

Bildungsdirektionen/LSR/SSR für Wien
Schulaufsicht, Fachaufsicht

Schulstandorte

Sachbearbeiter/in:
AL Mag. Martin Bauer, MSc
Abteilung Präs/15
Tel.: +43 1 531 20-3538
Fax: +43 1 531 20-813538
martin.bauer@bmbwf.gv.at

Antwortschreiben bitte unter Anführung der GZ:
BMBWF-9.000/0025-Präs/15/2018

Empfehlungen zur Nutzung digitaler Technologie an Schulstandorten

1 Einleitung

Gesellschaft, Arbeitswelt und Schule verändern sich durch die Digitalisierung aller Bereiche im zunehmenden Ausmaß. Grundsätze einer reflektierten Mediennutzung müssen breit kommuniziert werden, um den Lernenden, den Lehrenden und in letzter Konsequenz uns allen einen sachlichen Umgang mit Informationen und Daten zu gewährleisten.

Grundsätze sind:

1. Eine Stärkung der Eigenverantwortung und Souveränität in (elektronischen) Netzen
2. Die Umsetzung von Strategien des Wissenserwerbs und den Umgang mit geistigem Eigentum
3. Propagieren eines verantwortungsvollen und respektvollen Umgangs im Netz
4. Erkennen der Geschäftsmodelle, die hinter der Beteiligung und von Mitgliedschaften im Internet bestehen
5. Erkennen der Rechtslage und Kennen der persönlichen Rechte im Internet

Mit diesen fünf Schwerpunkten kann man, als Schülerin bzw. Schüler oder Lehrerin bzw. Lehrer, als Schulpartner oder in Kontakt mit Firmen und Berufsausbildungen die digitale Zukunft mitgestalten, ohne sich ausgenutzt und manipuliert zu fühlen. Dann kann man auch die Rolle der digitalen Medien als Veränderungspotential gut erkennen und nutzen. Eine wichtige Grundlage für eine „Digitalisierungsstrategie der Bildung“ ist eine Policy an den Schulstandorten und in der Schulverwaltung, mit vernetzten IT-Geräten bzw. „Streaming Media“ für die Unterrichtsarbeit umzugehen. Diese Ansätze sollten diese Information und Empfehlung liefern.

2 Zielsetzungen

Bereits 2008 gab es eine Empfehlung zur Mediennutzung und zu einer Internetpolicy, damals in enger inhaltlicher Verbindung zur Darstellung eines einfachen und sicheren Schulnetzes (Erlass „Digitale Kompetenz an Österreichs Schulen“ Zl. 17.200/110-II/8/2010 – hiermit aufgehoben).

Viele neue Hard- und Softwareentwicklungen sind seither passiert, der Kompetenzerwerb im digitalen Zeitalter ist aber als wichtige Prämisse von Bildungsarbeit gleich geblieben, wird allerdings seit eineinhalb Jahren durch die Bildungspolitik in besonderer Weise unterstützt. In einem „Policypaper“ geht es um eine gemeinsame Richtlinie, mit dem komplexen Thema „Digitale Bildung“ als Grundsatzvereinbarung umzugehen.

Dazu gehört

- Der Umgang mit der den Lernenden, den Lehrenden und den Schulen als Organisationseinheit anvertrauten Infrastruktur (Hard- und Software, Kommunikations-einrichtungen zur und in den Schulen wie Firewalls und WLAN), die unter Beachtung von modernen Sicherheitskonzepten vereinheitlicht werden soll
- Der Umgang mit Verwaltungssoftware und im pädagogischen Betrieb eingesetzter Software einschließlich dem relativ neuen Thema „elektronische Prüfungsumgebung“
- Chancen und Risiken bei der Publikation von pädagogischen und fachdidaktischen Inhalten in informatischen Netzen

Mit einem Überblick über die drei genannten Bereiche erscheint ein sorgsamer und effizienter Umgang mit Einrichtungen, Geräten und Anlagen der digitalen Medien gewährleistet. Informationstechnologien im Unterricht und beim individuellen Lernen kosten Geld – sowohl persönlich, als auch den öffentlichen oder privaten Schulträgern. Eine „Policy“ im Umgang mit diesen (hohen) Investitionen erscheint daher aus vielen Gesichtspunkten angebracht.

3 Inhaltliche Festlegung und Abgrenzung

3.1 Infrastruktur

3.1.1 Zielsetzung und Leitprinzipien

Den Grundsätzen der reflektierten Mediennutzung folgend, soll möglichst allen Schülerinnen und Schülern ein Zugang zur digitalen Welt und somit zu digitalen Lehr- und Lernangeboten ermöglicht werden. Dafür sollen Schulen den Lernenden und Lehrenden folgende Rahmenbedingungen anbieten:

- Internetzugang mit einer Bandbreite, die sinnvolles und effizientes Arbeiten ermöglicht
- WLAN in allen Unterrichtsräumen für Lernende sowie für Lehrkräfte
- Nutzungsmöglichkeit von Endgeräten (schuleigene Geräte und/oder mobile Endgeräte im Eigentum von Lernenden - BYOD)

- Festlegung der Nutzungsbedingungen seitens der Schule, z.B. in Form eines Nutzungsvertrages bzw. einer allgemein gültigen Hausordnung, hinsichtlich des pädagogisch-didaktischen Einsatzes digitaler Medien und Geräte sowie für Prüfungen

Ziel ist eine **effiziente Administration der IT-Infrastruktur** an Schulstandorten durch zunehmende Vereinheitlichung bei Hard- und Software sowie Verwaltung und Organisation des IT-Betriebs. Soweit möglich, kosteneffizient und sinnvoll umsetzbar, sollen Cloud-Dienste eine moderne IT-Infrastruktur bereitstellen (z. B. Office 365).

3.1.2 Vereinheitlichung von Hardware, Software und Verwaltung

Um eine ressourcenschonende und effiziente Betreuung von Bundesschulstandorten zu ermöglichen, ist eine Abstimmung von Bundesschulstandorten unabdingbar. Dies wird insbesondere zumindest auf jene Bundesschulstandorte zutreffen, die von ein und derselben IT-Systembetreuung betreut werden, z.B. Bundesschulen in einem IT-Betreuungscluster. Weiteres Potenzial soll ausgeschöpft werden, wenn sich darüber hinaus im Bundesland eine Einigung aller betroffenen Bundesschulstandorte über Hard- und Softwareanschaffungen sowie die Verwaltung der IT erzielen lässt.

Eine Abstimmung auf IT-Betreuungscluster-Ebene ist seitens aller im IT-Betreuungscluster vereinten Bundesschulen durchzuführen und betrifft zumindest die Neu- bzw. Ersatzbeschaffung von

- Firewall mit Konfiguration
- Netzwerkinfrastruktur (Verkabelung, Switches, WLAN)
- Serverinfrastruktur (Serverbetriebssystem, Virtualisierung, Managementlösung)
- Mobile Device Management (MDM)
- Sicherheitsmaßnahmen (IT-Security, Firewall, Schutz vor Malware, Backup)

Vereinheitlichung der Infrastrukturausstattung

In Hinblick auf Internetzugang und WLAN-Ausstattung wurden Empfehlungen für die jeweils für die Umsetzung und Implementierung verantwortlichen Schulerhalter ausgearbeitet. Die Unterlage versteht sich schulartenübergreifend für ganz Österreich und umfasst die Basis IT-Infrastruktur für das allgemeine Unterrichtsgeschehen (Volksschule, Sekundarstufe I und Sekundarstufe II). Ausgenommen sind darüberhinausgehende spezielle Anforderungen bestimmter Schul- und Ausbildungsformen (z.B. spezielle Schwerpunkte bei Berufsschulen oder HTL).

Link: https://www.bmb.gv.at/schulen/it/it_angebote/it_infrastruktur_empfehlung.pdf?61edw6

Vereinheitlichung der Firewall mit Sicherheitseinstellung

Wird in einem IT-Betreuungscluster von einem Bundesschulstandort eine neue Firewall beschafft, so ist darüber mit den anderen Bundesschulstandorten im IT-Betreuungscluster Einigung zu erzielen, welcher einheitliche Firewall-Typ eines Herstellers im IT-Betreuungscluster verwendet werden soll. Diese Vorgangsweise ermöglicht eine einheitliche Betreuung durch die IT-Systembetreuer/in sowie eine weitgehend idente Konfiguration der Sicherheitseinstellungen. Als zusätzliches Einsparungspotenzial ergibt sich die Möglichkeit, für einen IT-Betreuungscluster eine Ersatzfirewall für die Ausfallsicherheit zu beschaffen. Diese Kosten teilen sich die Bundesschulstandorte im IT-Betreuungscluster.

Vereinheitlichung von WLAN-Ausstattung mit Konfiguration

Wird in einem IT-Betreuungscluster von einem Bundesschulstandort ein neues WLAN beschafft, so ist darüber mit den anderen Bundesschulstandorten im IT-Betreuungscluster Einigung zu erzielen, welcher einheitliche WLAN-Typ eines Herstellers im IT-Betreuungscluster verwendet werden soll. Diese Vorgangsweise ermöglicht eine einheitliche Betreuung durch die IT-Systembetreuerinnen und Systembetreuer sowie eine weitgehend idente Konfiguration. Als zusätzliches Einsparungspotenzial ergibt sich die Möglichkeit, für einen IT-Betreuungscluster Ersatzgeräte, z.B. Controller, AccessPoints, für die Ausfallsicherheit zu beschaffen. Diese Kosten teilen sich die Bundesschulstandorte im IT-Betreuungscluster.

Vereinheitlichung der Serverbetriebssysteme und des Gerätemanagements

Um eine effiziente Betreuung aller Bundesschulstandorte in einem IT-Betreuungscluster zu ermöglichen, ist zumindest im IT-Betreuungscluster darüber Einigung zu erzielen, welches Serverbetriebssystem, welche Virtualisierungslösung und welche Geräte-Managementsoftware (Mobile Device Management) eingesetzt werden. Ergänzend können darüberhinausgehende spezielle Anforderungen bestimmter Schul- und Ausbildungsformen berücksichtigt werden. Für die Nutzung pädagogischer Software und Apps auf schülereigenen Geräten, z.B. Smartphones, Tablets, Notebooks (BYOD), wird die Verwaltung der mobilen Geräte mittels Managementsoftware empfohlen (Mobile Device Management, MDM).

Vereinheitlichung der Sicherheitsmaßnahmen

Betreffend der zu ergreifenden Sicherheitsmaßnahmen ist zwischen allen Bundesschulstandorten im IT-Betreuungscluster darüber Einigung zu erzielen, welche Schutzmaßnahmen ergriffen werden, z.B. IT-Security, Firewall-Regeln, Virenschutz/Schutz vor Malware, Sicherungsstrategien.

3.1.3 Dokumentation

Zu den genannten Bereichen, die im IT-Betreuungscluster zwischen den Bundesschulstandorten abgestimmt werden, ist von der IT-Systembetreuung eine Dokumentation anzufertigen und jedem Bundesschulstandort im IT-Betreuungscluster zur Verfügung zu stellen. Diese Dokumentation umfasst insbesondere:

- Firewall mit Konfiguration
- Netzwerkinfrastruktur (Verkabelung, Switches, WLAN)
- Serverinfrastruktur (Serverbetriebssystem, Virtualisierung, Managementlösung)
- Mobile Device Management (MDM)
- Sicherheitsmaßnahmen (IT-Security, Firewall, Schutz vor Malware, Backup)

Die Dokumentation beinhaltet sowohl eine technische Beschreibung als auch die getroffenen Vereinbarungen im IT-Betreuungscluster zwischen den Bundesschulstandorten hinsichtlich der genannten Bereiche, die im Sinne einer effizienten Betreuung vereinheitlicht wurden. Die Dokumentation ist laufend zu aktualisieren, zumindest jährlich.

3.1.4 Ebenen der IT-Betreuung

Um eine effiziente und hochverfügbare IT-Betreuung an Schulen zu ermöglichen, werden folgende Betreuungsebenen eingerichtet:

- Betreuung am Bundesschulstandort, z.B. durch IT-Manager/innen und/oder entsprechend geschulte Lehrkräfte bzw. IT-Systembetreuer/innen zur Unterstützung oder externe Unternehmen¹
- Betreuung von Bundesschulen in einem IT-Betreuungscluster, z.B. durch IT-Systembetreuer/innen, die an mehreren Schulstandorten tätig sind²
- Betreuung seitens der Bildungsdirektionen durch entsprechend geschulte Mitarbeiter/innen

Wo sinnvoll und möglich, soll eine Vereinheitlichung auf Bundeslandebene erzielt werden, z.B. durch Einsatz einheitlicher Firewall-Typen oder einer einheitlichen Managementsoftware.

3.2 Software

3.2.1 Verwaltungssoftware

Das Bundesministerium für Bildung, Wissenschaft und Forschung stellt den Bundesschulen Software für die Verrichtung von Verwaltungsaufgaben bereit. Die Nutzung dieser Softwareprodukte ist für die Bundesschulen verpflichtend, damit wird die Verwaltung vereinheitlicht und standardisiert:

- **Schülerverwaltungssoftware** („Sokrates Bund“, Einsatz an Bundesschulen verpflichtend)
- **Digitales Dienstpostsystem** („ISO-Web“, Kommunikationssystem für Bundesschulen mit übergeordneten Dienststellen)
- **Bewerbungsverwaltung** („Get your teacher“, Bewerbungstool für Schulen und Jungpädagog/innen)
- **Unterrichtsinformationssystem** („GP UNTIS“)
- **Unterrichtspersonalsystem** („PM UPIS“)
- **Dienst-E-Mail für Lehrende** (bildung.gv.at)

3.2.2 Pädagogische Software

Das Bundesministerium für Bildung, Wissenschaft und Forschung stellt als Erhalter für Bundesschulen zentral beschaffte Softwarelizenzen für die Ausbildung auf schuleigenen Geräten den Bundesschulstandorten zur Verfügung. Dies betrifft insbesondere folgende Bereiche:

- Betriebssystem und Office-Anwendungen, z.B. MS-ACH (Microsoft)
- Software für das berufsbildende Schulwesen, z.B. technische und kaufmännische Software (MathCAD, 3DCAD, Mesonic, BMD, SAP etc.)
- Lernplattformen

¹ vgl. BMBF-16.700/0008-II/2e/2014

² ebenda

Zusätzlich benötigte Software für den Unterrichtseinsatz kann von den Schulstandorten nach individuellen Bedürfnissen direkt beschafft werden.

Über eine Nutzung schülereigener Geräte im Rahmen des Unterrichts, wie z.B. Smartphones, Tablets und Notebooks, entscheidet die Lehrkraft. Ein sinnvoller Geräteinsatz, etwa durch Lern-Apps, Lernspiele, Kollaborationstools oder Lernplattformen, fördert das Lernklima und kann, z.B. durch Individualisierung, zu einem effizienteren Unterricht führen. In diesem Zusammenhang werden auch Angebote für Learning Analytics und Deep Learning eine noch größere Rolle spielen.

Mobile digitale Lernbegleiter im Unterricht

Um einen Einsatz digitaler Medien im Rahmen des Unterrichts zu ermöglichen und zu fördern, soll die Hausordnung der Schule den Einsatz mobiler digitaler Lernbegleiter (schuleigene sowie auch schülereigene, BYOD) für den Unterrichtseinsatz zulassen. Digitale Geräte sollen von den Lehrenden möglichst umfassend sowie zielgerichtet unter Anleitung der Lehrkraft zur Unterstützung des Unterrichts von den Schülerinnen und Schülern verwendet werden. Die Hausordnung kann, insbesondere zum Schutz der Lernenden vor übermäßiger Nutzung von Smartphones oder Tablets, die Nutzungsmöglichkeit auf den Unterricht beschränken.

4 Rechtsrahmen

Ziel der Internet Policy für das Publizieren von fachdidaktisch-pädagogischen Inhalten ist es, Richtlinien und Empfehlungen im Zusammenhang mit unterrichtsbezogenen Internetdiensten und Datendiensten an Schulen zur Verfügung zu stellen. Damit soll dem Vertrauensvorschuss der Schulpartner wie Lehrpersonen, Lernenden und Eltern entsprochen werden, die die neuen Technologien nutzen.

Während die Vervielfältigung von Materialien, die nicht aus Büchern und Publikationen stammen, die direkt für den Unterrichtsgebrauch geschrieben sind (Schulbücher, Lehrbücher im tertiären Bereich), im Klassenbereich möglich ist, stellt sich die Publikation von Materialien auf einer Schulhomepage, die theoretisch weltweit zugänglich ist, ganz anders dar. Hier sind Belange des Urheberrechts zu berücksichtigen, wobei auf jeden Fall bei Skizzen und Bildern Quellen anzugeben sind. Auch sollten auf öffentlich zugänglichen Webseiten personenbezogene Daten von Lernenden nur mit Zustimmung verfügbar gemacht werden (z.B. Klassenfotos mit Namensnennung, Gewinner/innen von Wettbewerben etc.). Texte schreibt man am besten um, sodass sie für die eigene Zielgruppe (Schülerinnen und Schüler) am besten passen. Im Einzelnen gilt:

4.1 Urheberrechtsgesetz

Die Urheberin/Der Urheber genießt für das von ihr/ihm geschaffene Werk den umfassenden Schutz des Urheberrechts und kann über ihr/sein Werk uneingeschränkt verfügen. Das gilt für alle Werkkategorien: Literatur, Musik, bildende Kunst (dazu zählen Malerei, Photographie, Grafik etc.) und Film – unabhängig davon, ob das jeweilige Werk in einer analogen oder digitalen Form vorliegt.

Fremde Werke dürfen im Rahmen der freien Werknutzung zitiert (vgl. § 42f UrhG Zitate), vervielfältigt, verbreitet und der Öffentlichkeit zur Verfügung gestellt werden, dabei sind jedoch die Zitatregereln zu beachten: Es muss im unmittelbaren Zusammenhang ersichtlich gemacht werden, dass ein fremdes

Werk - unter Nennung der Autorin/des Autors - verwendet wird. Das Zitat setzt immer ein eigenes Werk voraus, in dem auf das fremde Werk Bezug genommen wird. Ein Auszug aus einem fremden Werk alleine, sohin ohne einen Zusammenhang herzustellen, darf nicht verwertet werden.

Für Unterrichtszwecke dürfen Lehrende in dem dadurch gerechtfertigten Umfang Vervielfältigungsstücke von geschützten Werken in der für eine bestimmte Schulklasse erforderlichen Anzahl herstellen (Vervielfältigung zum eigenen Schulgebrauch) und verbreiten; dies gilt auch für digital vorliegende Werke (§ 42 Abs. 6 Urheberrechtsgesetz), sofern damit keine kommerziellen Zwecke verfolgt werden.

Erfolgt die Vervielfältigung zum eigenen Schulgebrauch in digitaler Form, so ist sicher zu stellen, dass diese Kopien nur für Lernende einer Klasse zugänglich gemacht werden und nicht (wenn auch nur unbeabsichtigt) im Internet publiziert werden.

Ergänzt wird diese Erlaubnis, durch die Bestimmung, dass für Unterrichtszwecke Schulen auch Werke zur Veranschaulichung im Unterricht für einen bestimmt abgegrenzten Kreis von Unterrichtsteilnehmenden vervielfältigen und der Öffentlichkeit zur Verfügung stellen dürfen, soweit dies zu dem jeweiligen Zweck geboten und zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt ist.

Die Befugnis zu dieser Vervielfältigung zum eigenen Schulgebrauch (§42 Abs.6 UrhG) und zur öffentlichen Zurverfügungstellung für Unterricht (§42g) gilt nicht für Werke, die ihrer Beschaffenheit und Bezeichnung nach zum Schul- oder Unterrichtsgebrauch („Schulbücher“ oder „AV-Schulmedien“) bestimmt sind.

Daher sind Netzwerklaufwerke und Lernplattformen, z.B. mittels Passwort, gegen den Zugriff Dritter abzusichern.

Falls Lehrende selbst Unterrichtsunterlagen erstellen und beabsichtigen diese auch größeren (d.h. über eine Klasse hinausgehenden) Nutzerkreisen zur Verfügung zu stellen, gelten uneingeschränkt die Regeln für das Verwenden fremder Werke (Zitat bzw. Einholung der Genehmigung zur Verwendung).

Durch die mittlerweile zur Verfügung stehenden technischen Werkzeuge (z.B. Google Bildersuche) ist es für Rechteinhaber leicht geworden, zu kontrollieren, wo im Web ihre Werke verwendet werden und damit auch feststellen, ob der jeweiligen Verwendung auch zugestimmt wurde. Für die Verwendung im nicht kommerziellen Bereich des Internets wird daher auf das wachsende Angebot an Fotos und Grafiken, aber auch Musik hingewiesen, das im Rahmen einer Creative Commons – Lizenz genutzt werden darf.

Grundsätzlich: Wenn man Fotos, Grafiken oder Texte auf einer Website entdeckt, darf man sie dann auf die eigene Website übernehmen?

Fotos, Zeichnungen, Cartoons etc., auf keinen Fall. Diese genießen auch dann Urheberrechtsschutz, wenn sie nur ganz primitiv sind. Bei Grafiken und Texten kommt es darauf an, ob sie Werkcharakter im Sinne des Urheberrechtsgesetzes (UrhG) genießen, d.h. eine sogenannte eigentümliche geistige Schöpfung darstellen. Das ist eine relativ schwere Abgrenzung, die mit großer Unsicherheit behaftet ist, weshalb man auch davon die Finger lassen sollte. Was man schon darf, ist auszugsweises Zitieren (wenn man die Quelle angibt) oder auf die fremde Information linken; der Link sollte allerdings nicht in einem

Frame der eigenen Seite dargestellt werden und sollte insgesamt so ausgeführt werden, dass für den User klar erkennbar ist, dass er damit auf eine andere Website wechselt. Ansonsten sollte man fremde Inhalte (vor allem Fotos) nur mit Zustimmung des Urhebers (= Ersteller) übernehmen, wobei man sich versichern sollte, dass der Übergeber wirklich der Ersteller ist. Es nützt im Streitfall wenig, wenn sich herausstellt, dass derjenige, der die Bilder überlassen hat, selbst nicht deren Urheber ist. Man haftet vielmehr selbst trotzdem für die Urheberrechtsverletzung.

4.2 Bildnisschutz

Beim Betrieb einer Schulhomepage (oder anderer Formen der Veröffentlichung wie Projektwebseiten, öffentlich zugänglichen Blogs, Wikis, Kurse) ist der sog. Bildnisschutz nach § 78 Urheberrechtsgesetz zu beachten. Die Veröffentlichung von Bildern und Videos von Personen darf nur mit deren Einverständnis (bzw. dem Einverständnis der Eltern) erfolgen.

Beim "Recht am eigenen Bild" handelt es sich um ein Persönlichkeitsrecht, das in § 78 Urheberrechtsgesetz geregelt ist.

Nach dieser Bestimmung dürfen Bildnisse von Personen nicht veröffentlicht werden, wenn dadurch "berechtigte Interessen des Abgebildeten verletzt werden". Personenfotos dürfen vor allem nicht in einen negativen Zusammenhang gebracht werden; dabei kann es auch auf den Text im Zusammenhang mit dem Bild ankommen. Der Begriff "negativer Zusammenhang" ist aber weit auszulegen; es genügt schon die Möglichkeit der Missdeutung, dass das berechtigte Interesse der/des Abgebildeten verletzt wird, und die Veröffentlichung wird damit unzulässig. Andererseits kommt es nicht auf das subjektive Empfinden der/des Abgebildeten an, sondern es ist ein objektiver Maßstab anzulegen. Ist nach objektiven Kriterien kein berechtigtes Interesse an einem Unterbleiben der Veröffentlichung erkennbar, besteht kein Unterlassungsanspruch.

Als grobe Richtschnur hilft es vielleicht, wenn man sich fragt, ob es irgendeinen objektiven Grund geben könnte, warum eine Person gegen die Veröffentlichung in der konkreten Form sein könnte.

4.3 Datenschutz

Mit der zunehmenden Digitalisierung des Alltags, dem Potenzial elektronischer Medien zur Vereinfachung von Verwaltungsabläufen und zur didaktischen Unterstützung des Unterrichts spielen Informationstechnologien in der Schule eine wichtige Rolle. Der Einsatz von IT & Internet bedeutet aber auch die zunehmende Verwendung von personenbezogenen Daten, vor allem von Lernenden. Die Verwendung dieser Daten unterliegt rechtlichen Regeln, die im Schulbereich im Besonderen zu berücksichtigen sind, da Lernende als Minderjährige besonders schützenswert sind. Für die Schulleitung bzw. Administration ebenso wie für die IT-Kustodinnen und IT-Kustoden sowie Systembetreuerinnen und Systembetreuer und generell für alle Lehrenden stellen sich zahlreiche, immer komplexer werdende Fragen der Verwendung personenbezogener Daten in der Schule.

Generell kann davon ausgegangen werden, dass für die Verarbeitung personenbezogener Daten im Rahmen der Schulverwaltung bzw. auf Lernplattformen eine gesetzliche Grundlage erforderlich ist, die etwa für die Anwendungen Schülerverwaltung, elektronisches Klassenbuch, Lernplattform, Digi4school, Office 365 (MS-ACH) etc. durch das Ressort zentral berücksichtigt wurde. Generell wird für alle zentral

bereitgestellten Komponenten auch die Konformität zu den bestehenden datenschutzrechtlichen Bestimmungen geprüft.

Für schulautonome Projekte ist zu beachten, dass die Schulleitung gemäß Bildungsdokumentationsgesetz auch der datenschutzrechtliche Auftraggeber (neuer Name: datenschutzrechtlicher Verantwortlicher) ist. Insbesondere bei der Beauftragung von externen IT-Partnern, die Anwendungen der Schule betreuen, ist zu beachten, dass jeweils eine gültige Dienstleistervereinbarung (neuer Name: Vereinbarung mit Auftragsverarbeitern) geschlossen wird.

Verkehrsdaten müssen unmittelbar nach Beendigung einer Kommunikation gelöscht werden (zum Kommunikationsgeheimnis: §§ 93ff TKG). Log-Dateien mit personenbezogenen bzw. pseudonymisierten Daten sind generell nicht zulässig und dürfen nur auf Grund einer geeigneten gesetzlichen Verpflichtung (§ 14 DSGVO 2000, §§ 79 ff BDG) möglichst kurz verarbeitet (siehe DSGVO bzw. DSGVO) werden. (Begründung: Schulen sind keine öffentlichen Kommunikationsdienstleister und benötigen daher auch keine personenbezogenen Daten für Verrechnungszwecke. Vorratsdatenspeicherung wurde durch den VfGH aufgehoben und bis dato in Österreich auf gesetzlicher Ebene nicht wieder neu aufgegriffen)

Art. 32 DSGVO sieht als technisch organisatorische Maßnahme zur Sicherheit der Datenverarbeitung grundsätzlich die Pseudonymisierung und Verschlüsselung personenbezogener Daten vor.

Aus Sicht des BMBWF wird ein überwiegender Großteil der notwendigen Änderungen aufgrund der einschlägigen Rechtsnormen zum neuen EU-Rechtsrahmen der Datenschutzgrundverordnung, die seit 25. Mai 2018 das „alte“ Datenschutzgesetz 2000 ersetzt hat, durch die Zentralstelle bzw. den Bildungsdirektionen (Stadtschulrat für Wien/Landesschulräte) umgesetzt, sodass an den Schulen selbst kein großer Handlungsbedarf entstehen wird.

Für Lehrende gelten die Arbeitnehmerschutzbestimmungen, für Lernende – entsprechend dem Alter – ergänzend auch die jeweiligen Jugendschutzgesetze. Der Jugendschutz ist von Bundesland zu Bundesland unterschiedlich geregelt und soll Kinder und Jugendliche vor gesundheitlichen, sittlichen und sonstigen Gefahren (Übervorteilung) bewahren. Im Hinblick auf das Internet ist diese Verantwortung konkret vom Medienanbieter wahrzunehmen. Erschwerend ist, dass im Gegensatz zu Gaststätten und Kinos im Internet keine direkte Alterskontrolle quasi face-to-face möglich ist. Ev. Verstöße sind aufgrund der Weitläufigkeit des Internets schwer zu ahnden.

Hinsichtlich eines vernünftigen Jugendmedienschutzes obliegt es den Lehrpersonen und insbesondere den Eltern, Kindern und Jugendlichen frühzeitig den verantwortungsvollen Umgang mit dem Medium Internet zu vermitteln.

4.4 Empfehlungen für sichere Internetnutzung im Unterrichtseinsatz

- Festlegung einer Internet-Nutzungsvereinbarung für den Standort – auf der Basis „keine rechtswidrigen Handlungen im Schulnetz“ – als Teil der Hausordnung. Diese Vereinbarung sollte als Grundlage für die Schaffung einer Security Awareness am Standort dienen. Beispiel einer Benutzerordnung der Universität Wien: <https://zid.univie.ac.at/uaccount-benutzungsordnung/>
- Gemäß der Datenschutzgrundverordnung, sowie des Telekommunikationsgesetzes dürfen personenbezogene und pseudoanonymisierte Log-Dateien ohne explizite Zustimmung nicht

gespeichert und im Sinne von Profiling nicht weiterverarbeitet werden. Ausgenommen ist das kurzfristiges Speichern von Authentifizierungsvorgängen zur Fehlersuche – sowie technisch unveränderbare Voreinstellungen – es gilt aber auch hier die Richtlinie: möglichst minimal personenbezogen (sowie entsprechender Verweis in der Internet-Nutzungsvereinbarung). Beispiel: Anmeldung am Schulnetz darf nicht rückführbar bzw. verknüpfbar mit dem Surfverhalten der Person sein.

- Als technische Maßnahme werden Contentfilter und Endpointsecurity empfohlen. Beispiele: illegale Inhalte, Waffen, Gewalt, kriminelle Aktivitäten, extremistische Inhalte, Drogen (warnen), Pornografie. Details der Einstellungen sollen am Schulstandort unter Einbeziehung von SGA bzw. Schulforum entwickelt werden und auch in die Internet-Nutzungsvereinbarung einfließen.
- Folgend einer technischen Grundtendenz der Datenschutzgrundverordnung sollen personenbezogene Daten prinzipiell verschlüsselt gespeichert und übermittelt werden.
- Technische Komponenten im Schulnetzwerk sollten aktuell gehalten werden, Updates, Virendefinitionen etc. ebenfalls regelmäßig aktualisiert werden. Warnungen von CERTs etc., umgehend berücksichtigen. Im Sinne einer Risikominimierung wird empfohlen, nur die „mission critical“ Services und Dienste am Schulstandort selbst zu implementieren.
- Einige juristische Gutachten kommen auch zum Schluss, dass WhatsApp nicht zu schulischen Zwecken eingesetzt werden darf, da die Nutzungsbedingungen (Stand: 8/2016) nur die private Nutzung zulassen (Schulverwaltung ist nicht private Nutzung), sowie der Verwender von WhatsApp bestätigt, dass er autorisiert sei, regelmäßig die Kontaktdaten seines Adressbuches zur Verfügung zu stellen. Diese Authorisierung liegt in der Schulverwaltung üblicherweise nicht vor. Ausführlich dazu: *Burgstaller, Urheberrecht für Lehrende; Wien 2017; weiters Datenschutzbeauftragter Niedersachsen, Merkblatt für die Nutzung von „WhatsApp“ in Schulen, https://www.lfd.niedersachsen.de/download/124022/Merkblatt_fuer_die_Nutzung_von_WhatsApp_in_Schulen.pdf*
- Für Unterrichtszwecke und Schulverwaltung gibt es spezielle Angebote, sodass die allgemeinen sozialen Netze (WhatsApp, Facebook, Instagram etc.) dort nicht benötigt werden.
- Lehrer/innen sind um mit Schüler/innen kommunizieren zu können, nicht auf soziale Netze, wie z.B. WhatsApp, Facebook, Instagram, angewiesen. Das BMBWF empfiehlt selbst IT-Anwendungen für elektronische Kommunikation (z. B. Webeinsicht in das elektronische Klassenbuch; Lernplattformen; Kommunikation über den Schüler/innen von der Schule zur Verfügung gestellten E-Mail-Adressen). Eine schulische Belange betreffende Kommunikation zwischen Schüler/innen und Lehrkräften sollte deshalb über diese Möglichkeiten erfolgen.
- Bilden Schüler/innen und Lehrer/innen im privaten Bereich Gruppen in sozialen Medien, z. B. WhatsApp-Gruppen, sind sie selbst für die Beachtung des Datenschutzes verantwortlich. Wie jeder andere dürfen sie keine nicht allgemein bekannten Daten von Personen austauschen, die nicht Teil der Gruppe sind. Gleiches gilt für Daten, die einem Mitglied von einem anderen unter dem Siegel der Verschwiegenheit anvertraut wurden. Auch hier bringt die DSGVO keine Veränderungen.

5 Literatur

Datenschutz für die digitale Schülerverwaltung:

<http://pubshop.bmbf.gv.at/detail.aspx?id=586#>

Folienskriptum: Datenschutz, IT-Sicherheit und Urheberrechte in der Schulverwaltung:

<http://pubshop.bmbf.gv.at/detail.aspx?id=648>

Datenschutzgrundverordnung:

<http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE>

Empfehlung für die Basis IT Infrastrukturausstattung an österreichischen Schulen:

https://bildung.bmbwf.gv.at/schulen/it/it_angebote/it_infrastruktur_empfehlung.pdf?61edw6

Dieses Dokument wird auf dem Webserver des BMBWF bereitgestellt und laufend aktualisiert.

Wien, 27. August 2018

Für den Bundesminister:

Mag.^a Heidrun Strohmeyer

Elektronisch gefertigt