DSGVO für Lehrpersonen

Warum Datenschutz in der Schule?

- Die Verwendung der Daten von Schüler/innen wird aufgrund neuer Technologien für den Unterricht immer wichtiger
- Unternehmen beuten Daten von Schüler/innen zunehmend aus
- Die Schüler/innen haben ein Recht darauf, dass auch die Lehrer/innen ihre Daten schützen

Was kann ich als Lehrkraft tun?

- **Bewusstsein**: Wann und in welchem Zusammenhang verwende ich Daten von Schüler/innen?
- **Weitergabe**: Wem gebe ich die Daten weiter und wieso?
- **Sicherheit**: Wie verhindere ich, dass die Daten in falsche Hände geraten?
- **Apps**: Mit welchen Apps arbeite ich? Sammeln Firmen dabei Schülerdaten?
- **Löschen**: Daten sollen nicht gesammelt werden! Lösche ich die Daten, wenn ich sie nicht mehr brauche?

E-Mails

Berufliche Kommunikation über private E-Mail-Adressen zu führen oder weiterzuleiten, ist wie in anderen Berufen nicht zu empfehlen.
Pseudonymisierung: Namen von SchülerInnen zB in eMails abkürzen: Pe Ma – Peter Mayer

Einverständnis

Für jede Datenverarbeitung, für die es keine gesetzliche Grundlage gibt, braucht es je nach Alter (bis 14 Jahre) die Einwilligung der Jugendlichen oder der Eltern.

Messenger, WhatsApp

Für die Kommunikation unter Lehrenden und zwischen Lehrkräften und SchülerInnen sollen natürlich auch alle Möglichkeiten digitaler Technologien offenstehen. Aber nicht jeder Anbieter ist geeignet. Aus Unwissenheit oder Bequemlichkeit wurden bisher oft WhatsApp (das seit 2014 zum Facebook-Konzern gehört) und der Facebook-Messenger genutzt. Genau wie Facebook selbst, sind sie nicht nur aus datenschutzrechtlicher Sicht problematisch für den Einsatz im Unterricht. Das ist nicht nur die Ansicht von Datenschützern, sondern auch offizielle Position des Ministeriums für Bildung, Wissenschaft und Forschung.

Für die **gesicherte Kommunikation mit Eltern** sind u.a. folgende Dienste sinnvoll:
digitale Mitteilungshefte: SchoolUpdate, SchoolFox, WebUntis, skooly.at, klassenpinnwand.at, ...
WhatsApp-Ersatz: Signal, Wire, Mattermost, Threema, Pidgin und andere

Schulleitung
Da die Schulleitung verantwortlich ist, kann sie auch Weisungen zum datenschutzkonformen Umgang geben. Datenschutzrechtlich sinnvoll ist, dass sich die Lehrperson zu gewissen Verhaltensregeln verpflichten, um nicht haftbar zu sein. Dazu gehören Punkte wie das regelmäßige Updaten des Betriebssystems, das Einrichten einer automatischen Bildschirmsperre und das Verbot der Nutzung unsicherer Cloud-Dienste. Hier wird also kein Fachwissen verlangt, sondern nur ein Mindestmaß an Sorgfalt.

Aufzeichnungen für Beurteilungen
Wenn ich als Lehrkraft Microsoft mit meinem Schulkonto nutze, um solche Aufzeichnungen zu führen, ist die rechtliche Situation durch die Verträge mit dem Bildungsministerium gedeckt. Im Gegensatz dazu ist ein Google-Konto denkbar ungeeignet, um Daten über Schüler zu speichern. Google analysiert alle Informationen inklusive Textinhalten von E-Mails. Das notwendige Datenschutzniveau, um Daten von bzw. über Schutzbefohlene zu speichern, ist keinesfalls gegeben.

Datenschutz als Thema für den Unterricht
Übersichtlich aufbereitete Information zu den Rechten aus der DSGVO von der Grundrechtsorganisation epicenter.works finden Sie hier:
https://epicenter.works/content/dsgvo-du-hast-rechte-nutze-sie

das alltägliche Verhalten am Arbeitsplatz
- Wenn Sie den PC-Arbeitsplatz verlassen, sperren Sie diesen mittels Bildschirmschoner.
- Lassen Sie wichtige Unterlagen weder am Schreibtisch noch elektronisch am PC oder nach Besprechungen offen liegen, sondern versperren diese (Schreibtischlade oder PC-Sperre) bzw. nehmen Sie sie in Ihr Büro zurück.
- Wenn Sie unterwegs sind, achten Sie darauf, dass vertrauliche Informationen nicht auf Ihrem Notebook ungeschützt verfügbar sind.
- Wenn Sie Verdacht schöpfen, setzen Sie sich unmittelbar mit Ihren Datenschutzbeauftragten der Bildungsdirektion für Vorarlberg in Verbindung.

Umgang mit Passwörtern

verantwortungsvolle Umgang mit Passwörtern, mit denen der Zugang zu Anwendungen geschützt ist. Fahrlässigkeit ist hier kein Kavaliersdelikt und kann dienstrechtliche Konsequenzen nach sich ziehen.

- Verwenden Sie nicht das gleiche Passwort im Dienstbereich wie auch im privaten Bereich (z.B. private Mail-Adressen, Facebook, Twitter usw.) – unterschiedliche Passwörter für verschiedene Anwendungen.
- Passwörter sind in regelmäßigen Abständen zu ändern.
- Passwörter dürfen nicht weitergegeben werden.
- Passwörter unbeobachtet von Dritten eingeben.
- Wenn Sie den Verdacht haben, dass Ihr Passwort einem Dritten bekannt ist, ändern Sie es umgehend.
- Schreiben Sie Passwörter nicht auf, versperren Sie diese eventuell in einem elektronischen Passworttresor.
- Es gilt das Grundprinzip: Das Passwort muss für Sie leicht merkbar, aber für andere schwer erratbar bzw. aufgrund seiner Merkmale nicht ableitbar (z.B. Geburtsdatum, Namen) sein.
- Verwenden Sie bei der Gestaltung des Passwortes immer eine Kombination aus Buchstaben, Zahlen und Sonderzeichen.
- Helfen Sie sich mit Eselsbrücken, z.B. für das Passwort **„IfmsadUi2W!**“: „**Ich freue mich schon auf den Urlaub in 2 Wochen!“**.
- Ist Ihr Passwort gut: http://www.passwordmeter.com/
- Alternative: Handysignatur

Sicherheit auch außerhalb des Büros

- Nehmen Sie nur jene Daten mit, die Sie auch tatsächlich benötigen.
- Achten Sie bei der Verwendung des Notebooks, Tablets, Smartphones, usw. in öffentlichen Bereichen (Flughafen, Bahnhof usw.), dass niemand Ihre vertraulichen Informationen mitliest oder mithört.
- Auf Dienstreisen behalten Sie Notebook, Tablet, Handy, Smartphone, Datenstick, usw. immer im Handgepäck.
- Achten Sie bei Ihren mobilen Geräten auf einen aktuellen Virenscanner führen Sie regelmäßig Updates durch.
- Automatische Formularfunktion deaktivieren
- Individueller Login notwendig
- USB-Stick, externe Festplatten verschlüsseln (zB mit Bitlocker)

Erstellt von Dir. Hanno Metzler, MS Hittisau in Abstimmung mit der Bildungsdirektion für Vorarlberg - Juni 2019