Kanton Schaffhausen
Erziehungsdepartement
Herrenacker 3
CH-8200 Schaffhausen
schulen.datenschutz@sh.ch

Kanton Schaffhausen
Datenschutzbeauftragter
Vorstadt 18
CH-8200 Schaffhausen

Version: 01.09.2021

Merkblatt
Digitale Datenablage und Kommunikation an den Schulen der Primar- und Sekundarstufe I

1. Ausgangslage

Bei der digitalen Datenspeicherung und Kommunikation an den Schulen müssen datenschutzrechtliche Vorgaben beachtet werden. Diese verhindern, dass die Persönlichkeitsrechte der Schülerinnen und Schüler, der Lehrpersonen und der übrigen Angestellten einer Schule sowie auch der gesetzlichen Vertretung verletzt werden. Der Umgang mit Personendaten wird im Kanton Schaffhausen durch das kantonale Datenschutzgesetz vom 7. März 1994 (SHR 174.100) geregelt.

Verantwortlich für die Einhaltung des Datenschutzgesetzes sind die Schulgemeinden. Die vorliegenden Empfehlungen des Erziehungsdepartementes sollen den Schulgemeinden aufzeigen, wie sie diese Verantwortung wahrnehmen können.

2. Datenkategorien im schulischen Bereich

Informationen, die digital gespeichert oder übermittelt werden, sind je nach Inhalt unterschiedlich sensibel. Das Datenschutzgesetz unterscheidet zwischen zwei verschiedenen Kategorien von Personendaten. Allgemeine Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen (z.B. Name oder Adresse) werden als «Personendaten» bezeichnet. Bei Personendaten, bei denen aufgrund ihrer Bedeutung eine grössere Gefahr einer Persönlichkeitsverletzung besteht, handelt es sich um «besonders schützenswerte Personendaten». Dazu gehören zum Beispiel schulpsychologische Berichte, Aufzeichnungen von Lehrpersonen über das Verhalten oder die Leistungen von Schülerinnen und Schülern oder Gesundheitsdaten. Den «Sachdaten» werden diejenigen Informationen zugeordnet, die keine Personendaten sind, die sich somit nicht auf eine bestimmte oder bestimmbare Person beziehen.

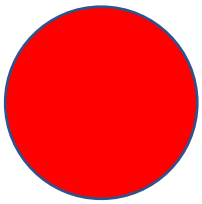
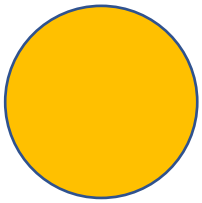
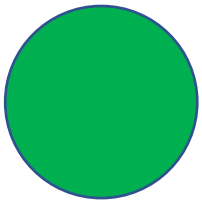
2.1 Beachte:

- Der Personenbezug besteht nicht nur, wenn unmittelbar aufgrund des Namens die betroffene Person bestimmt ist, sondern auch wenn die betroffene Person im konkreten Kontext bloss mittelbar bestimmt werden kann (z.B. «die Schulleiterin der Schule xy»).
- Zu beachten ist, dass je nach Situation auch Sachdaten oder Personendaten zu besonders schützenswerten Daten werden können (z.B. leben die Eltern aufgrund von Gewalt in der Familie getrennt, ist auch die simple Adresse besonders schützenswert).

Eine datenschutzkonforme Datenspeicherung und Kommunikation erfordern eine vorgängige Kategorisierung der Daten. Je nach Kategorie sind die Daten unterschiedlich streng zu schützen und dementsprechend unterscheiden sich die zulässigen technischen Lösungen bei der Speicherung und Übermittlung.

Mit der nachfolgenden Tabelle soll die Einteilung der Daten in die drei Kategorein verdeutlicht werden:

Tabelle 1: Datenkategorien

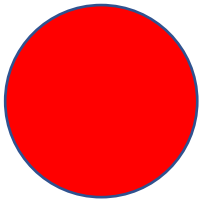
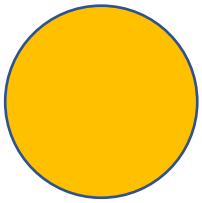
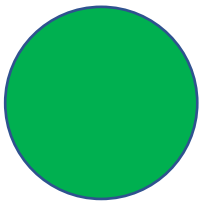
Datenkategorien	**Art der Informationen**
Besonders schützenswerte Personendaten 	Informationen, die sich auf eine bestimmte oder eine bestimmbare Person beziehen und bei deren Offenlegung die Gefahr einer Persönlichkeitsverletzung besteht. Im schulischen Bereich sind das z.B.: - Zeugnisse, Notenlisten und andere Leistungsbeurteilungen - Notizen zu Leistungen und Verhalten der SuS, Disziplinarmassnahmen etc. - Zuteilung Religionsunterricht - Ärztliche Untersuchungen, Notizen zu Allergien, Medikamente etc. - Sensible Foto-, Video- oder Audiodateien von bestimmbaren Personen - Sensible Texte (z.B. persönliche Ansichten zu Religion oder Politik) mit Namensbezug - Sensible Informationen über die Eltern und Elternkorrespondenz - Personaldossiers (Lebensläufe, Bewerbungsschreiben, Lehrerbeurteilung etc.)
Personendaten 	Informationen, die sich auf eine bestimmte oder eine bestimmbare Person beziehen. Im schulischen Kontext sind dies z.B.: - Schülerarbeiten mit Namensbezug (d.h. auf einem Dokument steht der Vorname oder Nachname des Autors), sofern keine Informationen über Krankheiten, familiäre Situation etc. des Autors oder einer anderen bestimmbaren Person vorkommen - Foto -, Video- oder Audiodateien von bestimmbaren Personen - Klassenliste, Gruppeneinteilung - Nicht sensible Texte mit Namensbezug (d.h. im Text steht der Vorname oder Nachname des Autors oder einer anderen Person)
Sachdaten 	Informationen, die sich nicht auf bestimmte oder bestimmbare Personen beziehen. Im schulischen Umfeld sind dies z.B.: - Arbeits- und Übungsblätter ohne Namensbezug (d.h. auf einem Dokument steht nirgends ein Vorname oder Nachname) - Foto-, Video- oder Audiodateien (sofern keine Person bestimmbar ist) - Nicht sensible und sensible Texte (z.B. persönliche Ansichten zu Religion oder Politik) ohne Namensbezug (d.h. im Text steht nirgends der Vorname oder Nachname des Autors oder einer anderen Person)

3. Speichermedien für Daten im schulischen Bereich

Die Wahl des geeigneten Speichermediums hängt von der Sensibilität der zu speichernden Daten (Datenkategorie) ab.

Mobile Speichermedien (USB-Sticks, mobile Festplatten-Speicher [HD, SSD], CD, DVD) sollen grundsätzlich nicht verwendet werden, in begründeten Ausnahmefällen aber mit elektronischer Verschlüsselung und jederzeitigem Schutz vor Verlust oder Entwendung.

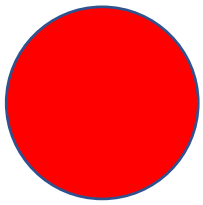
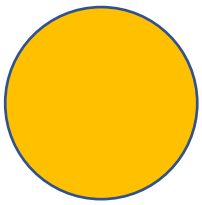
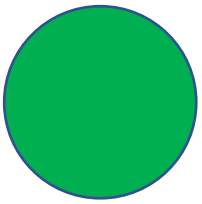
Tabelle 2: Zulässige Speichermedien

Datenkategorien	**Speichermedien**
Besonders schützenswerte Personendaten 	☑ interne Dateiablage - z.B. lokal (verschlüsselte lokale Festplatte) ☑ clientseitige verschlüsselte Daten in Public-Clouds - z.B. Tresorit.com, lokal verschlüsselte Dateien (Passwortschutz) in Microsoft 365, falls nicht in LehrerOffice gespeichert werden kann ☑ passwortgeschützte Schuladministrationssoftware mit Gerichtsstand CH und Serverstandort (wenn immer möglich) CH, ansonsten EU - z.B. Scolaris, LehrerOffice
Personendaten 	☑ Passwortgeschützte Cloud mit Gerichtsstand CH und Serverstandort (wenn immer möglich) CH, ansonsten EU - z.B. Microsoft 365 (Share Point, OneDrive) ☑ Passwortgeschützte Lernplattform mit Gerichtsstand CH und Serverstandort (wenn immer möglich) CH, ansonsten EU - z.B. Schabi, LearningView, Padlet, etc.
Sachdaten 	☑ Öffentliche Medien und Plattformen - z.B. Schulwebsite, öffentliche Padlets, etc.

4. Digitale Kommunikationstools für Daten im schulischen Bereich

Auch die Wahl des geeigneten Kommunikationstools ist abhängig vom Inhalt der Nachricht und somit von der Art der Daten (Datenkategorie), die übermittelt werden.

Tabelle 3: Zulässige Kommunikationstools

Datenkategorien	**Kommunikationstools**
Besonders schützenswerte Personendaten 	☑ E-Mail-Nachrichten über den Mail-Server der Schule innerhalb des Schulnetzes (Mailadresse des Empfängers hat gleichlautende Endung nach dem @-Zeichen) ☑ E-Mail-Nachrichten über den Mail-Server der Schule an externe Mailadressen -> müssen verschlüsselt werden (z.B. mit PrivaSphere) ☑ Digitale Plattform mit persönlichem Login - z.B. einzeln verschlüsselte Datei via Microsoft 365 (Teams) ☑ Datenschutzkonforme Messenger-Dienste mit passwortgeschütztem Chat - z.B. privater Chat in Threema
Personendaten 	☑ Datenschutzkonforme Messenger-Dienste - z.B. Threema, Wire ☑ Digitale Plattformen mit Gruppen-Login - z.B. Microsoft Teams
Sachdaten 	☑ E-Mail-Nachrichten ☑ Digitale Plattformen (öffentlicher Bereich) - z.B. Edupad, Kommentarfunktionen auf Lernplattformen

5. Umsetzungshilfen

5.1 E-Mailadressen für Schülerinnen und Schüler

Bei der Vergabe von E-Mail-Adressen empfiehlt das Erziehungsdepartement abgekürzte Namen oder Pseudonyme zu verwenden. Dadurch wird der Missbrauch der Konten durch Dritte erschwert. Grundsätzlich ist es aber auch zulässig, Schülerinnen und Schüler eine mit ihrem Namen verbundene schulische E-Mail-Adresse zu vergeben. Die gesetzliche Vertretung muss in diesem Fall schriftlich und nach umfassender Information über die entsprechende Nutzung in der Schule zustimmen. Bestehen Bedenken, ist auf den Namen zu verzichten und eine Abkürzung oder ein Pseudonym zu verwenden. Die verantwortliche Lehrperson thematisiert mit den Schülerinnen und Schülern den Gebrauch und die Risiken der Logins im Unterricht.

5.2 Interne und externe E-Mail-Kommunikation

E-Mail-Nachrichten innerhalb des Schulnetzes sind in der Regel sicher. Eine E-Mail-Adresse aus derselben Schul-Domain erkennt man an der gleichlautenden Endung nach dem @-Zeichen. Beim Austausch von Informationen über diese E-Mail-Adressen bleiben alle Informationen auf dem gleichen E-Mail-Server. Die Kommunikation verläuft somit in einem in sich geschlossenen Netz, weshalb diese Art von Kommunikation auch für besonders schützenswerte Personendaten empfohlen werden kann.

Die Kommunikation mit E-Mail-Nachrichten an Empfänger mit einer E-Mail-Adresse mit einer anderen Endung (z.B. private E-Mail-Adresse von Eltern oder Lehrpersonen) gilt als unsicher. Enthalten solche Nachrichten Personendaten oder besonders schützenswerte Personendaten müssen diese verschlüsselt werden.

5.3 Messenger-Dienste

Wird über Messengers kommuniziert, sind vor allem die Verschlüsselung, der Serverstandort und die Möglichkeit der anonymen Nutzung datenschutzrelevant. Es sind Anbieter zu berücksichtigen, die europäische Standorte und eine Transport-Verschlüsselung anbieten (z.B. Threema, Wire).

Auf der Website von educa findet sich eine Übersicht der verschiedenen Standard-Messengers und ihren Eigenschaften:

Link: ("Vergleich von Messenger-Diensten durch educa")

Es gilt zu beachten, dass sich der Markt der angebotenen Messenger-Dienste dynamisch weiterentwickelt und folglich einem steten Wandel unterliegt. Es ist somit möglich, dass ein bisher empfohlener Dienst infolge Änderungen auf einmal nicht mehr datenschutzkonform eingesetzt werden kann. Beim Einsatz von Messenger-Diensten ist deshalb regelmässig zu überprüfen, ob die ursprünglich datenschutzfreundlichen Vorgaben auch zu einem späteren Zeitpunkt noch gegeben sind.

5.4 Digitale Plattformen

Die Kommunikation über digitale Plattformen (Portale, Schulverwaltungssoftware), die den datenschutzrechtlichen Anforderungen genügen und über einen geschlossenen Bereich verfügen, für den durch die Schule eine personalisierte Zugangsberechtigung vergeben wird, kann aus Datenschutzperspektive auch für besonders schützenswerte Personendaten empfohlen werden.

5.5 Einsatz von Software mit Alterslimite

Diverse Programme, Apps und Webdienste sehen aufgrund der Datenschutz-Grundverordnung der EU (DSGVO) ein Mindestalter vor. Diese vertraglichen Vorgaben sind zu beachten.

SEA - **01.09.2021**