Nutzungsvereinbarung zum Gebrauch privater IKT-Systeme (Informations- und Kommunikationstechnologie) an der Gewerblichen Berufsschule Wetzikon

1. Allgemeine Bestimmungen

1.1 Zweck

An der GBW werden in verschiedenen Bereichen vom Kanton Zürich bereitgestellte oder private IKT-Systeme zur Arbeit eingesetzt.

Diese Richtlinie bezweckt, den Benutzenden verständliche und nachvollziehbare Vorgaben zum korrekten Umgang mit kantonalen IKT-Systemen zu geben. Diese Vorgaben regeln unter anderem Datensicherheit, Datenschutz und Umgang mit urheberrechtlich geschützten Werken im schulischen Kontext.

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.

1.3 Geltungsbereich

Diese Nutzungsrichtlinie gilt für Mitarbeitende, Lehrpersonen, Lernende, Studenten sowie Lernende (nachfolgend genannt «Benutzende»), die Zugang zu IKT-Systemen der Gewerblichen Berufsschule Wetzikon (nachfolgend genannt «Schule») 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 Verwendungszweck

Die IKT-Systeme und Anwendungen sind auf schulische oder institutionelle Zwecke ausgerichtet. Die Verwendung von IKT-Systemen und Anwendungen zu privaten Zwecken ist erlaubt, soweit sie sich auf ein verträgliches Mass beschränkt und den Lizenzbedingungen entspricht.

1.5 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.

2. Nutzung von IT-Arbeitsmitteln

An der Schule werden IT-Arbeitsmittel verwendet, die von der Schule bereitgestellt werden. Darüber hinaus werden BYOD-Geräte zur Nutzung an der Schule zugelassen.

Die nachfolgenden Regelungen 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.

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

2.2 Anwendungen
Auf den bereitgestellten Geräten dürfen - nach Beantragung bei und Bewilligung durch den IT-Verantwortlichen - lediglich die von der Schule bzw. vom Kanton freigegebenen Anwendungen installiert werden.

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

2.3 Supportorganisation
Für den Support sind der schulinterne Vor-Ort-Support und der Service Desk des Digitalen Service Center SekII zuständig. Die Kontaktangaben sind im Intranet auffindbar. Der schulinterne Vor-Ort-Support dient als erste Anlaufstelle.

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

Benutzerkonto
Erhält der/die Benutzende ein Benutzerkonto, dient dies für:

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

Passwortschutz
Die Benutzenden sind verpflichtet, für sämtliche Zugänge ein starkes Passwort zu wählen (siehe Passwortrichtlinien).

3.2 Schutz von Informationen
Mitarbeitende und Lehrpersonen unterstehen 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.

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.

Berechtigungen

Die Schule verfügt über ein Rollen- und Berechtigungskonzept, 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.

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 Informationsklassifizierung 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 Personendaten	Öffentlich	Intern	Vertraulich	Geheim	Grundschutz	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 (soweit nicht zur Veröffentlichung vorgesehen), etc.	Bspw. Zeugnisse, einzelne Noten, Lernprofile, Disziplinarmassnahmen, Angaben über die Gesundheit wie auch Quarantänemassnahmen, Religionszugehörigkeit, Massnahmen zum Nachteilsausgleich etc.	Hochsensible Informationen über Lernende, bspw. strafrechtliche Sanktionen, ärztliche Gutachten, Korrespondenz zum Nachteilsausgleich (Diagnosen)

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.

Sorgfaltspflichten

Es herrscht eine strikte Clean Desk und Clear Screen Policy (z.B. Bildschirmsperre mit Win-Taste +L und Passwort zum Entsperren bei Windows-Rechnern, Mac Tastenkombination [ctrl – cmd – Q]). 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 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.

3.2 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:

- Schutzsoftware darf nicht umgangen oder deaktiviert werden.
- Es müssen immer sämtliche offiziellen Aktualisierungen und Updates installiert werden, insbesondere die des Virenschutzes.
- 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.
- 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.
- Es dürfen keine Anhänge, die von unbekannten oder verdächtigen Absendern stammen, geöffnet werden.
- Generell dürfen Werbungen oder Pop-Ups in Nachrichten oder im Internet nicht angeklickt werden, bei externen Links ist Zurückhaltung geboten.
- Es dürfen keine fremden, nicht autorisierten bzw. bewilligten Wechselmedien an die IT-Infrastruktur der Schule angeschlossen werden.
- Auffälligkeiten und konkrete Verdachte müssen umgehend gemeldet werden.

3.3 Schutz von Kommunikation

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

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

– Die Benutzenden sind für die Kontrolle und Pflege ihres Postfachs verantwortlich.
– Auf E-Mails ist an Werktagen innerhalb von 48 Stunden zu reagieren.
– Vertraulich und höher klassifizierte Nachrichten müssen verschlüsselt und signiert versendet werden.
– E-Mails können nicht an externe (private oder geschäftliche) Postfächer weiter- oder umgeleitet werden.
– Das E-Mail-Konto darf nicht zum Versand oder zur Verbreitung von rechtswidrigen Inhalten benutzt werden.
– Die E-Mailadresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshopping, etc.) genutzt werden.

Collaboration Tools

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

– Die Benutzenden verwenden Collaboration Tools für die schulinterne Kommunikation.
– Die Anzahl neuer Kanäle ist auf das Nötige zu limitieren;
– Der bzw. 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;
– 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.

3.4 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:

– Up- und Downloads von umfangreichen, nicht unterrichts- oder schulbezogenen Dateien sind verboten.
– Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden.
– Auf dem Schulareal sind Zugriffe per Hotspots verboten.
– Der Besuch des Darknets ist verboten.
– 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.
– Während des Unterrichts ist der Besuch von Social Media und sonstige Unterhaltungsseiten verboten, ausser dies gehört zum Unterrichtsstoff;
– Schulinterne, administrative Informationen dürfen nur in Absprache mit der Schulleitung ins Internet hochgeladen werden, z.B. um Übersetzungen in Gratistools zu erwirken.

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.

3.5 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.
– Ein Zugang mit Benutzername und Passwort auf das schulinterne Netz ist möglich.
– 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.

3.6 Meldepflicht

Sicherheitsvorfälle, der Verlust bzw. Defekt von IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem schulinternen Vor-Ort-Support / IT-Verantwortlichen 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.
Bei mobilen Arbeitsgeräten (z.B. Laptops) sind zusätzliche Mindestanforderungen nötig

– Installation eines Virenschutzes
– aktuelle Firewall
– aktuelles Betriebssystem

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

4.2 Support

Für persönliche Geräte besteht kein Supportanspruch. Für fachgerechte Entsorgung (u.a. korrekte Datenlöschung) und Reparatur von persönlichen Geräten sind die Benutzenden selbst zuständig.

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 den/die Datenschutzverantwortliche/-n der Schule zu.

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).

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 IKT-Support.

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.

Besondere Personendaten
Schriftliche Aufzeichnungen (Aufsätze, 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 Ausbildung zu anonymisieren oder zu vernichten. Die Rekursfristen sind einzuhalten.

Bilder
Lernende 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.

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. Ebenso dürfen ohne explizite Einwilligung keine Porträts von Lernenden, Lehrpersonen oder Mitarbeitenden auf der öffentlich zugänglichen Schulwebseite veröffentlicht werden.

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 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 erhalten. Vor Erstellung eines Lehrmittels ist Rücksprache mit der Schulleitung zu nehmen.

6.2 Im Unterricht

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 zugänglich machen. Von der erlaubten Vervielfältigung nicht erfasst ist das Kopieren von Computerprogrammen sowie das Aufzeichnen von Vorträgen, Bühnenaufführungen und Konzerten.

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.

Bilder

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

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.

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

Urheberrecht der Schule

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 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.

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 75 Tage nach Austritt aus der Schule.
- 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.

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.

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 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 2017-2022 Archiv Link
- ProLitteris Tarif 7 Gültigkeit 2022-2026; Link
- Pro Litteris Merkblatt Schulen (GT 7), Link

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.