Allgemeine ICT-Nutzungsrichtlinie (AINRL) ABZ

Allgemeine ICT-Nutzungsrichtlinie (AINRL) ABZ V11.docx

Inhalt

Die Schulleitung beschliesst am 16.03.2023 nachfolgende ICT-Nutzungsrichtlinie.

I. Allgemeine Bestimmungen

1. Zweck

An dieser Schule werden in verschiedenen Bereichen vom Kanton Zürich bereitgestellten IKT-Systeme 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.

2. Grundlagen

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

Die Schule erfüllt einen kantonalen Leistungsauftrag. Aus diesem Grund untersteht sie in diesem Bereich dem Gesetz über die Information- und den Datenschutz IDG sowie den weiteren kantonalen Rechtserlassen, und ist an die Grundrechte gebunden. In Bereichen, in denen sie mit privaten Anbietern konkurrenzieren, gilt das Bundesgesetz über den Datenschutz. Wo die Schule ihr Angebot in den EU/EWR-Markt richtet, gilt ausserdem die Datenschutz-Grundverordnung.

3. Geltungsbereich

Diese Nutzungsrichtlinie gilt für Mitarbeitende, Lehrpersonen, Lernende, Studenten sowie Lernende, die Zugang zu IKT-Systemen der ABZ (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 akzeptieren die Benutzenden die **Nutzungsrichtlinie** und bestätigen, über die Konsequenzen bei deren Nichtbeachtung informiert worden zu sein.

4. Begriffe

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

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.

6. Auswertungen von Randdaten

Rückverfolgung von Sicherheitsvorfällen können die Schule und der Kanton Zürich innert der gesetzlichen Frist auf diese Logfiles zurückgreifen.

II. Nutzung von IT-Arbeitsmitteln

Interne IT-Arbeitsmittel sind Eigentum des Kantons Zürich oder der Schule. Diese behandeln die Benutzenden mit Sorgfalt und schützten sie vor Diebstahl und Beschädigung. Räume, die IT-Arbeitsmittel enthalten, sind beim Verlassen abzuschliessen.

Es dürfen keine fremden, nicht autorisierten bzw. nicht bewilligten IT-Arbeitsmittel verwendet werden.

1. Änderungen

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

2. 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.

3. Supportorganisation

Für den Support sind der schulinterne Field-Support und der Digitale Service Center SekII zuständig. Der schulinterne Field-Support dient als erste Anlaufstelle. Hierzu dient das interne **ABZ-Ticket-Tool 4me**.

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 im Intranet oder SharePoint auffindbar.

5. Entsorgung

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

III. Datensicherheit

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 betroffenen Benutzer/-in umgehend eine Meldung bei der zuständigen Supportorganisation vornehmen.

a. Benutzerkonto

Erhält der Benutzende ein Benutzerkonto, dient dies für die Office 365 Umgebung den Intranet Sek II (IS2) Zugang, dem internen WLAN Netzwerk Zugang sowie der Druckerinfrastruktur.

Der Zugang zum Benutzerkonto erfolgt über einen Benutzernamen und ein Passwort und einer Zwei-Faktor-Authentisierung **MFA**.

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 Schule stellt allen Benutzenden ein Initialpasswort zur Verfügung, welches zwingend durch ein persönliches Kennwort zu ersetzen ist. Die Benutzenden sind verpflichtet, für sämtliche Zugänge ein starkes Passwort zu wählen. Das Passwort muss mindestens 10 Zeichen lang sein, Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen (#$* etc.) enthalten.

Kennwörter für die ABZ IT-Infrastruktur dürfen nicht im Internetbrowser gespeichert werden. Zur Speicherung der Kennwörter wird ein Passwort-Manager (**bitwarden.com**) als Browser Add-On empfohlen (Hierzu bietet die technische IT aber keinen Support an).

Die für die IKT-Systeme verwendeten Passwörter dürfen nicht für private Zugänge verwendet werden.

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.

a. Datensicherung

Sämtliche schulinternen Informationen müssen auf der von der Schule bzw. dem Kanton bereitgestellten Datenablage (bspw. schuleigener Server oder Clouddienst) gespeichert werden. Das 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.

Es ist verboten, schulinterne Informationen auf nicht autorisierten bzw. bewilligten externen Wechselmedien bzw. nicht freigegebenen Clouddiensten zu speichern.

b. Berechtigungen

Die Schule verfügt über ein Berechtigungs- und Zugriffskonzept, das für die Benutzenden verbindlich ist.

Es dürfen nur jene Daten geöffnet bzw. verwendet werden, die 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.

c. 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.

Die kantonale Einstufung lautet folgendermassen:

Datenkategorien			**Informations-Klassifizierung**				**Schutzstufen**	
1	2	3					1	2
Sachdaten	Personendaten	Besondere Personen-daten	Öffentlich	Intern	Vertraulich	Geheim	Grund-schutz	Erhöhter Schutz

Für 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			
Öffentlich	Intern	Vertraulich	Geheim
Bspw. Broschüren, Webseite, Plakate und weitere, veröffentlichte Informationen	Bspw. Intranet, Lehrmittel, Prüfungsvorlagen, Unterrichtsfolien, Anleitungen, Adresslisten, Fotos	Zeugnisse, einzelne Noten, Lernprofile, Disziplinarmassnahmen, Angaben über die Gesundheit wie auch Quarantänemassnahmen,	Hochsensible Informationen über Lernende, wie bspw. strafrechtliche

	(soweit nicht zur Veröffentlichung vorgesehen), etc.	Religionszugehörigkeit, etc.	Sanktionen, ärztliche Gutachten

Schutzstufen	
1	2
Grundschutz	Erhöhter Schutz
Bspw. Cookies auf Web-Seiten, Log-Files zur Änderungsverfolgung	Benutzer mit Passwort und Zugriffssteuerung von Anlage-Ordnern / Zuweisung der Verzeichnisse, Zwei-Faktoren-Authentifizierung

- Konkret bedeutet das, dass z.B. Sachdaten, die öffentlicher Natur sind, mit einem **Grundschutz** ausreichend versehen sind und daher für Benutzer leicht zugänglich gehalten werden können.
- Hingegen **Personendaten** oder **Besondere Personendaten**, die **intern, vertraulich oder geheim** sind, erfordern einen **erhöhten Schutz** durch mindestens einer Zwei-Faktoren-Authentifizierung und bestenfalls weitergehende Kontrollen, z.B. die Freigabe durch eine Kontrollstelle, oder eine Mehrfaktoren-Authentifizierung.

d. 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.

e. Weitere Sorgfaltspflichten

Es herrscht eine strikte **Clean Desk** und **Clear Screen Policy**, somit muss jeder Laptop oder PC beim Verlassen des Arbeitsplatzes, durch eine Bildschirmsperre geschützt werden (Windows-Taste +L auf Tastatur drücken). Jede Mitarbeiterin und jeder Mitarbeiter müssen bei Abwesenheit seine vertraulichen Unterlagen verschliessen.

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

Whiteboards und Wandtafeln mit schulinternen Informationen sind nach dem Gebrauch zu reinigen.

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

Zutritt zu nicht öffentlich zugänglichen Räumen darf nur autorisierten bzw. angemeldeten Personen gewährt werden. Auffällige Personen müssen umgehend gemeldet werden (vgl. Ziff. 7).

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;
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 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 umgehend gemeldet werden (vgl. Ziff. 7).

4. Schutz von Kommunikation

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.
2. E-Mails dürfen nicht an externe (private oder geschäftliche) Postfächer weiter- oder umgeleitet werden.
3. Die E-Mailadresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshopping, etc.) genutzt werden.
4. 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.

5. Netzwerk- und Internetnutzung

Das Schulnetzwerk steht den Benutzenden via einen persönlichen Zugang zur Verfügung. Benutzenden, 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 grossen Dateien sind zu verhindern, insbesondere sind die Installationen von Spielen und grossen Audio- und Videodateien aus dem Internet;

2. Der Besuch von Webseiten, die über kein SSL-Zertifikat (HTTPS) verfügen, ist zu vermeiden.
3. Der Besuch des Darknets ist verboten;
4. 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;
5. Während des Unterrichts ist der Besuch von Social-Media und sonstige Unterhaltungsseiten verboten, ausser dies gehört zum Unterrichtsstoff;
6. Schulinterne Informationen dürfen nicht ins Internet hochgeladen werden, z.B., um Übersetzungen in Gratistools zu erwirken;
7. 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.

6. Arbeiten von unterwegs oder zu Hause

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

7. Meldepflicht

Sicherheitsvorfälle, der Verlust bzw. Defekte von internen IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem schulinternen Field-Support / IKT Verantwortlichen zu melden.

IV. Persönliche Geräte / BYOD

Das Mitführen von persönlichen mobilen Geräten an der Schule ist grundsätzlich erlaubt. Eine Verbindung mit dem WLAN-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.

Es gelten folgende Mindestanforderungen:

- Passwort- oder PIN-Schutz
- Installation eines Viren-/ Anti-Malwareschutzes
- aktuelle Firewall
- regelmässige Updates (Firewall, Betriebssystem, Virenschutz und Applikationen)
- Verschlüsselung sensitiver Daten bei der Speicherung und Übermittlung.

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

E-Mails und Termine können auf das BYOD synchronisiert werden. Für persönliche Geräte besteht kein Supportanspruch. Für Entsorgung und Reparatur von persönlichen Geräten sind die Benutzenden selbst zuständig.

V. Datenschutz

1. Generell

Die Benutzenden halten sich im schulischen Kontext an das geltende Kantonale Datenschutzrecht (siehe **Anhang I**) und seinen Bestimmungen, welche hier eingesehen werden können Link.

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

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 datenschutzrechtlicher 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 richten sich die Benutzenden an den Support.

b. Nutzung von Social Media

Der Einsatz von Social Media im schulischen Kontext (bspw. das Erstellen einer Facebook-Klassengruppe, eines YouTube-Kanals, etc.) liegt in der Zuständigkeit der Verantwortlichen Person für die Öffentlichkeitsarbeit an der ABZ oder der Schulleitung.

Ist der Einsatz von Social Media bewilligt, sind Kanäle, Gruppen, Benutzerzugänge, etc. zu löschen, sobald sie nicht mehr benötigt werden, spätestens jedoch sobald die jeweilige Lehrperson die Klasse nicht mehr betreut (siehe Anhang I Merkblätter)

c. Auswertungen über die Lernenden

Es ist nicht zulässig:

- umfassende Persönlichkeitsprofile über Lernende zu erstellen (bspw. **Lernprofile**);
- personenbezogenen Statistiken oder Auswertungen in der Klasse offenzulegen oder anderen Lehrpersonen, Eltern oder Schulmitarbeitenden bekanntzugeben.

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 die erhöhte Schutzstufe. Sie sind spätestens Ende Semester zu anonymisieren oder zu vernichten.

e. Bilder

Lernende dürfen nicht ohne deren 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/des betroffene/n Lernenden veröffentlicht oder Dritten bekanntgegeben werden. Es dürfen keine Porträts von Lernenden auf der Schulwebseite veröffentlicht werden.

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

VI. Urheberrechte

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, vervielfältigen, 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 Nutzer, 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. ausgenommen MS Teams und OneDrive.
    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 erhalten. Vor Erstellung eines Lehrmittels ist Rücksprache mit der [Schulleitung] zu nehmen.

2. Im Unterricht

a. Grundsatz

Im Unterricht dürfen urheberrechtlich geschützte Werke auf jegliche Art verwendet werden, das beinhaltet auch das Anfertigen von analogen oder digitalen Kopien (sog. Vervielfältigungen) von Werkausschnitten, nicht aber von ganzen Werken, die im Handel erhältlich sind. Lehrpersonen dürfen Werke für einzelne Klassen auf dem Intranet 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. Beim Bereitstellen solcher Kopien für mehrere Lehrpersonen aus Quellen, die nicht Radio- oder Fernsehsendungen sind, muss die Erlaubnis des Rechteinhabers eingeholt werden.

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

Für andere Lehrpersonen, für die ganze Schule oder öffentlich dürfen keine Zusammenstellungen von fremden Werkausschnitten verwendet werden.

g. Ausserhalb des Unterrichts

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

VII. 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, die anwendbaren gesetzlichen Bestimmungen.

Zwecks Feststellung von Missbrauchsvorfällen können Randdaten und sonstige Log-Files bzw. Protokolle ausgewertet und ein Personenbezug hergestellt werden.

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

Die Schule kann folgende Massnahmen ergreifen:

1. In der Regel erfolgt zuerst eine Abmahnung bzw. Verwarnung, bevor weitere Massnahmen ergriffen werden;

2. Bei Lernenden erfolgt je nach Schwere des Verstosses eine Meldung an die Inhaber der elterlichen Sorge, weitere Erziehungsberechtigte und den Ausbildungsbetrieb;
3. Vorfälle werden personenbezogen protokolliert und gespeichert;
4. Bei gravierenden oder wiederholten Verstössen kann die Schule direkt Disziplinarmassnahmen gemäss der anwendbaren Schulordnung bzw. dem anwendbaren Disziplinarreglement oder Personalrecht ergreifen.
5. Die Schule kann nebst Schadenersatz und, sofern rechtlich zulässig, die Wiederherstellung des ursprünglichen Zustands verlangen.
6. Stellt die Schule strafbares Verhalten fest, kann sie ohne Vorwarnung eine Strafanzeige einreichen bzw. eine Meldung bei der zuständigen Behörde vornehmen.

VIII. Ende der Benutzerrolle

Die Rolle als Benutzerin oder Benutzer der IKT-Systeme kann aus verschiedenen Gründen enden (Beendigung des Arbeitsverhältnisses, Ausschluss oder Absolvieren der Schule, Beendigung von Nutzungsvereinbarungen; nachfolgend «Austritt»).

Das Benutzerkonto erlischt nach Austritt aus der Schule. Die O365 Apps können noch bis zu 30 Tage nach Austritt weiter genutzt werden, die Lizenz läuft danach automatisch ab.

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.

IX. 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 (Allgemeine Informationssicherheitsrichtlinie) und anwendbaren BISR (Besondere Informationssicherheitsrichtlinie) [siehe AISR] entstehen.

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 für die kantonale Verwaltung vom 3. September 2019 Link
- Besondere Informationssicherheitsrichtlinien für die kantonale Verwaltung vom 17. Juni 2020, Inkrafttreten am 17. Juni 2022
- Richtlinien für die Informationsverwaltung an den kantonalen Mittel- und Berufsfachschulen sowie an den vom Kanton beauftragten Berufsfachschulen vom 4. April 2016 Link

Merkblätter

- Leitfaden Datenschutzlexikon Mittelschule und Berufsfachschule vom September 2020; Link
- Leitfaden Einsatz von mobilen Geräten in der Verwaltung vom März 2021; Link
- Leitfaden Bearbeiten im Auftrag vom April 2021; Link
- Social Media Guidelines 2014 des Kantons Zürich;
- Merkblatt Cloud Computing vom April 2021; Link
- Merkblatt Online-Speicherdienste vom November 2020; Link
- ProLitteris Merkblatt über den gemeinsamen Tarif 7: Schulische Nutzung vom 1. Januar 2017 Link
- ProLitteris Merkblatt über die gemeinsamen Tarife 8 und 9 (Reprografie/Netzwerke) vom 1. Januar 2017 Link

Glossare

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

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) 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.

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

Bekanntgeben: Das Zugänglichmachen von Informationen wie das Einsichtgewähren, 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 (L + Windowstaste) zu aktivieren.

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 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.

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 Unter-kategorien 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: Anwendung, mit deren Hilfe Zugangsdaten verschlüsselt gespeichert und verwaltet werden können.

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

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 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.

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, 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.

Anhang III – Netiquette

Die Schule ABZ 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 Schule 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.

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 Inhalten;
   e. keine Beiträge oder Kommentare mithilfe von Bots;
2. Ich verzichte auf namentliche Nennungen von schulischen Mitarbeitenden, Lehrpersonen 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 involvierten 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 Kontaktdaten 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 sonstigem Content den Social Media Anbieter ggf. zur beliebigen Nutzung der Bilder/des Contents 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, 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. Chatverläufe werden ggf. gespeichert, um Mobbingvorfälle und strafbare Handlungen aufzuklären;
5. Ich nehme keine Videokonferenzen mit dem Handy auf und kopiere – ausser bei berechtigtem Anlass gemäss Ziff. 3 – keine Chatverläufe;
6. Ich darf meine Videokamera im Rahmen von Aufnahmen jederzeit ausschalten oder meinen Hintergrund ausblenden und ich weise Lernende daraufhin, dass sie das dürfen;
7. Ich respektiere die Privatsphäre von Videokonferenzteilnehmern und fordere niemanden dazu auf, mir seine/ihre privaten Räumlichkeiten zu zeigen.