Kantonsschule Enge

IT-Nutzerrichtlinien

Stand: Dezember 2024

Die Schulleitung beschliesst:

1 Allgemeine Bestimmungen

1.1 Zweck

An dieser Schule werden in verschiedenen Bereichen vom Kanton Zürich bereitgestellten IKT-Systeme oder private Geräte (BYOD – Bring Your Own Device) im Unterricht und zur Arbeit eingesetzt.

Diese Richtlinie bezweckt, den Benutzenden verständliche und nachvollziehbare Vorgaben zum korrekten Umgang mit kantonalen IKT-Systemen zu geben. Diese Vorgaben regeln die Datensicherheit, den Datenschutz und den Umgang mit urheberrechtlich geschützten Werken im schulischen Kontext. Die Schulen prüfen nach eigenem Ermessen, ob die Sicherheitsmassnahmen des MBA für die von ihnen zu verantwortenden Daten ausreichen. Sie können zusätzliche technische Massnahmen prüfen oder bestellen, sowie organisatorische Massnahmen umsetzen.

1.2 Grundlagen

Diese Richtlinie entspricht den gesetzlichen und kantonalen Vorgaben und Rahmenbedingungen (vgl. Anhang I – Rechtliche Grundlagen).

Die Schule ist eine öffentlich-rechtliche Anstalt. Aus diesem Grund untersteht sie dem Gesetz über die Information- und den Datenschutz IDG sowie den weiteren kantonalen Rechtserlassen.

Als unselbständige Anstalt ist sie ausserdem an die Allgemeine Informationssicherheitsrichtlinie vom 3. September 2019 und die ergänzenden Besonderen Informationssicherheitsrichtlinien des Kantons gebunden.

1.3 Geltungsbereich

Diese Nutzungsrichtlinie gilt für Mitarbeitende, Lehrpersonen sowie Schüler*innen (nachfolgend genannt «Benutzende»), die Zugang zu IKT-Systemen der Kantonsschule Enge (nachfolgend genannt «Schule») haben («Benutzende»). Die Benutzenden sind persönlich dafür verantwortlich, diese Richtlinie einzuhalten.

Mit dem ersten Login oder der Nutzung der zur Verfügung gestellten IT-Infrastruktur nehmen die Benutzenden die Nutzungsrichtlinie zur Kenntnis und bestätigen, über die Konsequenzen bei deren Nichtbeachtung informiert worden zu sein.

1.4 Begriffe

Die in dieser Nutzungsrichtlinie verwendeten Begriffe orientieren sich an den vom Kanton verwendeten Fachbegriffen. Die Begriffsdefinitionen befinden sich im Glossar im Anhang.

1.5 Verwendungszweck

Die IKT-Systeme und Anwendungen sind auf schulische oder institutionelle Zwecke ausgerichtet. Der sorgsame und verantwortungsvolle Umgang mit allen IKT-Systemen garantiert einen störungsfreien Betrieb und dient allen Benutzenden.

Die Verwendung von IKT-Systemen und Anwendungen zu privaten Zwecken ist erlaubt, soweit sie sich auf ein verträgliches Mass beschränkt und den Lizenzbedingungen entspricht.

Die Verwendung von IKT-Systemen und Anwendungen für ressourcenintensive private Tätigkeiten ist (wie beispielsweise Mining) ist verboten.

Verschiedene Lizenzen (z.B. Microsoft 365) sind für private Nutzung zugelassen, deren kommerzielle Nutzung ist verboten.

1.6 Auswertungen von Randdaten

Bei der Nutzung der IKT-Systeme fallen Randdaten an, die in Logfiles unterschiedlicher Komponenten (Firewall, Server, Anwendung etc.) gespeichert werden. Zur Erkennung und Rückverfolgung von Sicherheitsvorfällen können die Schule und der Kanton Zürich innert der gesetzlichen Frist auf diese Logfiles zurückgreifen. Anonymisierte Standardauswertungen zur Gewährleistung der Sicherheit und Verfügbarkeit werden regelmässig durchgeführt. Sollen personenbezogene oder besondere Auswertungen erstellt werden, werden die betroffenen Nutzer/innen über einen Zugriff auf die Logfiles informiert.

2 Nutzung von IT-Arbeitsmitteln

An der Schule werden IT-Arbeitsmittel verwendet, die von der Schule bereitgestellt werden. Darüber hinaus werden BYOD-Geräte gemäss Ziff. 4.1 und 4.2 zur Nutzung an der Schule zugelassen. Andere IT-Arbeitsmittel, welche diesen Kriterien nicht entsprechen, sind zur Nutzung an der Schule nicht zugelassen.

Die nachfolgenden Regelungen in Ziff. 2.1 bis 2.5 betreffen IT-Arbeitsmittel, die den Benutzenden von der Schule zur Verfügung gestellt werden (d.h. nicht BYOD-Geräte).

Die Benutzenden behandeln die IT-Arbeitsmittel mit Sorgfalt und schützten sie vor Diebstahl und Beschädigung. Räume, die IT-Arbeitsmittel enthalten, sind beim Verlassen, wenn es der Schulalltag erlaubt, abzuschliessen.

2.1 Supportorganisation

Für den Support sind der schulinterne Vor-Ort-Support und der Service Desk des Digitalen Service Center SekII zuständig. Der schulinterne Vor-Ort-Support dient als erste Anlaufstelle.

2.2 Änderungen

An den bereitgestellten IT-Arbeitsmitteln dürfen keine unautorisierten Änderungen an den Grundeinstellungen vorgenommen werden. Solche Änderungen führt ausschliesslich die zuständige Supportorganisation durch.

2.3 Anwendungen

Auf den bereitgestellten Geräten dürfen lediglich die von der Schule bzw. vom Kanton freigegebenen Anwendungen installiert werden.

Ausnahmsweise können von der Schulleitung Fremdanwendungen bewilligt werden. Für Fremdanwendungen besteht kein Supportanspruch. Für Schäden, die durch Nutzung von Fremdanwendungen entstehen, ist der Benutzer verantwortlich und haftbar.

2.4 Weitere Hilfestellungen

Für gewisse IT-Arbeitsmittel existieren separate Nutzungsvorgaben und Anleitungen. Hilfestellungen der Schule oder des Kantons unterstützen die Benutzenden beim Setup und der Nutzung der IT-Arbeitsmittel im Schulalltag. Die Hilfestellungen sind in der schulinternen SharePoint Umgebung auffindbar.

2.5 Entsorgung

Die Entsorgung ausgedienter bzw. defekter IT-Arbeitsmittel oder deren Reparatur bzw. Austausch erfolgt in Abstimmung mit der Supportorganisation.

3 Datensicherheit

3.1 Schutz von Zugangsdaten

Sämtliche Zugangsdaten für die IKT-Systeme sind geheim zu halten. Gehen Zugangsdaten verloren oder besteht ein Verdacht auf Missbrauch, muss der/die betroffene(n) Benutzer/-in umgehend eine Meldung bei der zuständigen Supportorganisation vornehmen.

a. Benutzerkonto

Erhält der Benutzende ein Benutzerkonto, dient dieses insbesondere für:

- Den Zugriff auf und die Lizenzierung von Microsoft 365 auf privaten und von der Schule gestellten Geräten. Dies umfasst auch den Zugriff auf die schulische sowie private Dateiablage in der MS 365-Umgebung.
- Für die Anmeldung im schulischen Intranet zur Erfassung und Verwaltung von Absenzen, Kursanmeldungen, Noteneingabe, Notenverwaltung sowie Personendaten von Schüler*innen

Der Zugang zur Nutzung der IKT-Systeme erfolgt über einen Benutzernamen und ein Passwort.

Das Benutzerkonto ist persönlich und nicht übertragbar. Es darf keiner anderen Person Zugang zum eigenen Benutzerkonto verschafft werden. Die Benutzenden tragen für alle mit ihrem Benutzerkonto ausgeführten Aktivitäten die volle Verantwortung. Beim Verdacht auf Missbrauch kann das Benutzerkonto ohne Vorwarnung durch die Schule bzw. den Kanton gesperrt werden.

Die Benutzenden melden sich von allen Systemen ordnungsgemäss ab, wenn sie ihre Arbeitsstation definitiv verlassen.

b. Passwortschutz

Die Benutzenden sind verpflichtet, für sämtliche Zugänge ein starkes Passwort zu wählen Glossareintrag: «starkes Passwort»).

Für jeden Zugang ist ein separates, einzigartiges Passwort zu wählen. Das Passwort ist regelmässig zu ändern.

Die für die an der Schule verwendeten Passwörter dürfen nicht für private Zugänge verwendet werden.

3.2 Schutz von Informationen

Mitarbeitende und Lehrpersonen unterstehen im Rahmen des öffentlichen Leistungsauftrags dem Amtsgeheimnis.

Die Benutzenden haben Vorsichtsmassnahmen zu ergreifen, damit Informationen, die den Schulbetrieb, den Unterricht betreffen (nachfolgend «schulinterne Informationen»), nicht unbeabsichtigt offengelegt, entwendet oder gelöscht bzw. unkenntlich gemacht werden.

c. Datensicherung

Sämtliche schulinternen, administrativen Informationen (d.h. nicht Unterrichtsmaterialien) müssen auf der von der Schule bzw. dem Kanton bereitgestellten Datenablage (bspw. schuleigener Server oder Clouddienst) gespeichert werden, damit eine zentrale Datensicherung und Verfügbarkeit gewährleistet sind. Dies gilt auch für Informationen, die zusätzlich auf einem Wechselmedium gespeichert werden. Lokal gespeicherte Informationen sind nicht von der Datensicherung erfasst.

Wechselmedien, die klassifizierte Informationen enthalten, müssen gesichert aufbewahrt werden, um den Datenverlust zu vermeiden.

d. Berechtigungen

Die Schule verfügt über ein Rollen- und Berechtigungskonzept (Anhang IV), das für die Benutzenden verbindlich ist.

Es dürfen nur jene Daten geöffnet bzw. verwendet werden, welche der für die jeweiligen Benutzergruppe entsprechenden Klassifikationsstufe angehören.

Erhält ein/e Benutzer/-in Zugriff auf schulinterne Informationen, die nicht für sie/ihn bestimmt sind, muss sie/er dies dem Datenersteller umgehend mitteilen.

e. Schutzstufen

Sämtliche Informationen sind gemäss nachfolgender Kriterien in Datenkategorie, Informations-Klassifizierung und Schutzstufe kategorisiert.

In der Datenkategorie kommt zum Ausdruck, ob es sich um Sach- oder Personendaten handelt.

Die Informations-Klassifizierung zeigt, für wen die Daten bestimmt sind bzw. wie sie zu behandeln sind. Informationen, die auch Personendaten enthalten, sind in jedem Fall zumindest als «intern», besondere Personendaten zumindest als «vertraulich» zu klassifizieren.

Mit der Schutzstufe kommt zum Ausdruck, welche technischen und organisatorischen Massnahmen zum Schutz der Informationen vor Einsichtnahme und Veränderung vorgesehen werden, um die Daten ihrer Kategorisierung und Klassifizierung entsprechend zu schützen.

Die Schule hat in diesem Zusammenhang die vom Kanton vorgesehene Einstufung übernommen und konkretisiert. Verantwortlich für die korrekte Einstufung von Dokumenten (Kategorisierung und Klassifizierung) sowie die Einhaltung der entsprechenden Schutzstufen ist die erstellende bzw. versendende Person eines Dokuments.

Die Einstufung lautet folgendermassen:

Datenkategorien		
Sachdaten	Personendaten	Besondere Personendaten

Informations-Klassifizierung			
1	2	3	4
Öffentlich	Intern	Vertraulich	Geheim

Schutzstufen			
1	2	3	4
Grundschutz	Erhöhter Schutz		
Grundschutz	Interner Schutz	Vertraulicher Schutz	Höchster Schutz

Für Mitarbeitende und Lehrpersonen sind die folgenden Beispiele relevant:

Datenkategorien		
1	2	3
Sachdaten	Personendaten	Besondere Personendaten
Bspw. Lehrmittel, Prüfungen (soweit noch nicht ausgefüllt), Unterrichtsfolien etc.	Bspw. Name, Adresse, Telefon, Geburtsdatum, IP-Adresse, Gerätekennungen, Benutzernamen, einzelne Noten etc.	Bspw. Zeugnisse bzw. Notenzusammenstellungen, Lernprofile, Disziplinarmassnahmen, Angaben über die Gesundheit wie auch Quarantänemassnahmen, Religionszugehörigkeit etc.

Informations-Klassifizierung			
1	2	3	4
Öffentlich	Intern	Vertraulich	Geheim
öffentliche oder allgemeine schulische Informationen ohne personenbezogene Daten oder sensible Inhalte.	Interne Informationen, die für alle oder grössere Gruppen von Mitarbeitenden und/oder Schüler*innen zugänglich sein dürfen, aber nicht für externe Personen.	Personenbezogene und sensible Daten, die vor allem Schulleitung, Sekretariat und Lehrpersonen mit bestimmten Funktionen benötigen.	Für hochsensible Informationen, die einen erhöhten Schutz erfordern. Zugriffe sind nur für ausgewählte Personen möglich (Schulleitung, Verwaltung und gegebenenfalls einige Lehrpersonen mit besonderen Aufgaben).
Bspw. Broschüren, Webseite, Plakate und weitere, veröffentlichte Informationen	Bspw. Intranet, Lehrmittel, Prüfungsvorlagen, Unterrichtsfolien, Anleitungen, Adresslisten, Fotos (soweit nicht zur Veröffentlichung vorgesehen) etc.	Zeugnisse, einzelne Noten, Lernprofile, Disziplinarmassnahmen, Angaben über die Gesundheit wie auch Quarantänemassnahme, Religionszugehörigkeit etc.	Hochsensible Informationen über Schulangehörige, wie bspw. strafrechtliche Sanktionen, ärztliche Gutachten, Korrespondenz zum Nachteilsausgleich (Diagnosen), Maturitätsprüfungen

In offiziellen Austauschkanälen und Kollaborationsplattformen innerhalb der Schule (d.h. ohne Beteiligung schulexterner Personen) können Dokumente aller Schutzstufen bearbeitet werden. Für vertrauliche und geheime Informationen müssen gemäss Informations-Klassifizierung angemessene Zugriffsrechte bestehen, d.h. diese Kanäle, Seiten dürfen nur einem stark eingeschränkten Benutzerkreis zugänglich sein. Konkret ergeben sich folgende Handlungsmassnahmen für die 4 Schutzstufen:

Schutzstufe 1: Grundschutz

- Für den Zugang zu Informationen im Grundschutz sind keine speziellen Authentifizierungsmassnahmen erforderlich.
- Die Speicherung kann in freigegebenen Ordnern erfolgen, die allen Schulangehörigen zugänglich sind (z. B. allgemeine Informationen auf SharePoint).

- Eine Protokollierung von Zugriffen auf Daten dieser Schutzstufe ist nicht vorgesehen.

Schutzstufe 2: Interner Schutz

- Daten, die dem internen Schutz unterliegen, werden in vor externen Zugriff geschützten Bereichen der Microsoft 365-Umgebung gespeichert.
- Die Weitergabe solcher Daten erfolgt ausschliesslich innerhalb des schulischen Umfelds und ist auf Schüler*innen und Mitarbeitende beschränkt. Eine externe Weitergabe ist nur mit Genehmigung der Schulleitung gestattet.
- Zugriffe und Änderungen werden protokolliert, um eine spätere Nachverfolgung zu ermöglichen. Ungewöhnliche Aktivitäten (wie unberechtigte Zugriffsversuche) werden durch die IT-Abteilung überprüft.

Schutzstufe 3: Vertraulicher Schutz

- Vertrauliche Daten werden ausschliesslich in vor externem Zugriff geschützten Bereichen des Intranets oder der Microsoft 365-Umgebung gespeichert. Dabei sind die Zugriffsrechte auf die Personen eingeschränkt, die die Informationen betreffen.
- Die Weitergabe vertraulicher Daten ist auf Personen beschränkt, die direkt mit den Inhalten arbeiten. Eine externe Weitergabe erfolgt nur in Ausnahmefällen und bedarf der ausdrücklichen Genehmigung der Schulleitung.
- Beim Umgang mit vertraulichen Daten sollten öffentliche, unverschlüsselte WLAN-Netze gemieden werden.
- Alle Zugriffe auf vertrauliche Daten werden protokolliert und bei Auffälligkeiten überprüft.

Schutzstufe 4: Höchster Schutz

- Daten der höchsten Schutzstufe werden ausschliesslich in speziell geschützten Bereichen innerhalb der offiziellen schulischen und kantonalen IT-Umgebungen verarbeitet und gespeichert. Innerhalb der Microsoft 365-Umgebung können dies z.B. eingeschränkte SharePoint-Ordnern mit erweiterten Zugriffsrechten sein.
- Eine Weitergabe solcher Daten ist streng limitiert auf berechtigte Personen innerhalb der Schule und erfolgt nur über gesicherte Kanäle innerhalb der Microsoft 365-Umgebung. Externe Weitergaben sind grundsätzlich nicht zulässig.
- Beim Mailversand an schulische Verteiler ist der Name der betroffenen Person zu codieren. Anhänge mit sensiblen Daten sollen nicht versendet werden. Stattdessen soll ein Zugriffslink mit personalisierten Zugriffsrechten versendet werden. Zudem wird empfohlen die Verschlüsselungsfunktion in Microsoft Outlook zu nutzen, um das Weiterleiten, Drucken und Kopieren der Nachricht zu verhindern.
- Bei der Verarbeitung von Daten der höchsten Schutzstufe ist auf geschützte Umgebungen und auf Massnahmen gegen unbefugte Einsichtnahme zu achten. Öffentliche Netzwerke sollten nur unter Verwendung eines verschlüsselten VPNs genutzt werden.
- Die Speicherung solcher Daten auf privaten Geräten ist grundsätzlich untersagt. Falls eine Ausnahme notwendig ist, sind die Daten sowohl verschlüsselt als auch passwortgeschützt aufzubewahren.
- Alle Zugriffe auf Daten der höchsten Schutzstufe werden umfassend protokolliert und regelmässig auf unbefugte Aktivitäten überprüft. Im Falle eines Zugriffsversuchs durch unberechtigte Personen wird die Schulleitung informiert.

f. Bekanntgabe von Informationen

Schulinterne Informationen dürfen nur gestützt auf eine Rechtsgrundlage, oder wenn die betroffene Person im Einzelfall eingewilligt hat, weitergegeben werden. In Zweifelsfällen entscheidet die Schulleitung.

g. Sorgfaltspflichten

Es herrscht eine strikte Clean Desk und Clear Screen Policy

Die Benutzenden lassen keine physischen Träger von Informationen (d.h. Wechselmedien, USB-Sticks, etc.) unbeaufsichtigt liegen.

Störungen oder Defekte an bereitgestellte IT-Arbeitsmitteln sind umgehend dem schulinternen Vor-Ort-Support zu melden.

Zutritt zu nicht öffentlich zugänglichen Räumen darf nur autorisierten bzw. angemeldeten Personen gewährt werden. Auffällige Personen müssen umgehend gemeldet werden (vgl. Kap 3.7).

3.3 Schutz vor Malware

Alle IT-Arbeitsmittel, welche im Schul- und Verwaltungsumfeld benutzt werden, sind mit Schutzsoftware ausgestattet. Die Benutzenden sind gehalten, die ergänzenden Schutzvorschriften zu berücksichtigen:

1. Schutzsoftware darf nicht umgangen oder deaktiviert werden;
2. Es müssen immer sämtliche offiziellen Aktualisierungen und Updates installiert werden, insbesondere die des Virenschutzes;
3. Persönliche Geräte müssen, soweit sie an der Schule zugelassen sind, auf Malware gescannt werden, wenn sie zuvor an einem anderen Netzwerk angeschlossen waren oder Dritte mit dem Gerät gearbeitet haben;
4. Verdächtige E-Mails müssen umgehend gelöscht und als Spam gemeldet werden, bei einer Häufung solcher Fälle hat eine Meldung bei der zuständigen Supportorganisation zu erfolgen;
5. Es dürfen keine Anhänge, die von unbekannten oder verdächtigen Absendern stammen, geöffnet werden;
6. Generell dürfen Werbungen oder Pop-Ups in Nachrichten oder im Internet nicht an-geklickt werden, bei externen Links ist Zurückhaltung geboten;
7. Es dürfen keine fremden, nicht autorisierten bzw. bewilligten Wechselmedien an die IT-Infrastruktur der Schule angeschlossen werden;
8. Auffälligkeiten und konkrete Verdachte müssen umgehend gemeldet werden (vgl. Kapitel 3.7).

3.4 Schutz von Kommunikation

a. E-Mail

Die Benutzenden erhalten ein eigenes E-Mail-Konto mit einer E-Mailadresse der Schule. Das E-Mail-Konto dient für:

- Die Korrespondenz im Zusammenhang mit dem Schulbetrieb;
- Empfang von allgemeinen Informationen und Weisungen der Schule bzw. des Kantons;
- Organisation des Klassenbetriebs etc.

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

1. Die Benutzenden sind für die Kontrolle und Pflege ihres Postfachs verantwortlich. Auf E-Mails ist an Werktagen innerhalb von 48 Stunden zu reagieren.
2. Vertraulich und höher klassifizierte Nachrichten müssen verschlüsselt und signiert versendet werden.
3. E-Mails dürfen nicht an externe (private oder geschäftliche) Postfächer weiter- oder umgeleitet werden.
4. Das E-Mail-Konto darf nicht zum Versand oder zur Verbreitung von beleidigenden, persönlichkeitsverletzenden, rassistischen, sexistischen oder pornographischen Inhalten

oder zur Planung, Vorbereitung, Organisation und Durchführung von Verbrechen und Vergehen benutzt werden.

5. Die E-Mailadresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshopping etc.) genutzt werden.

b. Collaboration Tools

Im Zusammenhang mit der Nutzung von Anwendungen zur Zusammenarbeit wie Microsoft Teams (sog. Collaboration Tools) gelten folgende Vorgaben:

1. Die Benutzenden verwenden Collaboration Tools für die schulinterne Kommunikation;
2. Die Anzahl neuer Kanäle ist auf das Nötige zu limitieren;
3. Der / Die Betreibende eines Kanals ist für die spezifischen Berechtigungen verantwortlich und sorgt dafür, dass der Informationsaustausch auf das Notwendige beschränkt und die Netiquette auch im Chat eingehalten wird;
4. Vertrauliche oder höher klassifizierte Informationen sind – sobald sie den schulischen Tenant verlassen - End-zu-End verschlüsselt auszutauschen, egal ob im Chat, Kanal oder im Videoanruf. Chats und Social-Media-Kanäle sind dazu bestimmt, sich auszutauschen. Vertrauliche und höher klassifizierte Daten und Dokumente sollten nicht dort, sondern in dafür bestimmte Speicher abgelegt und in den Chats und Social Media nur referenziert / verlinkt werden.

3.5 Netzwerk- und Internetnutzung

Das Schulnetzwerk steht den Benutzenden via einen persönlichen Zugang zur Verfügung. Benutzende, die keinen persönlichen Zugang erhalten, steht das Gästenetzwerk zur Verfügung.

Im Zusammenhang mit der Nutzung des Schulnetzwerks gelten folgende Vorgaben:

1. Up- und Downloads von umfangreichen, nicht unterrichts- oder schulbezogenen Dateien sind zu verhindern, insbesondere die Installationen von Spielen und grossen Audio- und Videodateien aus dem Internet sind verboten. Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden;
2. Der Besuch des Darknets ist verboten;
3. Der Besuch von Webseiten mit folgenden Inhalten ist verboten: pornografische, sexistische, rassistische oder gewaltverherrlichende Äusserungen bzw. Darstellungen; Glücks- und Geldspiele; Pyramiden- und Schneeballsysteme; Terrorismusförderung und -Finanzierung, sonstige, rechtswidrige oder gegen die guten Sitten verstossende Inhalte;
4. Während des Unterrichts ist der Besuch von Social Media und sonstige Unterhaltungsseiten verboten, ausser dies gehört zum Unterrichtsstoff;
5. Schulinterne, administrative Informationen dürfen nur in Absprache mit der Schulleitung ins Internet hochgeladen werden, z.B., um Übersetzungen in Gratistools zu erwirken;
6. Die Netiquette gemäss Anhang III ist einzuhalten.

Sämtliche Webseitenzugriffe werden automatisch protokolliert. Die Protokolldaten können von der Schule bzw. vom Kanton im begründeten Verdachtsfall personenbezogen ausgewertet werden. Die Nutzer/innen werden im konkreten Fall informiert, sofern eine Rückverfolgbarkeit möglich ist.

3.6 Arbeiten von unterwegs oder zu Hause

Der Fernzugriff auf das schulinterne Netz erfolgt ausschliesslich über eine gesicherte Verbindung (VPN, Citrix). Die Clean Desk und Clear Screen Policy gilt auch im Homeoffice.

Beim Arbeiten von unterwegs muss der Bildschirm vor den Blicken Dritter geschützt sein (Sitzplatz entsprechend wählen, Sichtschutzfolie). Gespräche über schulinterne Angelegenheiten, Unterrichtsinhalte und sämtliche Informationen, die dem Amtsgeheimnis unterliegen, werden vermieden.

3.7 Meldepflicht

Sicherheitsvorfälle, der Verlust bzw. Defekt von IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem schulinternen IT-Support zu melden.

4 Persönliche Geräte / BYOD

4.1 Grundsatz

Der Einsatz von persönlichen mobilen Geräten an der Schule ist grundsätzlich erlaubt. Persönliche mobile Geräte sind mobile Arbeitsgeräte wie Laptops/Notebooks. Für mehr Sicherheit der mobilen Arbeitsgeräte gelangen zusätzliche unterstützende Geräte (z.B. Smartphone für die Authentifizierung) zum Einsatz.

Eine Verbindung mit dem Schulnetzwerk ist zulässig.

Die Nutzung im Unterricht erfolgt in Absprache mit der Lehrperson und der zuständigen Supportorganisation. Die Schule behält sich vor, die Nutzung im Unterricht nur zuzulassen, wenn die Geräte den kantonalen oder schulischen Vorgaben entsprechen.

4.2 Geräteanforderungen

Es gelten folgende Mindestanforderungen:

- Passwort- oder PIN-Schutz
- regelmässige Updates (Firewall, Betriebssystem, Virenschutz und Applikationen)
- Verschlüsselung sensitiver Daten bei der Speicherung und Übermittlung.

Die Schule ist berechtigt, vom Benutzenden einen Nachweis betreffend die Einhaltung der Mindestanforderungen einzuholen.

4.3 Synchronisation

E-Mails und Termine können synchronisiert werden, sofern das Gerät den kantonalen oder schulischen Vorgaben genügt.

Persönliche mobile Geräte können von der Schule inventarisiert werden.

Bei Verlust von persönlichen Geräten wird der Benutzer gesperrt. Wählen sich Dritte über dieses Gerät ins Internet ein, werden die letzten Änderungen (z.B. in SharePoint) übertragen.

4.4 Support

Persönliche Geräte können von der Schule eingeschränkt betreut werden, d.h. ein Vor-Ort-Support kann dafür genutzt werden. Anspruch auf weiteren Support besteht nicht. Für fachgerechte Entsorgung (u.a. korrekte Datenlöschung) und Reparatur von persönlichen Geräten sind die Benutzenden selbst zuständig.

4.5 Onlineprüfungen

Onlineprüfungen können gemäss den Weisungen der Schule durchgeführt werden.

5 Datenschutz

5.1 Generell

Die Benutzenden halten sich im schulischen Kontext an das geltende Datenschutzrecht.

Macht eine betroffene Person Rechte aus dem anwendbaren Datenschutzrecht geltend und stellt sie bspw. ein Auskunfts-, Berichtigungs- oder Löschgesuch, stellt der/die Benutzende das Gesuch an die/den Datenschutzverantwortliche*n der Schule zu.

Im Übrigen gilt die Datenschutzerklärung der Schule, die Bestandteil dieser Nutzungsrichtlinie bildet.

5.2 Im Unterricht

Lehrpersonen sind für den Schutz der Persönlichkeit der Lernenden während des Unterrichts verantwortlich, dazu gehört auch der Datenschutz. Die Lernenden sind betreffend datenschutzrechtliche Themen regelmässig zu sensibilisieren.

Lehrpersonen haben den Unterricht so zu gestalten, dass möglichst wenig Personendaten der Lernenden automatisiert bearbeitet werden (Prinzip der Datensparsamkeit und Datenminimierung).

a. Anwendungen

Anwendungen im Unterricht sind mit Blick auf die datenschutzrechtlichen Vorgaben (Speicherort, Aufbewahrungsdauer, Möglichkeit der endgültigen Löschung, technische Massnahmen wie Verschlüsselung etc.) zu prüfen. Die Verantwortung trägt die Schule. Im Zweifelsfall richtet sich die Lehrperson an den schulischen IT-Support bzw. die/den Datenschutzverantwortliche*n.

b. Nutzung von Social Media

Der Einsatz von Social Media im schulischen Kontext (bspw. das Erstellen einer Facebook-Klassengruppe, eines YouTube-Kanals etc.) ist nur mit vorgängiger Zustimmung der Schulleitung und unter Beachtung der Netiquette zulässig.

Ist der Einsatz von Social Media bewilligt, sind die Kanäle, Gruppen, Benutzerzugänge etc. regelmässig zu kontrollieren und jene Inhalte zu löschen, die nicht mehr benötigt werden.

Spätestens, sobald die jeweilige Lehrperson die Klasse nicht mehr betreut, sind die Kanäle, Gruppen, Benutzerzugänge und Dokumente zu löschen.

d. Besondere Personendaten

Schriftliche Aufzeichnungen (Aufsätze, Gedichte etc.), grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen von Lernenden, die Angaben über besondere Personendaten enthalten, sind mindestens als vertraulich zu klassifizieren, es gilt mindestens die Schutzstufe 3. Sofern sie keiner Archivierungspflicht unterliegen, sind sie spätestens Ende der Ausbildung zu anonymisieren oder zu vernichten. Die Rekursfristen sind dabei einzuhalten.

e. Bilder

Schulangehörige dürfen nicht ohne ihre Zustimmung gefilmt, fotografiert oder sonst wie aufgenommen werden. Gruppenbilder sind so aufzunehmen, dass einzelne Personen nicht herausstechen. Klassenfotos sind stets freiwillig.

f. Bekanntgabe

Es dürfen keine schriftlichen Aufzeichnungen, grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen ohne die explizite Zustimmung der betroffenen Personen veröffentlicht oder Dritten bekanntgegeben werden. Ebenso dürfen ohne explizite Einwilligung keine Porträts von Lernenden, Lehrpersonen oder Mitarbeitenden auf der öffentlich zugänglichen Schulwebseite veröffentlicht werden.

Bei Lernenden unter 14 Jahren ist die Zustimmung der Eltern einzuholen.

6 Urheberrechte

6.1 Generell (MA/LP)

Die Benutzenden halten sich im schulischen Kontext an das Urheberrecht. Es sind folgende Vorgaben zu beachten:

1. Es dürfen Ausschnitte von urheberrechtlich geschützten Werken («Werke») zum Eigengebrauch der Schule, d.h. zur internen Information und Dokumentation, vervielfältigt werden, sei dies analog oder digital;
2. Erlaubt ist die Nutzung ganzer Radio- und TV-Sendungen auf passwortgeschützten, digitalen Plattformen über die abonnierten Digi- und Mediatheken. Diese Nutzung beinhaltet das Vervielfältigen ganzer Radio- und Fernsehsendungen sowie das unentgeltliche Zugänglichmachen für berechtigte Benutzer, einschliesslich das Abrufen samt Download einzelner Sendungen aus einem schulinternen Netzwerk;
3. Nicht erlaubt ist namentlich:
    a. Das Vervielfältigen von ganzen Werken bzw. deren Exemplare, die im Handel erhältlich sind;
    b. Das Veröffentlichen von Werken oder Werkausschnitten auf der öffentlichen Schulwebseite, sozialen Medien (inkl. geschlossener Gruppen), Videoportalen etc.;
    c. Das Bearbeiten oder Verändern von Werken;
4. Werden für Lehrpersonen, die ganze Schule oder Dritte Lehrmittel erstellt, dürfen diese keine Zusammenstellungen von fremden Werkausschnitten enthalten. Vor Erstellung eines Lehrmittels ist Rücksprache mit der Schulleitung zu nehmen.

6.2 Im Unterricht (LP/L/S)

a. Grundsatz

Im Unterricht dürfen urheberrechtlich geschützte Werke auf jegliche Art verwendet werden, das beinhaltet das Anfertigen von analogen oder digitalen Kopien (sog. Vervielfältigungen) von Werkausschnitten, nicht aber von ganzen Werkexemplaren, die im Handel erhältlich sind. Lehrpersonen dürfen Werke für einzelne Klassen auf dem Intranet oder in der MS 365-Umgebung zugänglich machen. Von der erlaubten Vervielfältigung nicht erfasst ist das Kopieren von Computerprogrammen sowie das Aufzeichnen von Vorträgen, Bühnenaufführungen und Konzerten.

b. Ton-, Tonbild- und andere Leerträger

Erlaubt ist das Kopieren von Ausschnitten aus Büchern, Filmen, Musikstücken (d.h. auch Musiknoten) und auch Werken der bildenden Kunst sowie das vollständige Aufzeichnen von Radio- und Fernsehsendungen (exkl. im Handel erhältlicher Filme) durch eine einzelne Lehrperson für ihre eigenen Unterrichtszwecke.

c. Bilder

Fotografien, Gemälde, Grafiken, Zeichnungen und andere Werke der bildenden Kunst dürfen als Ganzes im Unterricht verwendet werden.

d. Musikaufführungen

Das Aufführen von Werken der nicht-theatralischen Musik und geschützter Leistungen an klassen-übergreifenden Anlässen (bspw. Konzerte, Schülerdiscos etc.) ist erlaubt, sofern:

1. die Aufführung durch Schulangehörige erfolgt;
2. der Anlass sich ausschliesslich an die Schüler- und Lehrerschaft sowie deren Familienangehörige richtet; und
3. der Anlass unentgeltlich ist.

e. Neukreationen

Lernende dürfen Teile von Werken zur Herstellung eigener Kreationen, seien es Texte, Bilder, Darbietungen oder Theaterstücke verwenden. Die neuen Werke dürfen der Klasse präsentiert werden.

f. Erstellung von Lehrmitteln

Erlaubt ist nur das Vervielfältigen, durch die Schule oder durch Dritte, von Werksauszügen für interne Zwecke. Dazu gehört auch das interne Verbreiten der Vervielfältigungen und das interne Zugänglichmachen inkl. der Möglichkeit des Downloads. Kein systematisches Verbreiten und Zugänglichmachen ausserhalb des eigenen Unterrichts. Keine Nutzung durch externe Personen erlaubt.

g. Urheberrecht der Schule

Hinweis zu den folgenden drei Abschnitten: Da in diesem Bereich an manchen Schulen bereits interne Regelungen bestehen und das Postulat der Lehrmittelfreiheit hoch gehalten werden soll, sind folgende Formulierungen nicht für alle Schulen relevant.

Erstellen angestellte Lehrpersonen im Rahmen ihres Arbeitsverhältnisses Werke im Sinne des Urheberrechts (Programme, Dokumentationen, Lehrmittel, Skripte, Publikationen, Designs usw.), so werden die Urheberrechte ohne weitere Entschädigung auf die Schule übertragen.

Werke, welche Mitarbeitende im Rahmen ihres Arbeitsverhältnisses erstellt haben, dürfen nur in Absprache mit der Schulleitung kostenpflichtig an Lernende weitergegeben werden.

Werke, welche Mitarbeitende nicht im Rahmen ihres Arbeitsverhältnisses erstellt haben, dürfen nur in Absprache mit der Schulleitung kostenpflichtig an die Lernenden weitergegeben werden.

6.3 Ausserhalb des Unterrichts

Das Veröffentlichen von Werken oder Werkausschnitten auf der öffentlichen Schulwebseite, sozialen Medien (inkl. geschlossener Gruppen), Videoportalen etc. ist untersagt.

7 Massnahmen bei Verstössen

Bei einer missbräuchlichen Nutzung der IKT-Systeme, inkl. Urheberrechtsverletzungen, drohen den Benutzenden Massnahmen. Missbräuchlich ist die Nutzung dann, wenn sie gegen diese Nutzungsrichtlinie, weitergehende schulinterne Richtlinien und Weisungen oder die anwendbaren gesetzlichen Bestimmungen verstösst, oder wenn die Rechte Dritter verletzt werden. Zwecks Abklärung von Missbrauchsvorfällen können Randdaten und sonstige Log-Files bzw. Protokolle ausgewertet und im begründeten Verdachtsfall personenbezogen ausgewertet werden. Werden Missbräuche und Verstösse erkannt, sollte immer zuerst das Gespräch gesucht werden. Bevor die Schule entscheidet, ob sie Disziplinarmassnahmen ergreift, wird den Benutzenden die Möglichkeit zur Äusserung gegeben.

Die fehlbare Person haftet für den durch die missbräuchliche Nutzung entstandenen Schaden.

Die Schule kann unter anderem folgende Massnahmen ergreifen:

1. Zuerst erfolgt ein persönliches Gespräch mit der Möglichkeit der Parteien, ihre Beweggründe zu nennen.
2. In der Regel erfolgt dann eine Abmahnung bzw. Verwarnung, bevor weitere Massnahmen ergriffen werden;
3. Bei Lernenden erfolgt je nach Schwere des Verstosses eine Meldung an die Inhaber der elterlichen Sorge, weitere Erziehungsberechtigte und den Lehrbetrieb;
4. Dossiereintrag
5. Bei gravierenden oder wiederholten Verstössen kann die Schule direkt Disziplinarmassnahmen gemäss der anwendbaren Schulordnung bzw. dem anwendbaren Disziplinarreglement oder Personalrecht ergreifen.
6. Die Schule kann nebst Schadenersatz auch, sofern rechtlich zulässig, die Wiederherstellung des ursprünglichen Zustands verlangen.
7. Stellt die Schule strafbares Verhalten fest, kann sie ohne Vorwarnung eine Strafanzeige einreichen bzw. eine Meldung bei der zuständigen Behörde vornehmen.

8 Ende der Benutzerrolle

Die Rolle als Benutzerin oder Benutzer der IKT-Systeme kann aus verschiedenen Gründen enden: die Beendigung des Arbeitsverhältnisses, der Arbeitgeber- oder Schulwechsel, Aus-schluss oder ein erfolgreicher Abschluss der Schule. Die Beendigung von Nutzungsvereinbarungen wird nachfolgend summarisch als «Austritt» bezeichnet.

Ihr Benutzerkonto wird bei Austritt deaktiviert.

Vor Ende der Benutzerrolle wird in ausreichender Frist ein Erinnerungs-E-Mail an die jeweiligen Benutzenden versendet.

Persönliche Daten sind bis zum Deaktivierungstag auf eigene Speichermedien oder Cloudspeicher zu übertragen.

Spätestens am Tag des Austritts sind sämtliche IT-Arbeitsmittel an die zuständige Supportorganisation zurückzugeben bzw. Anwendungen und Zugänge von BYOD-Geräten zu löschen.

Die zuständige Supportorganisation unterstützt die Benutzenden bei Bedarf. Der Unterstützungsbedarf sollte spätestens einen Monat vor Ende der Benutzerrolle angemeldet werden.

9 Haftungsausschluss

Soweit die Rechtsordnung dies zulässt, schliesst die Schule jede Haftung für Schäden durch Benutzerhandlungen aus. Die Schule haftet ausserdem nicht für Schäden, die den Benutzenden aus ihrer Missachtung dieser Nutzungsrichtlinie und des anwendbaren Datenschutzrechts sowie der Missachtung der kantonalen AISR und anwendbaren BISR entstehen.

10 Anhang I – Rechtliche Grundlagen

Nebst dem Bundesgesetz über die Berufsbildung und den kantonalen Gesetzen und Verordnungen über die Mittel- und Berufsfachschulen stützt sich diese Nutzungsrichtlinie auf die folgenden kantonalen Rechtsgrundlagen, Weisungen und Merkblätter:

Gesetze

- Gesetz über die Information und den Datenschutz vom 12. Februar 2007 («IDG») Link
- Personalgesetz vom 27. September 1998 («PG») Link

Verordnungen

- Verordnung über die Information und den Datenschutz vom 28. Mai 2008 («IDV») Link
- Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 Link
- Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 («IVSV») Link
- Archivverordnung vom 9. Dezember 1998 Link
- Personalverordnung vom 16. Dezember 1998 («PVO») Link
- Vollzugsverordnung zum Personalgesetz vom 19. Mai 1999 («VVO») Link

Reglemente

- Disziplinarreglement Berufsbildung vom 5. März 2015 Link
- Disziplinarreglement Mittelschulen vom 2. Februar 2015 Link
- Schulordnung für die Kantonale Maturitätsschule für Erwachsene vom 4. Februar 1997 Link

Richtlinien

- Allgemeine Informationssicherheitsrichtlinie des Regierungsrates AISR für die kantonale Verwaltung vom 3. September 2019 Link
- Besondere Informationssicherheitsrichtlinien für die kantonale Verwaltung BISR vom 17. Juni 2020, Inkrafttreten am 17. Juni 2022 Link
- Richtlinien für die Informationsverwaltung an den kantonalen Mittel- und Berufsfachschulen sowie an den vom Kanton beauftragten Berufsfachschulen vom 4. April 2016 Link
- Richtlinien Informationsschutz des MBA; Link

Merkblätter

- Leitfaden Datenschutzlexikon Mittelschule und Berufsfachschule vom September 2020; Link
- Leitfaden Einsatz von mobilen Geräten in der Verwaltung vom August 2022; Link
- Leitfaden Bearbeiten im Auftrag vom April 2021; Link
- Social Media Guidelines 2014 des Kantons Zürich; Link
- Merkblatt Cloud Computing vom Juli 2022; Link
- Merkblatt Online-Speicherdienste vom November 2020; Link
- Merkblatt Passwortmanager vom Juli 2022; Link
- ProLitteris GT 8+9 2017-2022 Archiv Link
- ProLitteris Tarif 7 Gültigkeit 2022-2026; Link

Glossare

- Glossar und Abkürzungen Informationssicherheit vom Oktober 2020; Link
- Glossar zu den Besonderen Informationssicherheitsrichtlinien vom 13. Mai 2020

Suche nach Datenschutz-Dokumenten im Kanton Zürich: Link

11 Anhang II – Glossar

Amtsgeheimnis: Das Amtsgeheimnis untersagt das Offenbaren von schulischen Angelegenheiten, die im Rahmen der amtlichen oder dienstlichen Stellung wahrgenommen werden, es sei denn, es liegt ein gesetzlicher Rechtfertigungsgrund vor. Diese Schweigepflicht bleibt nach Beendigung des Arbeitsverhältnisses bestehen. Die Verletzung des Amtsgeheimnisses ist strafbar.

Anonymisierte Personendaten: Daten, die keinen Personenbezug mehr aufweisen und bei denen eine Re-Identifizierung nicht möglich ist. Bei der Schule vorhandene Personendaten dürfen für nicht personenbezogene Zwecke wie Statistiken bearbeitet werden, wenn sie anonymisiert werden.

Anwendungen: Als Anwendungssoftware (englisch «application software», kurz App) wer-den Computerprogramme bezeichnet, die genutzt werden, um eine nützliche oder gewünschte nicht system-technische Funktionalität zu bearbeiten oder zu unterstützen. z.B. Geschäftsanwendungen, Clouddienste, gem. IKT-Strategie Fachapplikationen, Kantonsapplikationen.

Ausschnitt eines Werkexemplars: Als Faustregel gilt, dass der zu vervielfältigende Aus-schnitt max. 75% des Werkexemplars abdecken sollte. Es kommt allerdings immer auf den Einzelfall an. Ist der Ausschnitt dermassen umfassend, dass der Kauf des Werkexemplars für die Benutzenden nicht mehr interessant ist, darf er nicht vervielfältigt werden. Bei Büchern wird davon abgeraten, mehrere zusammenhängende Kapitel zu vervielfältigen.

Bearbeiten: Jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten.

Bekanntgeben: Das Zugänglichmachen von Informationen wie das Einsicht gewähren, Weitergeben oder Veröffentlichen.

Benutzende: Mitarbeitende, Lehrpersonen, Lernende sowie Dritte (bspw. Kursbesuchende, Bibliotheksbenutzende, Mieter von Schulräumen etc.), welche die Informatik-Infrastruktur der Schule benutzen.

Besondere Personendaten: Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht. Beispiel: Gesundheitsdaten, Zeugnis.

BYOD: Bring-your-own-device bezeichnet persönliche mobile Geräte, die nicht von der Schule zur Verfügung gestellt, aber zur Nutzung an der Schule zugelassen sind.

Clean Desk und Clear Screen: Grundsätze des aufgeräumten Schreibtischs («clean desk») und des leeren Bildschirms («clear screen»), d. h., bei jedem Verlassen des Arbeitsplatzes sind vertrauliche und wichtige Dokumente und Informationsträger wegzuschliessen sowie eine passwortgeschützte Bildschirmsperre (Windows: L + Windowstaste bzw. Mac: Tastenkombination [ctrl – cmd – Q]) zu aktivieren.

EDUzh-Tenant: Eine Verwaltungseinheit, die für den Education (Schulbereich) des Kantons Zürich eingerichtet wurde. Ein Tenant ist die logische Einheit, bei der Benutzer, Anwendungen, Lizenzen und Daten einer Organisationseinheit zusammengefasst und verwaltet werden. Der EDUzh-Tenant basiert auf der Lizenz von EDUCA und umfasst alle Schulen, die an den EDUzh-Tenant angeschlossen sind.

Ereignisprotokoll: Die Protokollierung aller Ereignisse, die Software auf dem Betriebssystem betreffen: Starten und Stoppen, Zugriff auf Dateien, Änderungen von Berechtigungen.

Grundeinstellungen: Basiskonfigurationen und Parametrisierung von IKT-Systemen, An-wendungen und Zugängen.

IKT-Systeme: IKT-Systeme bestehen aus IT-Infrastruktur und Plattformen/Middleware (z.B. Datenbanken, Netzwerkstacks, Protokollstacks, Laufzeitumgebung).

Informationen: Alle Aufzeichnungen betreffend die Ausübung einer öffentlichen Tätigkeit, ausgenommen Notizen zum persönlichen Gebrauch.

Informationssicherheit: Verantwortliche der Schule müssen dafür sorgen, dass die Informationen, die im Schulbereich bearbeitet werden, durch angemessene Massnahmen geschützt werden. Dies bedeutet beispielsweise, dass nur berechtigte Personen Zugriff und Kenntnis von Informationen erhalten. Dazu gehören auch Massnahmen, die sicherstellen, dass die Informationen zur Verfügung stehen oder verhindern, dass sie verloren gehen.

IT-Arbeitsmittel: Die den Benutzenden von der Schule zur Verfügung gestellten Geräte (statische Geräte wie Drucker, Bildschirme, PCs und mobile Geräte) und Anwendungen.

IT-Infrastruktur: Die IT-Infrastruktur umfasst Soft- und Hardwaresysteme z.B. Clients, Server, Netzwerkkomponenten, Betriebssysteme, Treiber, mobile Endgeräte.

Lernprofil: Stärken und Schwächen in Lernbereichen erkennen. Je nach Ausprägung können Lernprofile Persönlichkeitsprofile darstellen und daher unter die besonderen Personendaten fallen.

Malware: Der Begriff Malware steht für MALicious SoftWARE – also bösartige Software. Malware dient als Oberbegriff für die Gesamtheit von Schadsoftware. Viren, Würmer, Trojaner, Adware und Spyware sind zum Beispiel Unterkategorien von Malware.

Mobile Geräte: Mobile Endgeräte unterscheiden sich von üblichen IKT-Systemen in Grösse und Gewicht und können ohne grössere körperliche Anstrengung mitgeführt werden. Zum Beispiel: Laptops, Smartphones, Tablets, SmartDevices, Anzeigegerät für VDI-Sessions.

Passwort Safe / Passwort Manager: Anwendung, mit deren Hilfe Zugangsdaten verschlüsselt gespeichert und verwaltet werden können.

Persönlichkeitsprofil: Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben. Sie sind in der Terminologie des IDG eine Teilmenge der besonderen Personendaten. (https://www.datenschutz.ch/lexika/grundbegriffe-und-definitionen/persoenlichkeitsprofil)

Personendaten: Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen Beispiel: Name, Vorname, Adresse, Gerätekennungen.

Profiling: Automatisierte Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen.

Protokoll: Eine Aufzeichnung der Ereignisse, die in IKT-Systemen und Anwendungen auftreten.

Randdaten: Das sind Spuren, die bei der Benutzung der IT-Infrastruktur entstehen und vom betreffenden IKT-System bzw. einer Anwendung in Logfiles protokolliert werden.

Sachdaten: Informationen, die sich nicht auf Personen beziehen.

Sicherheitsvorfall: Jedes Ereignis, dass potenziell zu einer Gefährdung der Informationssicherheit oder des Datenschutzes führt, weil Informationen oder Personendaten unbeabsichtigt bekanntgegeben, zerstört, verändert und vernichtet werden.

Starkes Passwort: Starke Passwörter sind mindestens 10 Zeichen lang (empfohlen sind 16 Zeichen), verfügen über mindestens einen Grossbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen) und haben keine erkennbare Konstruktionsregel. Es sollten keine Wörter verwendet werden, die im Duden enthalten sind, sondern Phantasiebegriffe. Wie sicher Ihr Passwort ist, können Sie unter www.passwortcheck.ch testen. Geben Sie aber nicht das wirkliche Passwort auf Prüfseiten (wie www.passwortcheck.ch) ein, sondern ein von der Struktur her vergleichbares Passwort.

Urheberrechtlich geschützte Werke: Dies sind Texte, Abbildungen, Fotografien und Musiknoten, Filme, Musik und Theaterstücke, deren Urheber/-in nicht bereits seit 70 Jahren verstorben sind. Ebenfalls geschützt sind Computerprogramme, deren Urheber/-in nicht bereits seit 50 Jahren verstorben sind.

Urheberrechtlich geschützte Werke im Unterricht: Als Unterricht gilt jede Veranstaltung im Rahmen eines Lehrplans (inkl. Vorbereitung, Hausaufgaben und Fernunterricht) einer Lehrperson an ihre Klasse bzw. den ihr zugewiesenen Lernenden.

Wechselmedien: Bei Wechselmedien handelt es sich um digitale Datenträger, die anstelle der fest eingebauten Speichermedien zur Speicherung von Daten dient. Z.B. USB-Sticks, Smart-Devices, SmartPhones, SmartWatches, externe Festplatten (HDD/SSD), welche kabelgebunden, kabellose, physischen und logischen mit IKT-Systemen verbunden werden können.

Zugang: Mit Zugang wird die Nutzung von IKT-Systemen, insbesondere System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person oder einem IKT-System, bestimmte Ressourcen zu nutzen.

Zugangsdaten: Zugangsdaten erlauben es den Benutzenden, Zugang zu den IKT-Systemen zu erhalten. Es kann sich dabei um Benutzernamen, Zahlen-PINs, Passwörter und weitere Angaben handeln.

12 Anhang III – Netiquette

Die Kantonsschule Enge und ihre Organisationseinheiten/Fachschaften sind im Internet und auf unterschiedlichen Social-Media-Kanälen präsent. Die Schule freut sich auf einen konstruktiven und respektvollen Austausch, spannende Diskussionen und Kommentare. Auch kritische Meinungen sind erwünscht. Bei der Interaktion mit der Schule im Internet und auf Social Media erklären Sie sich mit der vorliegenden Netiquette einverstanden. Sie ergänzt die Nutzungsbedingungen der Schule, die Sie akzeptiert haben.

Die Kantonsschule Enge behält sich vor, im Fall von Verstössen einzelne Beiträge ohne Angaben von Gründen zu löschen oder bei schweren und wiederholten Verstössen Benutzende von ihren Kanälen auszuschliessen.

Hinweis: Bei einigen Punkten in der folgenden Aufzählung liegen gemäss Gesetz strafbare Handlungen vor (insb. Pt. 1a).

Allgemein

1. Ich verfasse, verbreite oder poste:
    a. keine ehrverletzenden, rassistischen, diskriminierenden oder beleidigenden Beiträge oder Kommentare;
    b. keine themenfremden Beiträge oder Kommentare bzw. solche mit kommerziellen oder werbenden Inhalten (Spam);
    c. keine Beiträge von politischen und gewerkschaftlichen Organisationen;
    d. keine Beiträge oder Kommentare mit sich wiederholenden und identischen In-halten;
    e. keine Beiträge oder Kommentare mithilfe von Bots;
2. Ich verzichte auf namentliche Nennungen von schulischen Mitarbeitenden, Lehr-personen sowie Lernenden in öffentlichen Beiträgen;
3. Persönlichen Anfragen richte ich direkt an die zuständige Stelle der Schule;
4. Ich rufe nicht zu illegalen oder gefährlichen Handlungen oder Mobbing auf:
5. Wenn ich Mobbing bemerke, schreite ich dagegen ein oder informiere den/die Klassenlehrer/-in oder eine dafür zuständige Stelle innerhalb der Schule.

SMS/Messangerdienst/E-Mail

1. Ich versende Nachrichten nicht im Affekt, sondern lese sie noch einmal durch, um verletzende oder unangebrachte Äusserungen zu vermeiden;
2. Ich bleibe stets höflich und vermeide Beleidigungen;
3. Ich vermeide es, Konflikte online auszutragen, sondern bespreche sie mit den in-volvierten Personen persönlich;
4. Ich versuche, den Empfängerkreis von Nachrichten gering zu halten und richte Nachrichten nur an Personen, die tatsächlich davon betroffen sind;
5. Ich versuche, Nachrichtenverteiler regelmässig zu reduzieren;
6. Ich leite keine Kettenbriefe weiter;
7. Für grössere Empfängerkreise verwende ich stets das BCC-Feld, um die Kontakt-daten der Empfänger zu schützen.

Social-Media-Nutzung

1. Ich verbreite persönliche Informationen über mich mit Vorsicht;
2. Mir ist bewusst, dass ich beim Hochladen von Bildern und sonstigen Inhalten (Content) den Social-Media-Anbieter ggf. zur beliebigen Nutzung der Bilder/des Contents berechtige;

3. Ich bleibe auch in hitzigen Diskussionen sachlich;
4. Ich gehe nicht auf Beschimpfungen und Beleidigungen ein;
5. Ich setze Ironie und Sarkasmus mit Vorsicht ein, um Missverständnisse zu vermeiden;
6. Ich bin mir stets bewusst, an wen sich meine Mitteilung richtet, und passe meine Sprache der privaten und öffentlichen Kommunikation an;
7. Ich leite keine gefährlichen oder illegalen «Challenges» weiter.

Foto- und Videoaufnahmen

1. Ich frage vorgängig immer sämtliche abgebildeten Personen, ob sie mit einer Aufnahme einverstanden sind;
2. Ich versende, verbreite oder veröffentliche keine Aufnahme ohne vorgängige Zu-stimmung der abgebildeten Personen;
3. Falls mir Gewaltdarstellungen oder Aufnahmen mit verbotenem Inhalt weitergeleitet/geteilt werden, lösche ich diese und melde den Vorfall der Schule;
4. Ich beachte bei meinen Aufnahmen stets das Urheberrecht;
5. Ich versende keine Aufnahmen von mir oder von anderen an unbekannte Personen.

Videokonferenzen

1. Ich zeichne Videokonferenzen nur auf, wenn alle Beteiligten einverstanden sind;
2. Ich speichere die Videokonferenzen nur ab, wenn es notwendig und abgestimmt ist;
3. Ich zeichne nur dann Videokonferenzen auf, wenn ich als Lehrperson an der Konferenz teilnehme;
4. Mir ist bewusst, dass Chatverläufe ggf. gespeichert werden, um Mobbingvorfälle und strafbare Handlungen aufzuklären;
5. Ich nehme keine Videokonferenzen mit dem Handy auf und kopiere – ausser bei berechtigtem Anlass gemäss Ziff. 4 – keine Chatverläufe;
6. Ich darf meine Videokamera im Rahmen von Aufnahmen in Absprache ausschalten und jedenfalls meinen Hintergrund ausblenden, und ich weise andere Teilnehmende darauf-hin, dass sie das ebenfalls dürfen;
7. Mir ist bewusst, dass das Einschalten der Kamera von allen Teilnehmern aus pädagogi-scher Sichtweise angefordert werden kann;
8. Ich respektiere die Privatsphäre von Videokonferenzteilnehmern und fordere niemanden dazu auf, mir seine/ihre privaten Räumlichkeiten zu zeigen.

13 Anhang IV – Rollen und Berechtigungskonzept

13.1 Übersicht über die Rollen

An der Kantonsschule Enge bestehen die folgenden Rollen, die Schulangehörigen zugewiesen werden können:

- Schulkommission
- Schulleitung
- Fachvorstand
- Lehrperson
- Sekretariat
- Hausdienst
- Schulsozialarbeit
- Mediothek
- IT-Support
- Verwaltungsadministration
- Administration MS365
- Stundenplanung
- Schüler*innen
- Absenzenverwaltung

Anhand dieser Rollen erfolgt eine Zuordnung von Zugriffsberechtigungen.

Übersicht über Zugriffsmöglichkeiten

Die folgenden Zugriffsmöglichkeiten zu Datenablagen bestehen an der KS Enge (01.11.2024)

- OneDrive des einzelnen Benutzers
- SharePoint-Bibliothek Schulkommission
- SharePoint-Bibliotheken der Fachschaften
- SharePoint-Bibliothek der Schule für die Lehrerschaft
- SharePoint-Bibliothek der Schule für die Schülerschaft

- SharePoint-Bibliothek Schularchiv
- SharePoint-Bibliothek des IT-Supports
- Datenserver Userhomes
- Datenserver Rektorat
- Datenserver Hausdienst
- Datenserver Verwaltung
- VDI Zugang zur kantonalen Datenablage «Sekretariatslaufwerk»
- VDI Zugang zur kantonalen Datenablage «Rektoratslaufwerk»
- Webseite www.ken.ch
- Intranet SEK II
- IM-Datenbank
- Email-Postfach des individuellen Benutzers
- Geteiltes Emailpostfach Sekretariat sekretariat@ken.ch
- Geteiltes Emailpostfach support@ken.ch

13.2 Rollen und Zugriffe

	Schulkommission	Schulleitung	Fachvorstand	Lehrperson	Sekretariat	Hausdienst	Schulsozialarbeit	Mediothek	IT-Support	Verwaltungsadministration	Administration MS365	Schüler*innen	Absenzenverwaltung
OneDrive des einzelnen Benutzers	x	x	x	x	x	x	x	x	x	x	x	x	x
SharePoint-Bibliothek Schulkommission	x	x			x						x		
SharePoint-Bibliotheken der Fachschaften			x	x							x		
SharePoint-Bibliothek der Schule für die Lehrerschaft	x	x	x	x	x				x		x		
SharePoint-Bibliothek der Schule für die Schülerschaft	x	x	x	x	x		x		x		x		
SharePoint-Bibliothek Schularchiv		x									x		
SharePoint-Bibliothek des IT-Supports		x							x		x		
Datenserver Userhomes										x	x		
Datenserver Rektorat		x								x	x		
Datenserver Hausdienst						x				x	x		
Datenserver Verwaltung		x								x	x		
VDI Zugang zur kantonalen Datenablage «Sekretariatslaufwerk»		x								x			
VDI Zugang zur kantonalen Datenablage «Rektoratslaufwerk»		x								x			
Webseite www.ken.ch	x	x	x	x	x	x	x	x	x	x	x	x	x
Intranet SEK II	x	x	x	x	x	x	x	x	x	x	x	x	x
IM-Datenbank										x			
Email-Postfach des individuellen Benutzers	x	x	x	x	x	x	x	x	x	x	x	x	x
Geteiltes Emailpostfach Sekretariat sekretariat@ken.ch		x			x						x		
Geteiltes Emailpostfach support@ken.ch									x	x	x		
Geteiltes Emailpostfach Mediothek mediothek@ken.ch								x			x		
Geteiltes Emailpostfach Hausdienst hausdienst@ken.ch						x							
Kantonale Ablage für Schulsozialarbeit								x					