Gebrauch bestimmt sind,
- die Eltern der anderen Kinder respektive diese Kinder selbst nichts dagegen einzuwenden haben und
- die Hausordnung der Schule kein Fotoverbot enthält.

Nicht erlaubt ohne Einwilligung sind

- Porträts anderer Kinder,
- Veröffentlichungen dieser Bilder (beispielsweise in sozialen Netzwerken oder auf Schulhomepages, auch nicht durch andere Schüler/innen oder Eltern).

Wenn Lehrpersonen, Medien oder Eltern im Freien fotografieren, dürfen sie dies grundsätzlich auch ohne Einwilligung der Betroffenen, solange die Personen nur als «Beiwerk» zur Aufnahme gelten. Wird beispielsweise eine «touristische» Kirche aufgenommen, vor welcher sich zufälligerweise mehrere Menschen befinden, darf das Foto gemacht werden. Sobald sich aber auch nur eine einzelne Person auf dem Bild, welche bestimmt oder durch die Umstände bestimmbar ist, gegen die Aufnahme oder die Veröffentlichung wehrt, sind deren Persönlichkeitsrechte zu wahren. Darüber sollten Eltern, Schüler/innen und Lehrpersonen informiert sein.

2.16 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 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.

2.17 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.

Wenn Schulen ein bestimmtes Supportunternehmen mit der Reparatur beauftragen, sind in den Supportverträgen auch Regelungen zum Datenschutz zu vereinbaren.
Hinweis: Siehe im Anhang ein Mustervertrag.

Erst wenn alle Daten sicher gelöscht sind, darf der PC entsorgt werden.

2.18 PC entsorgen

Wird ein beruflich genutztes Gerät nach Ende seiner Laufzeit entsorgt, sprich zum Wertstoffhof gebracht oder beim Kauf eines neuen Geräts beim Händler gelassen, so müssen im Vorfeld alle Daten sicher gelöscht sein.

Da eine wirklich sichere Löschung nicht einfach zu bewerkstelligen ist und weil das Gerät auf Wunsch der Schule beruflich genutzt worden ist, muss die Schule und nicht die Lehrperson für eine sichere Löschung sorgen. Dies kann durch mechanische Zerstörung der Festplatte, z.B. mit Hilfe einer Bohrmaschine, oder durch professionelle Programme geschehen. Das bloße Formatieren genügt nicht. Erst nach vollständiger Löschung der alten Daten kann ein beruflich genutztes Gerät einem Dritten überlassen werden.

2.19 IT-Support an der Schule

An vielen Schulen wird der IT-Support durch externe oder interne Dienstleister erbracht. Der externe Support kann durch ein IT-Unternehmen oder durch eine Dienstabteilung einer öffentlichen Verwaltung sichergestellt werden.

In allen Fällen, auch bei interner Wartung z.B. durch eine Lehrperson oder Schüler/innen, sind nach den jeweiligen Datenschutzgesetzen entsprechende Auftragsdatenverarbeitungsverträge zu schließen. Weiterhin sind entsprechende Regeln aufzustellen, die insbesondere bei Fernwartungszugriffen zu beachten sind. Denn ein externer IT-Dienstleister hat häufig den vollen Zugriff auf jegliche Informationen, welche auf dem Rechner bzw. Notebook liegen. Ungeschützte Fernwartungszugriffe (Remote) sind zu vermeiden, da diese nicht genügend überwacht und kontrolliert werden können.
Hinweis: Siehe im Anhang ein Mustervertrag.

2.20 Mobile private Geräte

Werden mobile private Geräte (Smartphones, Notebooks, Tablets) zur Erfüllung der schulischen Aufgaben eingesetzt, müssen die Informationen mit den geeigneten organisatorischen und technischen Maßnahmen geschützt werden. Unbeaufsichtigte, vergessene oder unsichere Geräte bergen Risiken. Minimummaßnahmen sind beispielsweise das Einrichten von Passwörtern, die Installation eines Virenschutzes und das Durchführen regelmäßiger Updates. Sensible Daten sind bei der Speicherung und Übermittlung durch Verschlüsselung zu schützen.

2.21 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.

Die Schulträger/Schulerhalter und Schulleitungen sollten eingreifen, um solche unrechtmäßigen Datenabgänge zu vermeiden. 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.

Wenn die Nutzung von privaten E-Mail-Konten von den Schulbetreibern mangels schulextern zugänglichen Geschäftsadressen geduldet wird, muss die Schule angemessene organisatorische und technische Maßnahmen umsetzen, um sensible Daten zu schützen und auch die Lehrpersonen vor Haftungsklagen abzusichern. E-Mails mit vertraulichem Inhalt müssen verschlüsselt sein, da der Datentransfer außerhalb des Schulnetzes nicht sicher ist.

2.22 Sponsoring: Angebote für Hard- und Software zum Einsatz im Unterricht

Kostenlose Angebote von Hardware oder Software entlasten die Kassen der Schulverantwortlichen. Aber sie schaffen Ungleichheiten im System und führen zu Angewohnheiten, die bei späteren Geräte- oder Systemwechseln nur mühsam zu ändern sind.

Schulische Organisationen sollten sich hüten, auf kostenlose Angebote einzusteigen. Die späteren Folgekosten und der potentielle Missbrauch des Rufs der Schule durch die nicht immer selbstlosen Unternehmen sollten mit einberechnet werden. Ausgenommen sind schulische IT-Pilotprojekte, die in einem juristisch einwandfreien Setting und mit gegenseitig geklärten Erwartungen durchgeführt und ausgewertet werden.

Kostenlose, exklusive Weiterbildungen in anderen Ländern sind ebenfalls mit Vorsicht anzunehmen und in jedem Fall mit Schulleitung und Arbeitgeber/Schulträger/Schulerhalter abzusprechen.

Anmerkung Deutschland und Schweiz: Wie für die Ausstattung mit Schulbüchern gilt auch für Klassensätze mobiler Geräte, dass der Klassensatz kein kostenfreies Gerät für die Lehrperson umfassen darf. Das wäre sonst unzulässige Vorteilsnahme durch die Lehrperson.

2.23 Regelungen und Schulung des Personals

Lehrpersonen sind genauso wie Mitarbeiter in Wirtschaftsunternehmen regelmäßig in Bezug auf den Datenschutz und die IT-Sicherheit zu schulen. Aufgrund der technischen Dynamik und dem Wechsel in den Teams sollten solche Schulungen regelmäßig insbesondere bei Neuerungen und Personalwechsel ohne Verzug durchgeführt werden. Gleiches gilt auch für das nichtunterrichtende Personal wie z.B. das Sekretariat und vielleicht in einem etwas geringeren Maße auch das weitere Dienstpersonal.

2.24 Prävention von Cybermobbing

Eine Schule kann im Rahmen der generellen Gewaltprävention einiges tun, um Cybermobbing vorzubeugen:

- Schulleitungen und Lehrpersonen kümmern sich um ein gutes Schul- und Klassenklima, geprägt von Würde, Respekt und ohne Beschämung. Sie schaffen ein dichtes Netz positiver Beziehungen im Kollegium, mit den Schülerinnen und Schülern sowie den Eltern.
- Teams bilden sich zum Thema Mobbing und Umgang mit Social Media weiter.
- Die Förderung von Medienkompetenz einschließlich Umgang mit Social Media sind Teil des Lehrplanes Schülerinnen und Schüler müssen die Kompetenzen entwickeln können, sich selber zu schützen. Medienkompetenz gilt als wichtige Grundlage, damit Schülerinnen und Schüler sich vor Missbrauch schützen können.
- Schulleitungen und Lehrpersonen kennen die möglichen Risiken, und die Vorgehensweisen im Krisenfall sind geregelt und bekannt. Schulleitungen und Behörden kennen die Pflichten der Arbeitgeberseite.
- Schülerinnen und Schüler kennen Ansprechpersonen und Beratungsstellen und wissen, dass sie sich an diese wenden können.
- Schülerinnen und Schüler kennen Strategien der Deeskalation bei Konflikten auf Online-Portalen und wissen, wie sie sich verhalten, wenn sie von Missbrauch und Mobbing erfahren oder betroffen sind.
- Es existiert ein einfaches, aber klares Regelwerk, das von Schulleitungen und Lehrpersonen im Alltag vorgelebt und in der Schulgemeinschaft durchgesetzt wird. Dazu gehören die Thematik im Umgang mit Fotos aus dem Unterricht, aus dem Schulleben, vom Pausenplatz oder von außerschulischen Lernorten genauso wie das Vorgehen im Falle von betroffenen Lehrpersonen oder Kindern und Jugendlichen der Schule.
- Zu möglichen Beratungsstellen im Krisenfall sind die Beziehungen eingespielt und die Aufgabenzuteilung geklärt.

2.25 Prävention von Datenmissbrauch oder -verlust

Insbesondere die Prävention von Krisensituationen sind zeitaufwendige Führungs- und Teamentwicklungsaufgaben. Ohne ausreichende Zeitressourcen und technische Vorkehrungen sind die Ziele der Datensicherheit und des Datenschutzes kaum zu erreichen.

- Sichere Technologien (E-Mail-Übermittlung, Server, Clouds, Software, Hardware etc.).
- Klare Regelungen für den Alltag.
- Sicherung der Zugänge.
- Vorbildwirkung von leitenden Personen.
- Regelmäßiger Erfahrungsaustausch und Weiterbildung (auch für neue Mitarbeitende und Praktikanten).
- Eingespielte Kontakte zu fachlicher Beratung und juristischen Behöden.
- Vorbereitete Szenarien für Krisensituationen.

2.26 Rechtsrisiken für Schulen

Obwohl Deutschland, Österreich und die Schweiz eigene Gesetze haben, um die Aktivitäten im Internet zu regeln, gelten allgemeingültige rechtliche Grundsätze für alle drei Länder. Unterschiede bestehen in der Höhe allfälliger Strafen bei Delikten und den Verfahrenswegen vor Gerichten, vor allem im Bereich Jugendstrafrecht.

Jegliche Auftritte in Internet/Social Media müssen aufgrund der bereits bestehenden Gesetze die Persönlichkeitsrechte, das Recht auf Datenschutz und den Urheberrechtsschutz gewährleisten. Der bestehende rechtliche Rahmen ist ausreichend für eine Strafverfolgung. Opfer von Cybermobbing können sich auf die Verfassung bzw. das Grundgesetz sowie auf die relevanten Gesetze berufen. Der Schutz der Menschenwürde und die freie Entfaltung der Persönlichkeit werden darin garantiert. Alle drei Länder sind zudem dem Übereinkommen des Europarates über die Cyberkriminalität beigetreten. Die Vertragsstaaten werden insbesondere verpflichtet, Datendiebstahl, Kinderpornografie, Computerbetrug und das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen.

Strafrechtlich gibt es zahlreiche Normen, welche dem Cybermobbing zugrunde liegende belästigende, drohende und verunglimpfende Handlungen beinhalten. Je nach Sachverhalt können folgende Rechtsverletzungen vorliegen: unbefugtes Eindringen in ein Datenverarbeitungssystem (Hacken), betrügerischer Missbrauch einer Datenverarbeitungsanlage, Datenbeschädigung, unbefugtes Beschaffen von Personendaten, z.B. für gefälschte Facebook-Profile, Erpressung, Urkundenfälschung, üble Nachrede, Verleumdung, Beleidigung, Drohung, Nötigung, sexuelle Belästigung, Pornografie etc.

3 ANHANG

Unter www.medien-datensicherheit-schulen.info/download finden Sie folgende Dokumente:

1. Einfache Regeln zum Merken von Passwörtern
2. Musterimpressum für Schulwebseiten (Deutschland)
3. Muster für einen Auftragsdatenvertrag (Deutschland, NRW)
4. Rechtsgrundlagen für Datenschutz bzw. Datensicherheit
5. Beispiele relevanter Rechtsprechungen
6. Beratungsstellen und Zuständigkeiten
7. Links zu Merkblättern und Ratgebern (exemplarische Auswahl)

Verband Bildung und Erziehung (VBE)
Behrenstraße 23/24
D-10117 Berlin
T. +49 30 726 19 66 0
F. +49 726 19 66 19
bundesverband@vbe.de
www.vbe.de

Gewerkschaft Öffentlicher Dienst –
Gewerkschaft Pflichtschullehrerinnen
und Pflichtschullehrer (göd aps)
Schenkenstraße 4/5
1010 Wien
T. +43 153 45 44 35
F. +43 153 45 44 52
kontakt@pflichtschullehrer.at
www. pflichtschullehrer.at

Dachverband Lehrerinnen
und Lehrer Schweiz LCH
Kulturpark
Pfingstweidstrasse 16
CH-8005 Zürich
T. +41 44 315 54 54
F. +41 44 311 83 15
www.lch.ch