Kantonsschule Zürich Nord
Lang- und Kurzgymnasium
Fachmittelschule

Nutzungsrichtlinien

für die IKT-Systeme des Kantons Zürich und der Kantonsschule Zürich Nord

20. Juni 2024

Inhaltsverzeichnis

Basierend auf den eidgenössischen und kantonalen Rechtsgrundlagen im Bereich der Digitalisierung, des Copyrights und des Datenschutzes gelten für die Verwendung der IKT-Systeme an der Kantonsschule Zürich Nord nachfolgende Nutzungsrichtlinien.

1 Allgemeine Bestimmungen

1.1 Zweck

An der Kantonsschule Zürich Nord werden in verschiedenen Bereichen vom Kanton Zürich bereitgestellte 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 Rahmenbedingungen und Vorgaben (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 Zürich gebunden.

1.3 Geltungsbereich

Diese Nutzungsrichtlinie gilt für Mitarbeitende, Lehrpersonen, Lernende, Studenten sowie Schülerinnen und Schüler (nachfolgend «Benutzende» genannt), die Zugang zu IKT-Systemen der Kantonsschule Zürich Nord (nachfolgend «Schule» genannt) haben. 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.

Der Einsatz der IKT-Systeme und Anwendungen zu privaten Zwecken ist erlaubt, solange er sich in einem angemessenen Rahmen hält und den Lizenzbedingungen entspricht. Die Verwendung der IKT-Systeme und Anwendungen für Mining und andere ressourcenintensive private Tätigkeiten ist verboten.

Die Lizenzen von Microsoft 365 EDU können zusätzlich zur geschäftlichen Nutzung auf weiteren Geräten eingesetzt werden. Die private Nutzung ist auf bis zu 5 Desktop-Computern, 5 Tablets und 5 Smartphones (insgesamt 15 Geräte) gestattet. Eine Nutzung der für kommerzielle Zwecke ist jedoch untersagt.

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 Benutzenden über einen Zugriff auf die Logfiles informiert.

2 Nutzung von IT-Arbeitsmitteln

2.1 IT-Arbeitsmittel

An der Schule werden IT-Arbeitsmittel eingesetzt, die von der Schule, dem Digital Service Center Sek II (DSC Sek II) und vom Amt für Informatik (AFI) bereitgestellt werden. Darüber hinaus werden BYOD-Geräte gemäss Ziff. 4 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 2.1 bis 2.5 betreffen IT-Arbeitsmittel, die den Benutzenden von der Schule zur Verfügung gestellt werden (d.h. nicht BYOD-Geräte).

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

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 – nach Beantragung bei und Bewilligung durch den IKT-Verantwortlichen – lediglich die von der Schule bzw. vom Kanton freigegebenen Anwendungen installiert werden. Diese sind über einen «Software Kiosk» zugänglich.

2.4 Supportorganisation

Der Support wird durch das IT-Team der KZN, das Digital Service Center Sek II (DSC Sek II) und das Amt für Informatik (AFI) gewährleistet. Das IT-Team der KZN dient dabei stets als erste Anlaufstelle. Die Kontaktangaben sind im Intranet und über das Webportal der IT (KZN) abrufbar.

2.5 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.

Nutzungsvorgaben und Anleitungen zu kantonalen Anwendungen können über den Helpdesk des Digital Service Center Sek II (DSC Sek II) abgerufen werden. Hilfestellungen und Nutzungsvorgaben zu Anwendungen, die nur an der KZN eingesetzt werden, sind im Intranet oder auf dem Webportal der IT (KZN) publiziert.

2.6 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 müssen betroffene Benutzende umgehend eine Meldung bei der Supportorganisation machen.

3.1.1 Benutzerkonto

Erhalten die Benutzenden ein Benutzerkonto, dient dies für den Zugriff auf folgende Dienste und Applikationen:

- WLAN und Netzwerk (LEUnet Schule)
- Microsoft 365 EDU Konto (inklusive Outlook E-Mail und Teams)
- Intranet und Druckerumgebung der Schule
- Diverse weitere Dienste wie Adobe CC, Moodle, Classtime, Exam.net, isTest etc.

Der Zugang zu den IKT-Systemen erfolgt über einen Benutzernamen und ein Passwort und ist zusätzlich durch eine Zwei-Faktor-Authentifizierung geschützt.

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.

3.1.2 Passwortschutz

Die Benutzenden sind verpflichtet, für sämtliche Zugänge ein starkes Passwort zu wählen. Die Verwendung eines Passwort-Managers (Software-Applikation) wird empfohlen.

Passwörter und alphanumerische PIN-Codes müssen entweder
– mindestens 12 Zeichen lang sein und aus vier Zeichenarten bestehen
– mindestens 24 Zeichen lang sein und aus zwei Zeichenarten bestehen

Die Zeichenarten sind dabei wie folgt kategorisiert:
– Grossbuchstaben (A, B, C etc.)
– Kleinbuchstaben (a, b, c etc.)
– Ziffern/Zahlen (0, 1, 2 etc.)
– Sonderzeichen (+, =, % etc.).

Für jeden Zugang ist ein separates, einzigartiges Passwort zu wählen. Das Passwort ist alle 90 Tage zu ändern, sofern der entsprechende Zugang nicht durch eine Zwei-Faktor-Authentifizierung abgesichert ist.

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 oder den Unterricht betreffen (nachfolgend «schulinterne Informationen»), nicht unbeabsichtigt offengelegt, entwendet, gelöscht oder unkenntlich gemacht werden.

3.2.1 Datensicherung

Sämtliche schulinternen administrativen Informationen (Unterrichtsmaterialien fallen *nicht* in diese Kategorie) müssen auf der vom Kanton bereitgestellten Datenablage (Microsoft 365 Cloud-Dienste und VDI) gespeichert werden, damit eine zentrale Datensicherung und Verfügbarkeit gewährleistet sind. Dies gilt auch für Informationen, die zusätzlich auf einem Wechselmedium (USB-Stick oder externe Festplatte) 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.

3.2.2 Berechtigungen

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

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

Erhalten Benutzende Zugriff auf schulinterne Informationen, die nicht für sie bestimmt sind, müssen sie dies dem Datenersteller umgehend mitteilen.

3.2.3 Schutzstufen

Je nach Inhalt einer Information kann ein Dokument kategorisiert und klassifiziert werden. 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. Verantwortlich für die korrekte Einstufung von Dokumenten (Kategorisierung und Klassifizierung) ist der Ersteller eines Dokuments.

Verwendete Einstufungen im Kanton Zürich

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

Informations-Klassifizierungen	
Öffentlich	Broschüren, Webseite, Plakate und weitere, veröffentlichte Informationen etc.
Intern	Intranet, Lehrmittel, Prüfungsvorlagen, Unterrichtsfolien, Anleitungen, Adresslisten, Fotos (soweit nicht zur Veröffentlichung vorgesehen) etc.
Vertraulich	Zeugnisse, einzelne Noten, Lernprofile, Disziplinarmassnahmen, Angaben über die Gesundheit, Quarantänemassnahmen, Religionszugehörigkeit etc.
Geheim	Hochsensible Informationen über Lernende, wie bspw. strafrechtliche Sanktionen, ärztliche Gutachten, Korrespondenz zum Nachteilsausgleich (Diagnosen) etc.

Schutzstufen	
Grundschutz	Log-Files zur Änderungsverfolgung, Cookies auf Web-Seiten, etc.
Erhöhter Schutz	Benutzer mit Passwort und Zugriffssteuerung von Ablage-Ordnern / Zuweisung der Verzeichnisse, Zwei-Faktor-Authentifizierung

In den offiziellen Austauschkanälen und Kollaborationsplattformen (Microsoft 365 Cloud-Dienste und VDI) innerhalb der Schule (d.h. ohne Beteiligung externer Personen) können Dokumente aller Schutzstufen geteilt und bearbeitet werden. Für vertrauliche und geheime Informationen müssen zusätzlich eingeschränkte Zugriffsrechte bestehen. Das bedeutet, dass diese Kanäle oder Arbeitsordner nur einem stark eingeschränkten Benutzerkreis zugänglich sein dürfen (Rollen- und Benutzerkonzept).

3.2.4 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.

3.2.5 Sorgfaltspflichten

Um sensible Daten zu schützen, herrscht eine strikte Clean Desk und Clear Screen Policy. Der Bildschirm eines unbeaufsichtigten Gerätes muss gesperrt und passwortgeschützt sein (Tastenkombination *Win* + *L* bei Windows resp. *Control* + *Command* + *Q* bei macOS).

Die Benutzenden lassen keine physischen Träger von Informationen (d.h. Wechselmedien, Papier etc.) unbeabsichtigt liegen.

Whiteboards und Wandtafeln, auf denen sensible Informationen und Personendaten ersichtlich sind, müssen nach dem Gebrauch gereinigt werden.

Störungen oder Defekte an bereitgestellte IT-Arbeitsmitteln sind umgehend dem IT-Team der KZN zu melden.

Zutritt zu nicht öffentlich zugänglichen Räumen darf nur autorisierten bzw. angemeldeten Personen gewährt werden. Auffällige Personen müssen gemäss Ziff. 3.7 umgehend gemeldet werden.

3.3 Schutz vor Malware

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

1. Die Schutzsoftware darf nicht umgangen oder deaktiviert werden.
2. Es müssen stets 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 markiert werden. Bei einer Häufung solcher Fälle hat eine Meldung beim IT-Team der KZN 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 angeklickt 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 sofort gemeldet werden (vgl. Ziff. 3.7).

3.4 Schutz von Kommunikation

3.4.1 E-Mail

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

– die Korrespondenz im Zusammenhang mit dem Schulbetrieb.
– die Organisation des Klassenbetriebs.
– den Empfang von allgemeinen Informationen und Weisungen der Schule bzw. übergeordneter Instanzen.

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

1. Die Benutzenden sind für die Kontrolle und Pflege ihres Postfachs verantwortlich. E-Mails werden innert zwei Werktagen beantwortet.
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. Die E-Mailadresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshopping etc.) genutzt werden.
5. Das E-Mail-Konto darf nicht zum Versand oder Verbreitung von beleidigenden, persönlichkeitsverletzenden, rassistischen, sexistischen oder pornographischen Inhalten oder zur Planung, Vorbereitung, Organisation und Durchführung von Verbrechen und Vergehen benutzt werden.

3.4.2 Collaboration Tools

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

1. Die Benutzenden verwenden Collaboration Tools für die schulinterne Kommunikation.
2. Die Anzahl neuer Teams/Kanäle ist auf das Nötige limitiert.
3. Der bzw. die Betreiberin eines Teams/Kanals ist für die spezifischen Berechtigungen verantwortlich und sorgt dafür, dass der Informationsaustausch auf das Notwendige beschränkt und dass die Netiquette auch im Chat eingehalten wird.
4. Vertrauliche oder höher klassifizierte Informationen sind – sobald sie den EDUzh-Tenant verlassen - End zu End verschlüsselt, egal ob im Chat, Teams-Kanal oder im Videoanruf. Im EDUzh-Tenant erfolgt die End-zu-End-Verschlüsselung automatisch.
5. Chats und Social-Media-Kanäle sind dazu bestimmt, sich auszutauschen. Vertrauliche und höher klassifizierte Daten und Dokumente sind nicht dort, sondern in den dafür vorgesehenen Speichern (Microsoft 365 Cloud-Dienste und VDI) abzulegen und durch eine Zugangskontrolle geschützt zu verlinken.

3.5 Netzwerk- und Internetnutzung

Das Schulnetzwerk steht den Schulangehörigen über einen persönlichen Zugang zur Verfügung. Benutzenden, die keinen persönlichen Zugang erhalten, steht das Gästenetzwerk zur Verfügung. Für die Nutzung des Schul- und Gästenetzwerks gelten folgende Vorgaben:

1. Das Hoch- und Herunterladen von umfangreichen, nicht unterrichts- oder schulbezogenen Dateien ist verboten.
2. Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden.
3. Der Einsatz persönlicher Hotspots ist auf dem Schulareal verboten, ausser er wird von der Supportorganisation ausdrücklich erlaubt.
4. Der Besuch des Darknets ist verboten.
5. 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.
6. Während des Unterrichts ist der Besuch von Social-Media-Plattformen und sonstigen Unterhaltungsseiten verboten, ausser diese sind Bestandteil der Unterrichtssequenz.
7. Schulinterne administrative Informationen (Unterrichtsmaterialien fallen *nicht* in diese Kategorie) dürfen nur in Absprache mit der Schulleitung ins Internet hochgeladen werden, um beispielsweise Übersetzungen in Gratis- und AI-Tools zu nutzen.
8. Die Netiquette gemäss Anhang III ist einzuhalten.

Sämtliche Webseitenzugriffe werden automatisch protokolliert. Die Protokolldaten können von der Schule oder von den kantonalen Institutionen im begründeten Verdachtsfall personenbezogen ausgewertet werden. Die Benutzenden werden im konkreten Fall informiert, sofern eine Rückverfolgbarkeit möglich ist.

3.6 Arbeiten von unterwegs oder zu Hause

Auf das Verwaltungs-Netzwerk (Schulleitung, Zentrale Dienste, Sekretariat etc.) der Schule erfolgt der Fernzugriff ausschliesslich über eine gesicherte Verbindung (VPN oder Citrix).

Auf das pädagogische Netzwerk (Microsoft 365 EDU Konto, Intranet Sek II etc.) ist der Zugang via Benutzername und Passwort möglich. Die entsprechenden Dienste sind so konfiguriert, dass die Verbindung via Browser oder entsprechender Software-App (z.B. Microsoft OneDrive) standardmässig verschlüsselt ist.

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, Privacy Filter). Gespräche über schulinterne Angelegenheiten und sämtliche Informationen, die dem Amtsgeheimnis unterliegen, werden vermieden.

3.7 Meldepflicht

Sicherheitsvorfälle, Verluste beziehungsweise Defekte von IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem IT-Team der KZN zu melden.

4 Persönliche Geräte / BYOD

4.1 Grundsatz

Der Einsatz von persönlichen mobilen Geräten (BYOD-Geräten) an der Schule ist grundsätzlich erlaubt. Dabei handelt es sich um Arbeitsgeräte wie Convertibles, Notebooks oder Tablets. Smartphones zählen ebenfalls zu den BYOD-Geräten, da sie für den Schutz (Zwei-Faktor-Authentifizierung) des persönlichen M365 EDU Kontos zum Einsatz kommen.

BYOD-Geräte von Mitarbeitenden und Lehrpersonen, die direkten Zugriff auf den Microsoft 365 EDUzh-Tenant und damit auf schützenswerte und besonders schützenswerte Daten haben, müssen vorgängig einen Registrierungsprozess durchlaufen.

Die Nutzung der BYOD-Geräte 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.

Eine Verbindung der BYOD-Geräte mit dem Schulnetzwerk ist zulässig.

4.2 Geräteanforderungen

Für den Einsatz der BYOD-Geräte an der Schule gelten folgende Mindestanforderungen:
– Passwort-, PIN- oder biometrischer Schutz (Finger- oder Gesichts-Scan)
– aktuelles Betriebssystem
– aktuelle Firewall und aktueller Virenschutz (ausgenommen Smartphones)
– 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 die schulischen und die kantonalen Vorgaben erfüllt.

4.4 Support

Für persönliche Geräte besteht kein Supportanspruch. Für die fachgerechte Entsorgung (z.B. 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 beispielsweise ein Auskunfts-, Berichtigungs- und Löschgesuch an eine/n Benutzende/n, leitet diese/dieser das Gesuch umgehend an die Schulleitung weiter.

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

5.2 Im Unterricht

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

Lehrpersonen haben den Unterricht so zu gestalten, dass möglichst wenig Personendaten der Schülerinnen und Schüler automatisiert bearbeitet werden. Es gilt das Prinzip der Datensparsamkeit und Datenminimierung.

5.2.1 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 die Supportorganisation.

5.2.2 Nutzung von Social Media

Der Einsatz von Social Media im schulischen Kontext (z.B. 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 dann, wenn die jeweilige Lehrperson die Klasse nicht mehr betreut, sind die Kanäle, Gruppen, Benutzerzugänge und Dokumente zu löschen.

5.2.3 Besondere Personendaten

Schriftliche Aufzeichnungen (Aufsätze, Gedichte etc.), grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen von Schülerinnen und Schülern, die Angaben über besondere Personendaten enthalten, sind mindestens als vertraulich zu klassifizieren und unterliegen einer erhöhten Schutzstufe. Sie sind spätestens am Ende der Ausbildung zu anonymisieren oder zu vernichten. Die Rekursfristen sind einzuhalten.

5.2.4 Bilder
Schulangehörige dürfen nicht ohne ihre Zustimmung gefilmt, fotografiert oder in anderer Form aufgenommen werden. Gruppenbilder sind so aufzunehmen, dass einzelne Personen nicht hervorgehoben werden. Klassenfotos sind stets freiwillig.

5.2.5 Bekanntgabe
Schriftliche Aufzeichnungen, grafische Darstellungen sowie Bild-, Ton- oder Video-Aufnahmen dürfen ohne die explizite Zustimmung der betroffenen Person weder veröffentlicht noch Dritten bekanntgegeben werden. Ebenso dürfen Porträts von Schulangehörigen ohne explizite Einwilligung nicht auf der öffentlich zugänglichen Schulwebseite veröffentlicht werden.

Bei Schülerinnen und Schüler unter 14 Jahren ist die Zustimmung der Eltern einzuholen.

6 Urheberrechte

6.1 Generell
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 umfasst das Vervielfältigen ganzer Radio- und Fernsehsendungen sowie das unentgeltliche Zugänglichmachen für berechtigte Benutzer, einschliesslich des Abrufens und Herunterladens einzelner Sendungen aus dem 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 Webpräsenz der Schule, in sozialen Medien (einschliesslich geschlossener Gruppen), auf Videoportalen etc.
    c. Das Bearbeiten oder Verändern von Werken.
4. Werden Lehrmittel für andere Lehrpersonen, die ganze Schule oder Dritte erstellt, dürfen diese keine Zusammenstellungen von fremden Werkausschnitten erhalten. Vor der Erstellung eines Lehrmittels ist Rücksprache mit der Schulleitung zu nehmen.

6.2 Im Unterricht
6.2.1 Grundsatz
Im Unterricht dürfen urheberrechtlich geschützte Werke auf jegliche Art verwendet werden. Das beinhaltet auch das Anfertigen von analogen oder digitalen Kopien von Ausschnitten eines Werkexemplars (Erläuterungen zum Umfang siehe Anhang II – Glossar), nicht aber von ganzen Werkexemplaren, die im Handel erhältlich sind. Lehrpersonen dürfen Werke für einzelne Klassen in einem geschützten Bereich (z.B. im Microsoft 365 EDUzh-Tenant mit Teams, OneNote, OneDrive oder über Moodle, Intranet etc.) zugänglich machen.

Von der erlaubten Vervielfältigung nicht erfasst sind jedoch das Kopieren von Computer-Programmen sowie das Aufzeichnen von Vorträgen, Bühnenaufführungen und Konzerten.

6.2.2 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. Beim Bereitstellen solcher Kopien für mehrere Lehrpersonen aus Quellen, die nicht Radio- oder Fernsehsendungen sind, muss die Erlaubnis des Rechteinhabers eingeholt werden.

6.2.3 Bilder

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

6.2.4 Musikaufführungen

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

1. die Aufführung durch Schulangehörige erfolgt;
2. der Anlass sich ausschliesslich an die Schul- und die Familienangehörigen richtet; und
3. der Anlass unentgeltlich ist.

6.2.5 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.

6.2.6 Lehrmittel

Es dürfen keine Zusammenstellungen von fremden Werkausschnitten für andere Lehrpersonen oder für die ganze Schule zugänglich gemacht werden.

Werke, welche Lehrpersonen im Rahmen ihres Arbeitsverhältnisses erstellt haben, dürfen nur in Absprache mit der Schulleitung kostenpflichtig an die Schülerinnen und Schüler abgegeben werden.

Werke, welche Lehrpersonen ausserhalb ihres Arbeitsverhältnisses erstellt haben, dürfen nur in Absprache mit der Schulleitung kostenpflichtig an die Schülerinnen und Schüler abgegeben werden.

6.3 Ausserhalb des Unterrichts

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

7 Massnahmen bei Verstössen

Bei einer missbräuchlichen Nutzung der IKT-Systeme, einschliesslich der Verletzung von Urheberrechten, drohen den Benutzenden Massnahmen. Missbräuchlich ist die Nutzung, wenn sie gegen diese Nutzungsrichtlinie, weitergehende schulinterne Richtlinien und Weisungen oder die anwendbaren gesetzlichen Bestimmungen verstösst oder die Rechte Dritter verletzt. Zwecks Abklärung von Missbrauchsvorfällen können Randdaten, Protokolle und Log-Files 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 (rechtliches Gehör) gegeben.

Die Schule kann unter anderem folgende Massnahmen ergreifen:
1. Zuerst erfolgt ein persönliches Gespräch, bei dem die Parteien ihre Beweggründe darlegen können.
2. In der Regel erfolgt dann eine Abmahnung beziehungsweise eine Verwarnung, bevor weitere Massnahmen ergriffen werden.
3. Bei Schülerinnen und Schülern erfolgt je nach Schwere des Verstosses eine Meldung an die gesetzlichen Vertreter.
4. Eintrag ins Schüler/innen- resp. Personal-Dossier.
5. Bei gravierenden oder wiederholten Verstössen kann die Schule gemäss dem anwendbaren Disziplinarreglement oder dem Personalrecht Disziplinarmassnahmen ergreifen.
6. Die Schule kann nebst Schadenersatz auch, sofern rechtlich zulässig, die Wiederherstellung des ursprünglichen Zustands verlangen.
7. Stellt die Schule ein strafbares Verhalten fest, kann sie ohne Vorwarnung eine Strafanzeige einreichen bzw. eine Meldung bei der zuständigen Behörde vornehmen.

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

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, Ausschluss oder ein erfolgreicher Abschluss der Schule. Die Beendigung von Nutzungsvereinbarungen wird nachfolgend summarisch als «Austritt» bezeichnet.

Das Benutzerkonto erlischt 14 Tage nach Austritt aus der Schule. Vor dem Ende der Benutzerrolle wird in ausreichender Frist ein Erinnerungs-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 zurückgegeben 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 BISR entstehen.

10 Anhang

10.1 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 des Regierungsrates (BISR) für die kantonale Verwaltung vom 17. Juni 2020, in Kraft getreten 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

- Suche nach Datenschutz-Dokumenten im Kanton Zürich: Link
- 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 August 2022 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 Gültigkeit 2017 - 2022 (Archiv) Link
- ProLitteris GT 7 Gültigkeit 2022 - 2026 Link und entsprechendes Merkblatt für Schulen Link

Glossare

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

10.2 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 auch 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) werden Computerprogramme bezeichnet, die genutzt werden, um eine nützliche oder gewünschte nicht system-technische Funktionalität zu bearbeiten oder zu unterstützen. z.B. Geschäftsanwendungen, Applikationen, Clouddienste, gem. IKT-Strategie Fachapplikationen, Kantonsapplikationen.

Ausschnitt eines Werkexemplars: Als Faustregel gilt, dass der zu vervielfältigende Ausschnitt maximal 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 (z.B. Kursbesuchende, Bibliotheksbenutzende, Mieter von Schulräumen etc.), welche die IT-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: *Win* + *L* oder macOS: *Control* + *Command* + *Q*) zu aktivieren.

EDUzh-Tenant: Eine Verwaltungseinheit, die für den Education-Bereich (Schulbereich) des Kantons Zürich eingerichtet wurde. Ein Tenant ist eine logische Einheit, in 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, Anwendungen und Zugängen.

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

Informationen: Alle Aufzeichnungen betreffend 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 Manager / Passwort Safe: 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 (siehe auch Link).

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: 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 potentiell 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 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, SmartDevices, SmartPhones, SmartWatches, externe Festplatten (HDD/SSD), welche kabelgebunden, kabellos, physisch oder logisch 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.

10.3 Anhang III – Netiquette

Die Kantonsschule Zürich Nord und ihre Organisationseinheiten sind im Internet präsent und nutzen zum Austausch von Informationen unter den Schulangehörigen verschiedene Kommunikationskanäle. 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 über die internen Kommunikationskanäle und im Internet richten sich die Schulangehörigen nach der vorliegenden Netiquette. Sie ergänzt die Nutzungsbedingungen der Schule, die Sie akzeptiert haben. Sie ergänzt die Nutzungsbedingungen der Schule, die Sie akzeptiert haben.

Die Schule behält sich vor, im Fall von Verstössen einzelne Beiträge ohne Angabe von Gründen zu löschen oder bei schweren und wiederholten Verstössen Benutzende von ihren Kanälen auszuschliessen und Disziplinarmassahmen in die Wege zu leiten.

Allgemein

1. Ich versende:
   a. keine ehrverletzenden, rassistischen, sexistischen, diskriminierenden oder beleidigenden Beiträge oder Kommentare;
   b. keine themenfremden Beiträge oder Kommentare bzw. solche mit kommerziellen oder werbenden Inhalten (Spam);
   c. keine sich wiederholende oder identische Beiträge oder Kommentare;
   d. keine Beiträge oder Kommentare mithilfe von Bots.
2. Ich verzichte auf namentliche Nennungen von schulischen Mitarbeitenden, Lehrpersonen sowie Lernenden in öffentlichen Beiträgen.
3. Persönliche 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.

E-Mail & Microsoft Teams

1. Ich bin mir stets bewusst, an wen sich meine Mitteilung richtet und passe meine Sprache der privaten und öffentlichen Kommunikation an.
2. Ich bleibe stets höflich und vermeide Beleidigungen. Ironie und Sarkasmus setze ich mit Vorsicht ein, um Missverständnisse zu vermeiden.
3. Ich erstelle Nachrichten so, dass sie mit einer höflichen Anrede beginnen, das Anliegen unter Berücksichtigung sprachlicher Normen korrekt zum Ausdruck bringen und mit einer freundlichen Grussformel enden. Bei längeren Konversationen auf Microsoft Teams gehe ich vor, wie in einem mündlichen Gespräch: Ich grüsse in der ersten Nachricht und verabschiede mich in der letzten.
4. Ich versende Nachrichten nicht im Affekt, sondern lese sie noch einmal durch, um verletzende oder unangebrachte Äusserungen zu vermeiden.

5. Ich vermeide es, Konflikte online auszutragen, sondern bespreche sie mit den involvierten Personen persönlich.
6. Ich kopiere keine Chatverläufe, ausser bei berechtigtem Anlass (beispielsweise um Mobbingvorfälle und strafbare Handlungen aufklären zu lassen).
7. Ich versuche, den Empfängerkreis von Nachrichten klein zu halten und richte Nachrichten nur an Personen, die tatsächlich davon betroffen sind.
8. Ich versuche, Nachrichtenverteiler regelmässig zu reduzieren.
9. Ich leite keine Kettenbriefe weiter.
10. Für grössere Empfängerkreise verwende ich stets das BCC-Feld, um die Kontaktdaten der Empfänger zu schützen

Nutzung von Social Media

1. Ich verbreite persönliche Informationen über mich mit Vorsicht.
2. Mir ist bewusst, dass ich beim Hochladen von Bildern und anderen Inhalten den Anbietern sozialer Medien (Facebook, Twitter, Snapchat, TikTok etc.) gegebenenfalls zur beliebigen Nutzung der Bilder/der Inhalte berechtigte.
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 Zustimmung der abgebildeten Personen.
3. Falls mir Gewaltdarstellungen oder Aufnahmen mit verbotenem Inhalt weitergeleitet/geteilt werden, melde ich den Vorfall der Schule und lösche die entsprechenden Inhalte nach der Beweisaufnahme.
4. Ich beachte bei meinen Aufnahmen stets das Urheberrecht.
5. Ich versende keine Aufnahmen von mir oder von anderen an unbekannte Personen.

Videokonferenzen

1. Das Streamen von Videokonferenzen ist nur erlaubt, wenn alle Beteiligten vorgängig ihr Einverständnis dafür gegeben haben.
2. Das Aufnehmen und Abspeichern von Videokonferenzen ist ausschliesslich im Rahmen der Aus- resp. Weiterbildung an der KZN erlaubt und auch nur dann, wenn sämtliche Beteiligten vorgängig ihr schriftliches Einverständnis dafür gegeben haben.
3. Das Weiterleiten von Videokonferenzen an unbeteiligte Dritte ist nicht erlaubt.
4. Ich darf meine Videokamera im Rahmen von Aufnahmen jederzeit ausschalten oder meinen Hintergrund ausblenden.
5. Ich respektiere die Privatsphäre von Videokonferenzteilnehmern und fordere niemanden dazu auf, mir seine/ihre privaten Räumlichkeiten zu zeigen.