Allgemeine Nutzungsrichtlinie der Kantonsschule Wiedikon

Inhaltsverzeichnis

Die Schulleitung, gestützt auf die Bestimmungen des Mittelschulgesetzes vom 13. Juni 1999, des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 und weiterer Verordnungen und Richtlinien des Kantons Zürich (siehe Anhang), beschliesst:

I. Allgemeine Bestimmungen

1. Zweck

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

Diese Richtlinie bezweckt, den Nutzer:innen verständliche und nachvollziehbare Vorgaben zum korrekten Umgang mit kantonalen IKT-Systemen zu geben. Diese Vorgaben regeln die Datensicherheit und den Datenschutz 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.

2. Grundlagen

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

3. Geltungsbereich

Diese Nutzungsrichtlinie gilt für Mitarbeitende, Lehrpersonen, Lernende, Praktikanten, Studenten und Schüler:innen (nachfolgend als «Nutzer:innen» bezeichnet), die Zugang zu IKT-Systemen der Kantonsschule Wiedikon (nachfolgend «Schule» genannt) haben. Personen, die nur für kurze Zeit an der Kantonsschule Wiedikon tätig sind (Praktikanten, Studenten), erhalten keinen persönlichen Zugang zu den IKT-Systemen der Schule. Die Nutzer:innen sind selbst dafür verantwortlich, diese Richtlinie einzuhalten.

Mit dem ersten Login oder der Nutzung der zur Verfügung gestellten IT-Infrastruktur nehmen die Nutzer:innen die Nutzungsrichtlinie zur Kenntnis 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 sind in einem Glossar auffindbar, das auf der Webseite der Schule abgerufen werden kann.

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 Nutzer:innen.

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

Die Verwendung von IKT-Systemen und Anwendungen für Mining und andere ressourcenintensive private Tätigkeiten ist verboten.

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

6. Auswertungen von Randdaten

Bei der Nutzung der IT-Systeme fallen Randdaten wie zum Beispiel Logfiles an. Zur Erkennung und Rückverfolgung von Sicherheitsvorfällen können die Schule und der Kanton Zürich innert der gesetzlichen Frist auf diese Randdaten zurückgreifen.

II. Nutzung von IT-Arbeitsmitteln

An der Schule werden IT-Arbeitsmittel verwendet, die von der Schule bereitgestellt bzw. verwaltet werden. Darüber hinaus werden BYOD-Geräte gemäss Ziff. IV 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 II.1 bis II.4 betreffen IT-Arbeitsmittel, die den Nutzer:innen von der Schule zur Verfügung gestellt werden (d.h. nicht BYOD-Geräte).

Die Schule kann für die Nutzung der Computerräume und der IT-Arbeitsmittel, die die Schule zur Verfügung stellt, besondere Vorschriften und Anleitungen erlassen. Die Nutzer:innen behandeln die IT-Arbeitsmittel mit Sorgfalt und schützten sie vor Diebstahl und Beschädigung. Räume, die IT-Arbeitsmittel enthalten, sind beim Verlassen abzuschliessen.

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. 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.

3. Supportorganisation

Für den Support ist der schulinterne Vor-Ort-Support zuständig. Die Kontaktangaben sind in der Webseite der Schule (www.kwi.ch) auffindbar. Anleitungen und andere Hilfestellungen für die Nutzung der IT-Dienste (z.B. WLAN) sind ebenfalls dort abrufbar.

4. Entsorgung

Für die Entsorgung ausgedienter bzw. defekter IT-Arbeitsmittel der Schule oder für deren Reparatur bzw. Austausch ist der schulinterne IT-Support zuständig. Der schulinterne IT-Support unterstützt die Lehrpersonen und Mitarbeiter/Mitarbeiterinnen auch bei der Entsorgung persönlicher Geräte, wenn diese für schulische Zwecke benutzt wurden.

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 betroffene Nutzer:in umgehend eine Meldung bei der zuständigen Supportorganisation vornehmen.

a. Benutzerkonto

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

Das Benutzerkonto ist persönlich und nicht übertragbar. Es darf keiner anderen Person Zugang zum eigenen Benutzerkonto verschafft werden. Die Nutzer:innen 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 Nutzer:innen sperren ihr IT-Arbeitsmittel bei einem zeitweiligen Verlassen und melden sich von allen Systemen ordnungsgemäss ab, wenn sie eine Arbeitsstation der Schule definitiv verlassen.

b. Passwortschutz

Die Nutzer:innen sind verpflichtet, für alle Zugänge (Intranet Sek II, Microsoft 365) ein persönliches Passwort zu wählen, das die Vorgaben des Kantons erfüllt. Diese Vorgaben können im Intranet Sek II im persönlichen Profil eingesehen werden.

Für jeden Zugang ist ein separates, einzigartiges Passwort zu wählen. Das Passwort muss regelmässig geändert werden, für Änderungen steht im Intranet Sek II ein Online-Formular zur Verfügung (im persönlichen Profil des Nutzers / der Nutzerin). Die für die Zugänge der Schule gewählten Passwörter dürfen nicht für private Zwecke verwendet werden.

Die Schule kann zur Erhöhung der Sicherheit verlangen, dass die Nutzer:innen bei der Anmeldung an ihren Diensten (Intranet Sek II, Microsoft 365) zusätzliche Mittel wie die Multi-Faktor-Authentifizierung mittels Smartphone einsetzen.

2. Schutz von Informationen

Mitarbeitende und Lehrpersonen unterstehen dem Amtsgeheimnis. Sie müssen Vorsichtsmassnahmen 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, administrativen oder personenbezogenen Informationen (betr. nicht Unterrichtsmaterialien) müssen auf den von der Schule bzw. dem Kanton bereitgestellten Datenablagen (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.

b. Berechtigungen

Die Nutzer:innen dürfen nur jene Daten öffnen bzw. verwenden, zu deren Nutzung sie berechtigt ist. Erhält ein / eine Nutzer: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 (Sachdaten, Personendaten, besondere Personendaten) und klassifiziert (öffentlich, intern, vertraulich, geheim) werden. Die Schule kann für den Umgang mit Informationen besondere Vorschriften erlassen.

d. Bekanntgabe von Informationen

Schulinterne Informationen dürfen nur gestützt auf eine Rechtsgrundlage oder mit der Einwilligung der betroffenen Person weitergegeben werden. In Zweifelsfällen entscheidet die Schulleitung.

e. Sorgfaltspflichten

Die Nutzer:innen müssen ihre Arbeitsplätze so zurücklassen, dass andere Personen nicht in den Besitz von Informationen und Daten gelangen können, zu deren Kenntnis und Verwendung sie nicht berechtigt sind. Störungen oder Defekte an den 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.

3. Schutz vor Malware

Die Nutzer:innen müssen IT-Arbeitsmittel, die sie im Schulumfeld benutzen, mit Schutzsoftware ausstatten bzw. die geräteeigenen Sicherheitsmittel aktivieren (Firewalls, Gateways, Antivirusprogramme). Zusätzlich sind sie gehalten, folgende ergänzende Schutzvorschriften bei der Bearbeitung von und im Umgang mit schulinternen Daten, Informationen und Dokumenten zu berücksichtigen:

1. Die Sicherheitsmittel der eigenen IT-Arbeitsmittel dürfen nicht umgangen oder deaktiviert werden.
2. Die Nutzer:innen müssen Aktualisierungen und Updates der Hersteller möglichst zeitnah auf ihren eigenen Geräten installieren. Dies gilt in erhöhtem Mass, wenn sie sicherheitsrelevant sind.
3. Verdächtige E-Mails müssen umgehend gelöscht werden. Auf keinen Fall dürfen Anhänge, die von unbekannten bzw. verdächtigen Absendern stammen, geöffnet werden, bei externen Links unklarer oder zweifelhafter Herkunft ist grösste Vorsicht und Zurückhaltung geboten. Bei einer Häufung solcher Fälle muss eine Meldung an den IT-Support der Schule erfolgen. Auch bei verdächtiger Werbung im Internet wird zu grosser Vorsicht geraten.
4. Es dürfen nur eigene, persönliche Medien und Geräte von Angehörigen der Schule an die IT-Infrastruktur der Schule angeschlossen werden.
5. Die Nutzer:innen müssen Auffälligkeiten und konkrete Verdachtsfälle umgehend dem IT-Support der Schule melden.

4. Schutz von Kommunikation

a. E-Mail

Die Nutzer:innen erhalten während ihrer Tätigkeit an der KWI ein eigenes E-Mail-Konto mit einer E-Mailadresse der Schule. Das E-Mail-Konto dient insbesondere für Korrespondenz im Zusammenhang mit dem Schulbetrieb.

Im Zusammenhang mit der Nutzung der E-Mail-Infrastruktur der Schule gelten folgende Vorgaben:

1. Die Nutzer:innen sind für die Kontrolle und Pflege ihres Postfachs verantwortlich.
2. Vertrauliche bzw. höher klassifizierte Nachrichten müssen verschlüsselt versendet werden.
3. E-Mails dürfen nicht an eigene externe Postfächer weitergeleitet werden.
4. Die Nutzer:innen dürfen ihr E-Mail-Konto oder andere Kommunikationsmittel der Schule (siehe unten b) nicht zum Versand oder zur Verbreitung von beleidigenden, persönlichkeitsverletzenden, rassistischen, sexistischen oder pornographischen Inhalten oder zur Planung, Vorbereitung, Organisation und Durchführung von Verbrechen und Vergehen benutzen.

b. Collaboration Tools

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

1. Die Nutzer:innen verwenden Collaboration Tools für die schulinterne Kommunikation.
2. Der bzw. die Betreibende eines Kanals ist für die spezifischen Berechtigungen verantwortlich und sorgt dafür, dass der Informationsaustausch auf das Notwendige beschränkt und dass die Vorgaben des Leitbilds und des Verhaltenskodexes der Schule auch im Chat eingehalten werden.
3. Vertrauliche oder höher klassifizierte Informationen dürfen nur End-zu-End verschlüsselt ausgetauscht werden, egal ob im Chat oder im Videoanruf.
4. Chats und Social Media-Kanäle sind dazu bestimmt, sich auszutauschen. Vertrauliche und höher klassifizierte Daten und Dokumente dürfen nicht dort, sondern müssen in die von der Schule dafür bestimmten Speicher abgelegt und in den Chats und Social Media nur referenziert / verlinkt werden.

5. Netzwerk- und Internetnutzung

Das Schulnetzwerk steht den Nutzer:innen im Rahmen der kantonalen Infrastruktur (LEUnet) für die persönliche Nutzung zur Verfügung. Sämtliche Netzzugriffe werden aufgrund gesetzlicher Vorschriften automatisch protokolliert. Die Protokolldaten können im begründeten Verdachtsfall personenbezogen ausgewertet werden. Die Nutzer/innen werden im konkreten Fall informiert, sofern eine Rückverfolgbarkeit möglich ist.

Im Zusammenhang mit der Nutzung des Schulnetzwerks gelten folgende Vorgaben:

1. Up- und Downloads von grossen Dateien sind nur für schulische Zwecke zulässig.
2. Die Nutzung des Internets muss mit der gebührenden Vorsicht erfolgen. Die Nutzung des Darknets und der Besuch von Webseiten oder anderer Angebote im Internet mit verbotenen bzw. anstössigen Inhalten (zum Beispiel pornografische, sexistische, rassistische oder gewaltverherrlichende Äusserungen bzw. Darstellungen) ist verboten.
3. Während des Unterrichts ist der Besuch von Social Media und sonstigen Unterhaltungsseiten verboten, ausser dies gehört zum Unterricht.
4. Schulinterne Dokumente, Daten und Informationen dürfen ohne Zustimmung der Schulleitung nicht in externen Internet-Tools verwendet oder gespeichert werden.

IV. Persönliche Geräte

1. Grundsatz

Das Mitführen von persönlichen mobilen Geräten an der Schule ist grundsätzlich erlaubt, eine Verbindung mit dem Schulnetzwerk ist für Angehörige der Schule zulässig. Persönliche mobile Geräte sind mobile Arbeitsgeräte wie Laptops/Notebooks.

Für kurzzeitig unterrichtende Lehrpersonen, Praktikanten, Studenten und andere Personen, die nicht der Schule angehören, steht im Rahmen der vom Kanton zur Verfügung gestellten Infrastruktur (LEUnet) ein Gastzugang zur Verfügung.

Für persönliche Geräte besteht kein Supportanspruch. Die Nutzer:innen sind selbst für die fachgerechte Entsorgung und für die Reparatur von persönlichen Geräten zuständig.

Die Schule ist berechtigt, von den Nutzer:innen einen Nachweis betreffend die Einhaltung der folgenden Anforderungen einzuholen.

2. Geräteanforderungen

Es gelten folgende Mindestanforderungen:

- Personalisiertes Login (z.B. Passwort, PIN, Fingerabdruck, Gesichtserkennung).
- Angemessene Sicherheitsvorkehrungen gegen eine Manipulation durch Malware: Installation eines Virenschutzes und einer Firewall oder Aktivierung, falls sie auf dem persönlichen Gerät schon vorinstalliert sind (z.B. Windows Defender).
- Regelmässiges Aktualisieren (Updates) des Betriebssystems, des Virenschutzes und anderer, auf dem persönlichen Gerät installierter Anwendungen.

3. Datenspeicherung

Lehrpersonen und Mitarbeiter / Mitarbeiterinnen können schulinterne Daten und Informationen auf ihrem persönlichen Gerät speichern und E-Mails bzw. Termine synchronisieren, sofern das Gerät den Vorgaben und Anforderungen der Schule und des Kantons genügt.

Lehrpersonen und Mitarbeitern / Mitarbeiterinnen wird dringend empfohlen, die Datenspeicher ihrer persönlichen Geräte und auch externe Datenspeicher zu verschlüsseln, wenn sie diese für schulische Zwecke einsetzen. Eine Verschlüsselung ist zwingend, wenn sensitive Daten (z.B. besondere Personendaten wie Noten oder Disziplinarmassnahmen) gespeichert werden.

Lehrpersonen und Mitarbeiter / Mitarbeiterinnen müssen alle schulinternen Daten löschen, die sie auf ihren personlichen Geräten oder externen Datenspeicher gespeichert haben, bevor sie diese entsorgen oder an Dritte übergeben. Die Schule empfiehlt Lehrpersonen und Mitarbeitern / Mitarbeiterinnen, ausgediente oder defekte Datenspeichern, die schulinterne Daten und Informationen enthalten, dem IT-Support der KWI zur Entsorgung zu übergeben.

5. BYOD

Die Nutzung persönlicher Geräte im Unterricht durch Schüler:innen erfolgt in Absprache mit der Lehrperson. Die Schule behält sich vor, die Nutzung im Unterricht nur zuzulassen, wenn die Geräte den kantonalen oder schulischen Vorgaben entsprechen.
Für den Einsatz von persönlichen Geräten der Schüler:innen im Unterricht und für Prüfungen (BYOD) kann die Schule weitere Vorgaben und Weisungen erlassen.

V. Datenschutz

1. Generell

Die Nutzer:innen halten sich im schulischen Kontext an das geltende Datenschutzrecht.

Wenn eine betroffene Person Rechte aus dem Datenschutzrecht geltend macht, zum Beispiel ein Auskunfts-, Berichtigungs- oder Löschgesuch, dann muss sie das Gesuch an die Schulleitung stellen.

2. Im Unterricht

Lehrpersonen sind für den Schutz der Persönlichkeit der Lernenden während des Unterrichts verantwortlich, dazu gehört auch der Datenschutz gemäss den aktuellen rechtlichen Vorgaben, siehe das Datenschutzlexikon für die Mittelschule des Kantons Zürich (datenschutz.ch/lexika).

Auch für die im Unterricht verwendeten Anwendungen müssen die datenschutzrechtlichen Vorgaben eingehalten werden (Speicherort, Aufbewahrungsdauer, Möglichkeit der endgültigen Löschung, technische Massnahmen wie Verschlüsselung, etc.). Im Zweifelsfall richtet sich die Lehrperson an den IT-Support oder an die Schulleitung.

a. 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 zulässig. Inhalte, die nicht mehr benötigt werden, müssen gelöscht werden. Es ist nicht zulässig, Ergebnisse und Auswertungen aus dem Einsatz solcher Medien zu veröffentlichen. Die Schule kann weitere Vorgaben für den Einsatz von digitalen bzw. Online-Medien erlassen.

b. Besondere Personendaten

Dokumente mit besonderen Personendaten (z.B. in Aufsätzen und anderen schriftlichen Arbeiten oder in Bild-, Ton- oder Videoaufnahmen) müssen mit der notwendigen Sorgfalt und Vertraulichkeit behandelt werden, für sie gilt eine erhöhte Schutzstufe. Sie sind spätestens mit dem Austritt des Urhebers / der Urheberin aus der Schule zu anonymisieren oder zu vernichten.

c. 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.

d. Bekanntgabe

Es dürfen keine schriftlichen Aufzeichnungen, grafischen 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.

Bei Schüler:innen unter 14 Jahren ist die Zustimmung der Eltern einzuholen.

VI. Massnahmen bei Verstössen

Bei einer missbräuchlichen Nutzung der IT-Systeme inkl. Urheberrechtsverletzungen drohen den Nutzer:innen 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 Feststellung von Missbrauchsvorfällen können Randdaten und sonstige Log-Files bzw. Protokolle ausgewertet und ein Personenbezug hergestellt werden. Werden Missbräuche und Verstösse erkannt, sollte immer zuerst das Gespräch gesucht werden. Bevor die Schule entscheidet, ob sie Disziplinarmassnahmen ergreift, wird den Nutzer:innen die Möglichkeit zur Äusserung gegeben.

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

VII. Ende der Benutzerrolle

Die Rolle als Nutzer:in der IKT-Systeme endet bei der Beendigung des Arbeitsverhältnisses (Mitarbeitende und Lehrpersonen) bzw. beim Austritt aus der Schule (Schüler:innen). Das Benutzerkonto wird danach vom Kanton deaktiviert.

Persönliche Daten sind vor dem Verlassen der Schule auf eigene Speichermedien oder Cloudspeicher zu übertragen.

Spätestens am Tag des Austritts sind sämtliche IT-Arbeitsmittel an den IT-Support der KWI zurückzugeben.

Anwendungen, die von der Schule lizenziert sind, und Zugänge (Logins) zum Schulnetzwerk müssen von den persönlichen Geräten gelöscht werden.

Lehrpersonen und Mitarbeitende müssen bei der Beendigung ihrer Anstellung alle vertraulichen schulinternen Daten löschen, die auf ihren Geräten gespeichert sind.

VIII. 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 Nutzer:innen aus ihrer Missachtung dieser Nutzungsrichtlinie und des anwendbaren Rechts (Datenschutz, Informationssicherheit) entstehen.

Anhang – 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 Mittelschulen vom 2. Februar 2015 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 März 2021; Link
- Leitfaden Bearbeiten im Auftrag vom April 2021; Link
- Social Media Guidelines 2014 des Kantons Zürich; Link
- Merkblatt Cloud Computing vom April 2021; Link
- Merkblatt Online-Speicherdienste vom November 2020; Link
- Merkblatt Passwortmanager vom Juli 2021; Link
- ProLitteris Merkblatt über die gemeinsamen Tarife 8 und 9 (Reprografie/Netzwerke) vom 1. Januar 2017 Link
- ProLitteris Tarif 7 Gültigkeit 2022-2026; Link

Glossare

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

Suche nach Datenschutz-Dokumenten im Kanton Zürich: Link