SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Leit-
faden

Datenschutzkonformer Einsatz digitaler Lehrmittel

I. Antragstellung und Installation digitale Lehrmittel (Softwareprozess)

- Digitale Lehrmittel sind über die Pädagogischen Medienkoordinatoren der Schulen (PMK) über das Ticketsystem beim AI zu bestellen.
- Die beantragte Software wird vom SA und AI geprüft, ob sie technisch auf den zur Verfügung stehenden Geräten eingesetzt werden kann. Des Weiteren wird geprüft, ob und inwieweit die bestellte Software pädagogisch zweckmässig eingesetzt werden kann. In Abstimmung mit dem/der schulischen Datenschutzbeauftragten wird ein datenschutzkonformer Einsatz der jeweiligen Software geprüft.
- Lehrpersonen sollten in Rücksprache mit der Schulleitung – sofern möglich – eine Lizenz für das digitale Lehrmittel beantragen. Derart sollte sichergestellt werden können, dass das Lehrmittel ohne Werbeeinschaltung genutzt wird. Ausserdem entfällt über ein Lizenzmodell vielfach eine webbasierte Registrierung.
- Das digitale Lehrmittel wird für die antragstellenden Lehrpersonen und – soweit erforderlich – auf den Endgeräten der Schülerinnen und Schüler freigegeben (Datenminimierung).

II. Nutzung digitaler Lehrmittel (Anwendung)

- Sofern ein digitales Lehrmittel auf den Endgeräten von Schülerinnen und Schülern installiert wird, erfolgt deren Anwendung und **Anmeldung unter Anleitung der zuständigen Lehrperson**.
- Soweit eine zweckmässige Nutzung **ohne Account eines Schülers oder einer Schülerin oder deren Registrierung möglich** ist, ist auf eine Registrierung zu verzichten (dies gilt insbesondere für webbasierte Anwendungen oder Plattformen).
- Sofern eine als digitales Lehrmittel genutzte Online-Plattform (z.B. ein Nachrichtenportal, Miro etc.) mittels Logins oder Registrierung genutzt werden kann, muss im Vorfeld eine **Datenschutzprüfung** in Abstimmung mit dem/der schulischen Datenschutzbeauftragten erfolgen und sichergestellt werden, dass die Datenverarbeitung auf das erforderliche Minimum begrenzt wird.
- Wenn ein digitales Lehrmittel die Erstellung eines Profils für Schülerinnen und Schüler erlaubt, dies für die Nutzung des Lehrmittels aber nicht erforderlich ist, ist die Bekanntgabe personenbezogener Daten (Name, Vorname, E-Mail-Adresse etc.) zu verhindern. Es sind stattdessen **pseudonymisierte Accounts** zu erstellen und zu verwenden (Beispiel: anstatt Maxi Muster einfach MaMu oder anderes Pseudonym bzw. sollte die pseudonymisierte schulische Alias-Adresse verwendet werden); zudem sollten Schülerinnen und Schüler sensibilisiert werden, keine personenbezogenen Bilddaten in Profilen zu hinterlegen, sondern gegebenenfalls nur auf pseudonyme Avatare zurückgreifen.

SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

- Bei Erstellung von Profilen von Schülerinnen oder Schülern sollte der gewählte Benutzername **keine Rückschlüsse auf die Identität der Person** oder sonstige Angaben (Beispiel: Schulbezeichnung) zulassen.
- **Zugriffsberechtigungen** sind auf das für den schulspezifischen Einsatz erforderliche Ausmass **einzuschränken** (Anpassung in Einstellungen von Applikationen, z.B. bezüglich Kamera, Standort, Mikrophon etc.).
- Lehrpersonen haben Schülerinnen und Schüler im Umgang mit Foto-, Audio- und Videoaufnahmen zu Schulunterrichtszwecken zu sensibilisieren. Sofern Foto-, Audio- und Videoaufnahmen nicht zu Schulunterrichtszwecken erfolgen, bedarf es unbedingt einer **vorherigen Einwilligung** der Erziehungsberechtigten.
- Die **Passwortvergabe** hat den Standards für **sichere Passwörter** zu entsprechen (siehe dazu die Richtlinie über die Nutzung der Schulinformatik).
- Eine verpflichtende Nutzung von privaten Endgeräten im Schulunterricht (im Pflichtschulbereich) ist nicht zulässig. Es braucht eine Einwilligung der Erziehungsberechtigten.
- Beim Einsatz von frei zugänglichen **Textverarbeitungsprogrammen**, **Übersetzungsprogrammen,** auf «***künstlicher Intelligenz***» basierenden Programmen (z.B. DeepL.com, ChatGPT) sind Lehrpersonen, Assistenzpersonal sowie Schülerinnen und Schüler zu sensibilisieren, dass **keine personenbezogenen Daten eingegeben** werden dürfen.
- **Besonders schützenswerte personenbezogene Daten** (bspw. Gesundheitsdaten) von Lehrpersonal, Assistenzpersonal sowie Schülerinnen und Schülern **dürfen über digitale Applikationen/Lehrmittel nicht verarbeitet werden** (ausgenommen bspw. Angaben zur Religionszugehörigkeit im Fach Ethik und Religionen).

III. Empfehlungen

- Im Primarschulbereich wird die Verwendung von altersgerechten **Internetsuchmaschinen für Kinder** (fragfinn.de, blinde-kuh.de, duckduckgo oder andere) empfohlen.
- Sofern für digitale Lehrmittel spezielle **kind- und jugendgerechte Versionen** verfügbar sind, sollte nach Möglichkeit auf diese zurückgegriffen werden.

IV. Löschung / Deinstallation

- Die Lehrperson ist für die **komplette Löschung** der von ihr erstellen Konten von Schülerinnen und Schülern auf digitalen Lehrmitteln zuständig und verantwortlich.

V. Ampelsystem zur Einstufung von Datensätzen

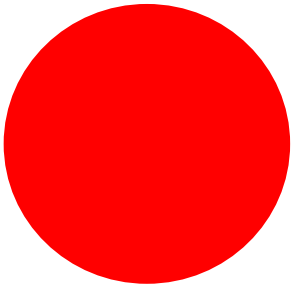
Dem Lehrpersonal sowie Assistenzpersonal wird empfohlen sich bei der Einstufung von Daten, d.h. zur Zuordnung von Personen- und Sachdaten, an folgendem Ampelsystem[1] zu orientieren. Dieses bietet eine vereinfachte Übersicht und soll dazu dienen, leichter einzuordnen, welche Daten auf welche Weise verarbeitet werden dürfen.

[1] vgl dazu Datenschutz-Ampel für Schulleitungen und Schulpersonal der Pädagogischen Hochschule Thurgau, Medien- und Didaktikzentrum, Version 1.0. (Stand 06.08.2020).

SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Besonders schützenswerte Personendaten

Grundsätzlich gilt: Beim Einsatz von digitalen Lehrmitteln sollten keine besonders schützenswerten Personendaten verarbeitet (z.B. gespeichert) werden. Besonders schützenswerte Personendaten dürfen nur über die den **Schulen zur Verfügung gestellte Verwaltungssoftware (z.B. Lehreroffice, LiSA etc.)** verarbeitet werden.



- Zeugnisse, Notenlisten, Leistungsbeurteilung, Leistungsevaluation
- Sensible unvorteilhafte Fotos, Videos oder Audiodateien von Schülerinnen und Schülern/Lehrpersonen usw. (z.b. entstanden bei Ausflügen, Klassenfahrten, Schulveranstaltungen etc.)
- Gesundheitsdaten (z.B. pädagogisch-therapeutische Massnahmen usw.)
- Sensible Informationen über schulische Massnahmen (Schulausschluss usw.)
- Personalinformationen (Protokoll Mitarbeitendengespräche)
- Informationen über berufliche, finanzielle und soziale Verhältnisse der Eltern (z.B. Scheidung)
- Gesundheitsinformationen (Arztzeugnisse usw.)

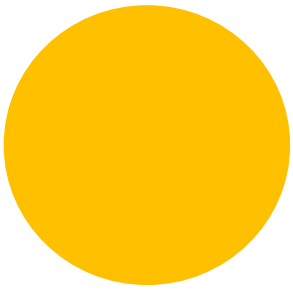
Beispiel: Eine Ablage von Klassenfotos sollte nicht auf MS-Teams, sondern über die Schulverwaltungslösung erfolgen; werden Fotos auf Klassenfahrten (vorbehaltlich einer Einwilligung) von Lehrpersonen ausnahmsweise auf privaten Mobiltelefonen aufgenommen, ist sicherzustellen, dass die Fotos nur lokal gespeichert und nicht in eine private Cloud übertragen werden; nach sicherer Übertragung der Fotos – bspw. über AirDrop oder andere Bluetooth-Verbindung – auf einen schulischen Datenträger, sind sie umgehend vom privaten Datenträger zu löschen. Grundsätzlich sollte für Fotoaufnahmen auf Klassenfahrten eine Schul-Kamera verwendet werden.

SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Personendaten

«Personendaten» dürfen nur soweit verarbeitet werden, wie es für schulische Zwecke unbedingt erforderlich ist.

Für Schulunterrichtszwecke an öffentlichen Schulen in FL ist eine Nutzung von MS 365-Diensten sowie über den Apple-School-Manager bezogene Applikationen zulässig. Eine Verarbeitung von Personendaten zu Schulzwecken ist über die zur Verfügung gestellten IT-Ökosysteme (iCloud im Primarschulbereich; Microsoft-Dienste an Sekundarstufe) gestattet.

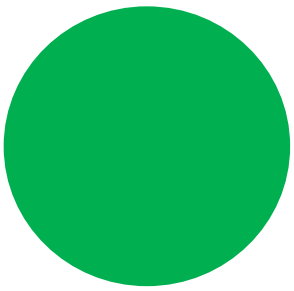


- Arbeits- und Übungsblätter mit Namensbezug (auf Dokument ist Vorname und/oder Nachname von Schülerinnen und Schülern ersichtlich)
- Foto-, Video- oder Audiodateien von Schülerinnen und Schülern aus dem Schulunterricht (z.B. Präsentiertraining oder Sprachunterricht, **ausgewählte** Fotos von Schulveranstaltungen)
- Nicht sensible Texte mit Namensbezug

Schutz: Als Personendaten qualifizierte Daten/Dokumente sollten – soweit unbedingt erforderlich – vor Ablage in anderen Cloud-Lösungen zumindest pseudonymisiert und/oder gegebenenfalls verschlüsselt werden (etwa durch Erstellung eines passwortgeschützten ZIP-Archivs).

Sachdaten

Sachdaten, d.h. Informationen ohne Personenbezug unterliegen nicht dem Datenschutz.



- Arbeits- und Übungsblätter ohne Namensbezug (z.B. kein Name ersichtlich)
- Fotos-, Videos- oder Audiodateien, auf denen keine Person erkennbar bzw. identifizierbar ist, ohne Namensbezug
- Texte ohne Personen- oder Namensbezug (z.B. persönliche Ansichten zu Politik/Religion/Weltanschauung)

Schutz: Sachdaten/Inhaltsdaten ohne jeglichen Personenbezug können aus datenschutzrechtlicher Sicht uneingeschränkt zu Schulunterrichtszwecken verarbeitet und gespeichert werden. Achtung: Amtsgeheimnisse sollten gewahrt bleiben.

Vaduz, August 2024, Version 1.1