Liebe Schulvertreter

Um die Schulen in den Bereichen Datenschutz und Datensicherheit bestmöglich zu unterstützen, hat das Digital Service Center Sek II eine Vorlage für eine Nutzungsrichtlinie erarbeitet. Die Arbeiten wurden im Projekt «Digitaler Wandel an den kantonalen Schulen Sek II (DiWaSekII)» angestossen. Die Vorlage soll Sie im Hinblick auf die Erstellung der Nutzungsrichtlinie für Ihre Schule unterstützen.

Die Nutzungsrichtlinie NRL wendet sich an Schülerinnen und Schüler, Lehrpersonen und Mitarbeitende. Sie gibt vor, wie diese sich verhalten sollen bei der Verwendung von kantonalen Informatikmitteln und persönlichen Geräten (BYOD). Sie versteht sich also als Weisung zum korrekten Verhalten der Benutzer.

Im Folgenden finden Sie die einzelnen Abschnitte der NRL und Hinweise dazu, wie diese auf Ihren Bedarf hin angepasst werden können. Darunter fällt die mögliche Anpassung für die Zielgruppen Mitarbeitende, Lehrpersonen und Lernende.

Hinweis: Basis hier ist die Allgemeine NRL (ANRL). Die Vorlage des MBA ist auf die schulische Situation und ihre individuelle Formatierung (Logo, Schriften) anzupassen.

Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Bettina Irnhauser

Verantwortliche Informationssicherheit und Datenschutz Sek II
Ausstellungsstrasse 80
8090 Zürich
bettina.irnhauser@mba.zh.ch
www.zh.ch/mba

**Präambel**

Die vorliegenden Nutzungsrichtlinien (Version 0.96) stellen ein Angebot und keine Verpflichtung des DSC SekII (Digital Service Center SekII) an die Schulen dar. Es gibt gute Gründe (z.B. fehlende, einfache technische Umsetzung oder andere Priorisierungen), an den Schulen anderslautende Bestimmungen zu erlassen, die dem jeweiligen Schulalltag besser gerecht werden, sofern mit diesen abweichenden Bestimmungen nicht übergeordnete, zwingend verbindliche Rechtsnormen verletzt werden.

Inhaltsverzeichnis

[I. Allgemeine Bestimmungen 4](#_Toc163118162)

[Wie dieses Dokument zu lesen ist 4](#_Toc163118163)

[Wie die Nutzungsrichtlinie in den Unterrichtsalltag eingebunden wird 4](#_Toc163118164)

[Zu 2. Grundlagen 5](#_Toc163118165)

[Zu 5. Verwendungszweck 5](#_Toc163118166)

[Zu 6. Auswertungen von Randdaten 5](#_Toc163118167)

[II. Nutzung von IT-Arbeitsmitteln 6](#_Toc163118168)

[Zu 1. Änderungen 6](#_Toc163118169)

[Zu 2. Anwendungen 6](#_Toc163118170)

[Zu 3. Supportorganisation 6](#_Toc163118171)

[Zu 4. Weitere Hilfestellungen 7](#_Toc163118172)

[III. Datensicherheit 7](#_Toc163118173)

[Zu 1. Schutz von Zugangsdaten 7](#_Toc163118174)

[Zu 2. Schutz von Informationen 8](#_Toc163118175)

[Zu 3. Schutz vor Malware 10](#_Toc163118176)

[Zu 4.a Schutz von Kommunikation 10](#_Toc163118177)

[Zu 4.b Collaboration Tools 11](#_Toc163118178)

[Zu 5. Netzwerk und Internetnutzung 11](#_Toc163118179)

[Zu 6. Arbeiten von unterwegs oder zu Hause 11](#_Toc163118180)

[IV. Persönliche Geräte /BYOD 12](#_Toc163118181)

[Zu 5. Onlineprüfungen 13](#_Toc163118182)

[V. Datenschutz 14](#_Toc163118183)

[Zu 1. Generell 14](#_Toc163118184)

[Zu 2. Im Unterricht 14](#_Toc163118185)

[VI. Urheberrechte 18](#_Toc163118186)

[Zu 2. Im Unterricht 18](#_Toc163118187)

[VII. Massnahmen bei Verstössen 20](#_Toc163118188)

[VIII. Ende der Benutzerrolle 21](#_Toc163118189)

[IX. Anhänge 21](#_Toc163118190)

# Allgemeine Bestimmungen

## Wie dieses Dokument zu lesen ist

Hinweis zum Color Coding im Dokument:

* Gelb – Diese Einträge betreffen Schulinformation oder Angebote der Schule. Hier kann die Schule gemäss Hausrecht wählen oder eigene Angaben machen.
* Türkis –Hier besteht ein Wahlrecht mit Optionen, also wird entweder Option 1 oder 2 gewählt – oder, wenn nur eine 1 verfügbar ist, 1 oder keins.

Wo gesetzliche oder kantonale Vorgaben bestehen, werden keine Optionen angeboten.

Des Weiteren können die Abschnitte gekürzt / zugeschnitten werden auf jene Zielgruppe, die sie betreffen:

* Alle bedeutet, dass der Text für alle Zielgruppen relevant ist, also für Mitarbeitende, Lehrpersonen und Lernende
* MA meint, dass der Absatz relevant ist für Mitarbeitende
* LP bedeutet, der Absatz ist relevant für Lehrpersonen
* S meint, dass der Absatz relevant ist für Schülerinnen, Schüler und Studierende bzw. Lernende

Diese Farb-Codierungen können genutzt werden, wenn die Schule zielgruppenspezifische Nutzungsrichtlinien erstellt. Sie sind als Vorschläge zu verstehen, selbstverständlich können die Zuordnungen anders entschieden werden.

Die Begriffe Schülerinnen und Schüler, Studierende, Lernende kann die Schule jeweils für sich festlegen. Wir führen hier der Einfachheit halber Lernende auf.

Im folgenden Verlauf werden entweder Hinweise zur Auswahl erteilt oder die dahinterstehende gesetzliche Erwägung beschrieben.

Die gesamte Nutzungsrichtlinie versteht sich als Angebot. 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.

## Wie die Nutzungsrichtlinie in den Unterrichtsalltag eingebunden wird

Mittel- und Berufsfachschulen sind in der Regel unselbstständige kantonale Anstalten. Im Rahmen ihrer Autonomie können Mittel- und Berufsfachschulen ihre Hausordnung und weitere schulinterne Verordnungen erlassen. Diese Kompetenz wird dort beschränkt, wo das Mittelschulgesetz und das Einführungsgesetz zur Berufsbildung sowie deren Verordnungen gewisse Themen einem spezifischen schulübergreifenden oder kantonalen Entscheidungsgremium überlassen.

Die Schule stellt im Rahmen ihrer Autonomie Regelungen zum Benützungsverhältnis auf und sorgt für einen geordneten Schulbetrieb. Dazu gehört auch die Benutzung der Anstaltseinrichtung wie die Informatikinfrastruktur, was keinem schulübergreifenden Gremium vorbehalten wurde.

Errichtet die Schule also Weisungen zur Benutzung ihrer Informatikinfrastruktur, handelt es sich dabei nicht um einen Vertrag, den die Lernenden oder die weiteren Benutzenden akzeptieren müssen (wie bspw. Nutzungsbedingungen), sondern muss lediglich zur Kenntnis genommen werden. Akzeptieren Benutzende die Nutzungsrichtlinie nicht, hat das keine Folgen für deren Wirksamkeit. Wir empfehlen deshalb eine Einbindung der Nutzungsrichtlinie, bspw. beim erstmaligen Login durch den Benutzer, wie folgt:

*“Ich bestätige, die Nutzungsrichtlinie gelesen und verstanden zu haben”.*

## Zu 2. Grundlagen

Hier gilt es Treffendes auszuwählen, die weitere Formulierungsvorschläge sind zu löschen.

Hinweis 2a: Dies sind Kantonsschulen, Berufsfachschulen

Hinweis 2b: Es ist möglich, dass einige Schulen selbständige kantonale Anstalten sind.

## Zu 5. Verwendungszweck

Geschäftliche Lizenzen von Microsoft 365 EDU können neben der geschäftlichen Verwendung auf weiteren Geräten eingesetzt werden. Auf 5 Desktop-Computern, 5 Tablets und 5 Smartphones (insgesamt also 15 Geräte). Eine Nutzung für kommerzielle Zwecke ist untersagt.

## Zu 6. Auswertungen von Randdaten

Hinweis zum Verständnis: Es wird angekündigt werden, wenn es zu Auswertungen kommt: «Es wurden Irregularitäten festgestellt, ab jetzt werten wir den Zugriff auf Webseiten/ Internet-Verhalten aus.» Das genaue Vorgehen bei Sicherheitsvorfällen ist in BISR 24 Seite 4 beschrieben.

Getrackt wird die Verwendung von Anwenderdaten, auch die Fremdverwendung der Benutzerkonten, sowie der Verbrauch grosser Ressourcen (Downloads, Mining, anderes). Beide können ad-hoc ausgewertet werden. Diese Auswertungen ermöglichen es den Schulen, disziplinarische oder strafrechtliche Massnahmen einzuleiten.

Randdaten werden so lange aufbewahrt, wie die gesetzlichen Fristen / Aktenfristen der Daten sind, auf die sie sich beziehen.

Weitere Details kommen in die Datenschutzerklärung.

# Nutzung von IT-Arbeitsmitteln

Hinweis **kommerzielle** Zwecke: Der Rahmenvertrag mit EDUCA, unter den die Anwendungen M365 laufen, lässt keinen kommerziellen Einsatz der Anwendungen zu. Schulen, die noch nicht im EDUCA-Vertrag eingebunden sind, können nach Rücksprache mit dem Anbieter eine Nutzung für kommerzielle Zwecke zulassen.

Hinweis **IT-Arbeitsmittel**: Wenn im folgenden IT-Arbeitsmittel genannt sind, handelt es sich immer um kantonale IT-Arbeitsmittel (im Gegensatz zu privaten Geräten BYOD, welche explizit genannt werden).

## Zu 1. Änderungen

Für Schulen, die ihre Konfiguration vom MBA beziehen, wird über das Benutzerprofil sichergestellt, dass nur zulässige Änderungen vorgenommen werden können. Handelt die Schule dieser Vorgabe zuwider und umgeht die Voreinstellungen des MBA, so kann daraus der Verlust des Support-Anspruches resultieren.

Schulen, die über andere Provider die Anwendungen beziehen, können hier den Satz stehen lassen, soweit ihr Service Desk die Dienstleistung bietet.

## Zu 2. Anwendungen

Falls eine Schule die Anwendungen selbst administriert oder eine entsprechende Erweiterung der Dienstleistungen des MBA bezieht, können hier Fremdanwendungen akzeptiert werden. Falls nicht, kann der Absatz gelöscht werden.

Hinweis Nutzungsvorgaben und Anleitungen: diese können im Internet unter dem Service Desk der MBA per <https://help.mba.zh.ch> abgerufen werden.

## Zu 3. Supportorganisation

Der vorgeschlagene Text geht vom momentanen Stand der Planung aus. Weitere Details werden durch die Umsetzung des Projekts «Digitaler Wandel Schulen Sek II» und das Digital Service Center (DSC) Sek II erarbeitet und bekannt gegeben.

Da wir gegenwärtig die konkrete zukünftige Organisation noch nicht kennen (bzw. sie nicht verabschiedet und implementiert ist), können wir weiterhin von einem Erstkontakt in der Schule ausgehen, der Themen weiterleitet, entweder an einen schulinternen IT-Verantwortlichen oder den Digital Service Center Sek II Service Desk.

In diesem Kapitel können die schulinternen Kontaktdaten und der Link auf die Service Desk Tools (DSC: https://help.mba.zh.ch und für Schulen mit IKT-Grundversorgung: https://serviceportal.zh.ch) publiziert werden.

## Zu 4. Weitere Hilfestellungen

Hilfestellungen können im Internet unter dem Service Desk der MBA per <https://help.mba.zh.ch> abgerufen werden.

# Datensicherheit

## Zu 1. Schutz von Zugangsdaten

Die Anforderungen an die **Passwortvergabe für System-Zugänge** ist in der BISR10 beschrieben. Es sind von Lehrpersonen Mitarbeitenden und Lernenden 12 Zeichen erforderlich.

Hinweis1 **Zwei-Faktor-Authentifizierung**: Falls die Schule über diesen Service verfügt, bitte diesen Passus hier stehen lassen, ansonsten löschen (1 oder keins).
Hinweis: Die Zwei-Faktor-Authentifizierung ist aus Datenschutzgründen generell zu empfehlen.

Hinweis2: **Zwei-Faktor-Authentifizierung** ist zu verwenden, wenn sich Benutzer von ausserhalb in das Schul-Netz einwählen. Es ist ggf. nicht nötig, wenn die Benutzer sich im technischen Empfangsbereich aufhalten (im [W]LAN sind).

Hinweis: **starkes Passwort und Passwort-Safe**: Hier Zutreffendes stehen lassen, sonst bitte löschen.

Hinweis aus dem **BISR 10**:

Passwörter und alphanumerische PIN-Codes müssen entweder

1. mindestens 12 Zeichen lang sein und aus vier Zeichenarten bestehen
2. mindestens 24 Zeichen lang sein und aus zwei Zeichenarten bestehen

Die Zeichenarten sind wie folgt kategorisiert:

1. Grossbuchstaben (A, B, C, etc.)
2. Kleinbuchstaben (a, b, c, etc.)
3. Ziffern/Zahlen (0, 1, 2, etc.)
4. Sonderzeichen (+, =, %, etc.).

Hinweis: Bevor man ein **neues PWD** setzt, sollte man noch einen ';--have I been pwned?-Abgleich machen mittel z.B. dieser Seite <https://haveibeenpwned.com/> oder per <https://www.ibarry.ch/de/>, wo weitere Anwendungen zur Verfügung stehen.

Hinweis **Merkblatt Passwort-Manager**: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_passwortmanager.pdf> .

## Zu 2. Schutz von Informationen

Hinweis **Amtsgeheimnis**: dieses gilt auch für Privatschulen mit kantonalem Auftrag. Die Schule kann den Teilsatz in der Klammer sowie die blaue Markierung im 2. Absatz löschen, wenn sie *keine* Privatschule ist.

Hinweis **Vorsichtsmassnahmen**: um Daten nicht unbeabsichtigt offen zu legen, dürfen sie nur nach Prüfung ins passende Tool ins Internet hochgeladen werden. Beispielsweise sind Personendaten nicht erlaubt, um Übersetzungen in Tools zu erwirken oder Dokumente in PDF zu konvertieren, während Sachdaten möglich sind. Näheres dazu weiter unten in den Schutzstufen.

Hinweis **Datensicherung / freigegebene** **Clouddienste**: Die Schule legt selbst fest, welche Clouddienste genutzt werden können. Es wird empfohlen, dass die Schule ihr Set an freigegeben Cloud-Diensten zusammenstellt und publiziert, z.B. in einer Anleitung oder auf einer Intranet-Seite.

Hinweis Datenablage von **Prüfungen**: Es wird eine Weisung geben betr. Abschlussprüfungen für Gymnasien. Bei Berufsschulen ist es anders, weil Berufsverbände für die Prüfungen verantwortlich sind.

Hinweis **Berechtigungen**: Schulen, die über das MBA die Applikationen betreiben, können in der Zusammenarbeit mit dem MBA das jeweilige Rollen- und Berechtigungskonzept erstellen.

Hinweis **Berechtigungen / Rollen**: Die Schule sollte über ein Rollen- und Berechtigungskonzept verfügen, das den Zugriff für Lernende, Lehrpersonen und Mitarbeiter regelt. Dies sollte in einem regelmässigen Zeitabstand aktualisiert werden.

Hinweis **Information an Ersteller**: Hier geht es vor allem darum, den Absender / Ersteller eines Dokumentes davon in Kenntnis zu setzen, dass sein Dokument ggf. nicht korrekt klassifiziert oder abgelegt wurde. Seitens der Anwendungen werden Rollen- und Berechtigungskonzepte erstellt, die den Zugriff steuern.

Hinweis **Datenkategorie**: Das M365 Konzept geht z.B. darauf ein wie folgt:

|  |  |
| --- | --- |
| Sachdaten  | Informationen, die sich nicht auf Personen beziehen Beispiel: Arbeitsblätter  |
| Personendaten  | Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen Beispiel: Name, Vorname, Adresse  |
| Besondere Personen-daten  | 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: Resultat der schulärztlichen Untersuchung oder der schulpsychologischen Abklärung, Zeugnisse  |

Hinweis zur **Informations-Klassifizierung**: BISR 3 beschreibt die Klassifikationen wie folgt:

* Informationen, die der Öffentlichkeit zugänglich sein können, werden als «Öffentlich» klassifiziert.
* Informationen, die keiner anderen Klassifikation zugewiesen werden, gelten als «Intern» klassifiziert.
* Informationen werden als «Vertraulich» klassifiziert, wenn sie nur für einen definierten Personenkreis zugänglich sein sollen und/oder durch deren Bekanntmachung (auch innerhalb der kantonalen Verwaltung) ein wesentlicher Schaden verursacht werden könnte.
* Informationen werden als «Geheim» klassifiziert, wenn Unberechtigte durch deren Kenntnisnahme den Interessen des Kantons Zürich einen schweren Schaden zufügen könnten.

Hinweis zu **Schutzstufen**:

* 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-Faktor-Authentifizierung und bestenfalls weitergehende Kontrollen, z.B. die Freigabe durch eine Kontrollstelle, oder eine Mehrfaktor-Authentifizierung.

Im Merkblatt (Vorgaben) Datenschutz und Informationsklassifizierung sind Definitionen und Beispiele zur Klassifizierung im Schulumfeld enthalten. Das Merkblatt wurde für die IKT-Grundversorgung erstellt, ist aber allgemein gültig. (https://help.mba.zh.ch/images/IKT-Grundversorgung/DSC-IKTGVSek2-Informationsklassifizierung.pdf)

Hinweis **Schutzstufen in Austausch-Kanälen**: Sämtliche Austausch-Kanäle verstehen sich lediglich als intern, da eine höhere Schutzstufe Verschlüsselungen oder gesicherten Zugang erwartet (also auch den Zugang der Provider unterbinden müsste). Die Lehrperson sollte daher darauf achten, dass keine vertraulichen oder geheimen Informationen geteilt werden, und diese ggf. sofort löschen.

Hinweis **Bekanntgabe von Informationen**: IDG §16 weitere mögliche Empfänger der Information zur Abwendung von Gefahren etc..

Hinweis **auffällige Personen** in nicht öffentlichen Räumen: es geht hier darum zu verhindern, dass Personen (Besucher) andere Personen (Lehrpersonen, Mitarbeitende oder sogar Lernende) zu unerlaubtem Verhalten oder zur Preisgabe von vertraulichen Informationen bewegt werden (Social Engineering).

## Zu 3. Schutz vor Malware

Hinweis **persönliche Geräte**: die Mindestanforderungen zum Einsatz von persönlichen Geräten entstammen dem Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich Informationssicherheit. Zu beachten ist insbesondere, dass es möglich sein muss, auf den privaten Geräten die kantonalen Sicherheitsroutinen umzusetzen und anzuwenden.

Hinweis **verdächtige E-Mails**: Grundsätzlich sollen E-Mails mit verdächtigen Anhängen oder Links in Einzelfällen kommentarlos gelöscht werden oder im Falle von bekannten Absendern, soll man sich bei diesen über die Vertrauenswürdigkeit der empfangenen E-Mail erkundigen. Kommen viele verdächtige E-Mails beim Endbenutzer in den Posteingang, soll sich dieser beim Servicedesk melden, da ein systematisches Problem (kompromittierter Benutzer, welcher intern Spam versendet o.ä.) bestehen könnte.

Hinweis Empfehlungen des **AFI/MBA**: Gerne stellt das MBA auf Anfrage eine jeweils aktuell geltende Empfehlungsliste an Anwendungen zur Sicherung des privaten Gerätes zur Verfügung.

## Zu 4.a Schutz von Kommunikation

Je nach Zielgruppe kann die NRL im Grundsatz angepasst werden.

Auch die Liste der Verwendungen der E-Mails kann ergänzt oder reduziert werden.

Die Reaktionszeit der Nutzenden kann je Zielgruppe innerhalb der Schule definiert werden.

Hinweis **E-Mail-Konto für Lernende**: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( E-Mail-Adressen für Lernende): «Grundsätzlich ist es möglich, Lernenden eine mit ihrem Namen verbundene schulische E-Mail-Adresse zu vergeben. Es ist von Vorteil, auf den vollständigen Namen zu verzichten und Abkürzungen zu benützen. Bei Bedenken oder auf Wunsch kann mit Pseudonymen gearbeitet werden.»

Vorgabe zu E-Mail-Verteilerliste/ -Adresslisten in Outlook aus dem Projekt Grundversorgung Schulen Sek II:

* Lehrpersonen sehen die Adressen aller Lehrpersonen und Lernenden aller Schulen. Dies weil eine erhebliche Anzahl an Lehrpersonen an mehreren Schulen unterrichtet bzw. sich austauscht
* Lernende sehen alle Lernende der eigenen Schule, auch andere Klassen, und die Lehrpersonen der eigenen Schule (aber keine Lernenden oder Lehrpersonen von anderen Schulen).

Hinweis: **E-Mail-Versand**: Verschlüsselung vertraulicher oder höher klassifizierter Daten: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich (Informationssicherheit): «Allgemeine Hinweise, Einladungen usw. dürfen per E-Mail versandt werden. Enthalten die Nachrichten sensitive Informationen, dürfen diese nur verschlüsselt oder anonymisiert über ungesicherte Netze wie das Internet versandt werden. Es dürfen keine Rückschlüsse auf die betroffenen Lernenden möglich sein, selbst wenn die Namen abgekürzt sind.»

Hinweis: **E-Mail Weiter- oder Umleitung** auf private Adressen: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Informationssicherheit): «Wenn Lehrpersonen, Mitglieder der Schulleitung oder andere Schulangehörige Informationen von ihrer schulischen E-Mail-Adresse an ihre private E-Mail-Adresse weiterleiten, muss die Schule angemessene organisatorische und technische Massnahmen zum Schutz dieser Daten umsetzen.»
In der EDU / EXO-Domain ist es heute per Policy unterbunden, E-Mails vom EDU-Account an externe Empfänger weiterzuleiten.

Die genannten Elemente können wahlweise behandelt, gelöscht oder ergänzt werden.

## Zu 4.b Collaboration Tools

Beim EDUzh-Tenant besteht eine Grundverschlüsselung*.* Vertrauliche oder geheime Informationen, die im EDUzh-Tenant bleiben, können, ohne weitere Verschlüsselung bearbeitet werden. Sobald Informationen (Dateien, Chat, Videocalls, Mails) den EDUzh-Tenant verlassen, müssen sie zusätzlich verschlüsselt werden.

Hinweis zum **Hintergrund**: hier haben wir uns an <https://www.avepoint.com/de/ebook/microsoft-teams-best-practices> orientiert.

## Zu 5. Netzwerk und Internetnutzung

Vergleiche dazu die **Verordnung über die Nutzung von Internet und E-Mail** <https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-177_115-2003_09_17-2003_10_01-043.html>

Hinweis: Die Verordnung stammt aus dem Jahr 2003. Die Anwendbarkeit und Relevanz in der heutigen Zeit dürfte etwas kontrovers angesehen werden.

## Zu 6. Arbeiten von unterwegs oder zu Hause

Die Schule kann hier wählen zwischen 1 oder 2.

Hinweis zur **Zwei-Faktor-Authentifizierung**: Hierzu wird es neue Vorgaben seitens MBA DCS SekII für den EDUzh-Tenant geben. Es werden laufend neue Policies aufgeschaltet, um die Risiken zu reduzieren, so wird z.B. der Zugriff aus dem Ausland nur noch mit Zwei-Faktor-Authentifizierung gewährt. Später werden weitere Regeln für z.B. Applikationen mit schützenswerten Daten eingeführt. Gilt jeweils für den EDUzh-Tenant. Schulen mit eigenem Tenant sind angehalten, ähnliche Restriktionen einzuführen.

Weitere Grundlagen: [Leitfaden Einsatz von mobilen Geräten in der Verwaltung](https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_einsatz_von_mobilen_geraeten_in_der_verwaltung.pdf) [https://docs.datenschutz.ch/u/d/publikationen/leit0faeden/leitfaden\_einsatz\_von\_mobilen\_geraeten\_in\_der\_verwaltung.pdf](https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_einsatz_von_mobilen_geraeten_in_der_verwaltung.pdf).

# Persönliche Geräte /BYOD

Hinweis Smartphone: Es ist zu erwarten, dass ein Smartphone ein fester Bestandteil des Arbeitsplatzes wird. In Bezug auf mehr Sicherheit kann ein Smartphone als Authentifizierungsmittel genutzt werden. Die Mindestanforderungen der Geräteanforderungen sind umzusetzen.

In Zukunft wird die Bereitstellung und der Betrieb einer Softwarelösung für die Verwaltung der Geräte (Enterprise Mobility Management) zur Verfügung stehen. Dies ermöglicht unter anderem bei einem Verlust des Gerätes, die Geschäftsdaten zu löschen.

Hinweis **Netzanbindung/Gastzugang**: Hier entscheidet die Schule, ob und unter welchen Bedingungen der Gast-Zugang ins schulinterne Netz erlaubt ist.

Hinweis **Mindestanforderungen**: s.o. 3. Schutz vor Malware.

Hinweis: Es ist zu erwarten, dass künftig (IKT-Grundversorgung Sek II) gewisse automatische Scans die Mindestanforderungen beim Anschluss an das LEUNET bzw. die IT-Infrastruktur prüfen (z.B. aktuelle Browserversion, aktueller Virenschutz). Je nach Ergebnis wird der Zugriff auf mehr oder weniger Ressourcen freigegeben (Drucker, Applikationen, OneDrive, etc.).

Hinweis zum **Virenschutz**: Mit einer über das MBA erworbenen Lizenz von Sophos können 10 Geräte mit einem Virenschutz ausgerüstet werden. Die Lizenz beinhaltet keine Version für Smartphones.

Hinweis zur **Synchronisation** mit dem persönlichen Gerät: die Schule muss die Voraussetzungen und kantonalen Vorgaben kennen bzw. selbst definieren und offenlegen. Zu beachten ist insbesondere, dass es möglich sein muss, auf den privaten Geräten die kantonalen Sicherheitsroutinen umzusetzen und anzuwenden.

Die genannten Elemente können wahlweise behandelt werden.

Hinweis **Support** von BYOD: Grundsätzlich gilt, dass BYOD Geräte privat gekauft und selber verwaltet und supported werden. Die Schulen können auch einen begrenzten Support durch ihre eigene IT-Organisation vorsehen.

Ein Support-Anspruch seitens des MBA auf BYOD muss vertraglich geregelt werden und gilt nicht per se. Dies gilt insbesondere für die Option, Daten von BYOD Geräten zu sichern.

## Zu 5. Onlineprüfungen

Empfehlung: Durchführung von digitalen Prüfungen auf schuleigenen Geräten. Dies verhindert viele Probleme und Unsicherheiten.

Zusammenfassend der Stand der Diskussionen mit dem Rechtsdienst (RD) des MBA im April 2021:

* Der RD ist dem digitalen Prüfen gegenüber zurückhaltend eingestellt, da diverse rechtliche Aspekte ungeklärt sind.
* Grundsätzlich sollten Prüfungen vor Ort durchgeführt werden.
* Wenn das nicht möglich ist, sollten die digitalen Prüfungen möglichst auf schuleigenen Geräten (bspw. in den Computerräumen der Schulen) durchgeführt werden.
* Lernende haben Anspruch auf Einsicht in ihre Prüfungen. Das schliesst die Aufgabenstellung mit ein, unabhängig davon, ob die Prüfungen physisch oder elektronisch stattgefunden haben.
* Bei Prüfungsarbeiten handelt es sich um Personendaten.
* Unlauteres Verhalten bei Prüfungen und Hausarbeiten sind Disziplinarfehler.
* Diese regeln die Schulen nach dem Maturitätsprüfungsreglement und dem Mittelschulgesetz selbst. Massnahmen kommen gemäss Disziplinarreglement in Betracht.
* Der Einsatz von Analysetools muss vorgängig klar und deutlich den Lernenden bekannt gegeben werden.
* Wenn Analysetools eingesetzt werden mit einer Cloud-Lösung, gelten zusätzliche Anforderungen.
* Die Überwachung der Lernenden während der Prüfung muss verhältnismässig sein.
* Wenn kein Betrugsfall festgestellt wurde, sind die Logdateien sofort zu löschen.
* Für Prüfungsüberwachungen per Video braucht es tiefergehende rechtliche Abklärungen.
* Für den Einsatz von Zoom sind konkrete Vorgaben des RD anzuwenden.
* Onlineprüfungen sind rechtlich nicht eindeutig geklärt und müssen im Einzelfall bewertet werden.
* Hinweis des RD: Letztendlich können Prüfungen nicht vor dem Kopieren geschützt werden.
* Der RD rät davon ab, Noten in irgendeiner Form in der Cloud abzulegen.
* Die datenschutzrechtliche Klassifizierung von Noten ist nicht abgeschlossen und muss von Fall zu Fall behandelt werden.

Das dieser Zusammenstellung zugrunde liegende Dokument findet sich im DLH unter: <https://dlh.zh.ch/component/jdownloads/?task=download.send&id=7&catid=3&m=0&Itemid=101> .

Hinweis zur **Überwachungs-Software bei Prüfungen**: Das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich sagt dazu Folgendes (Analyse Prüfungsbetrug): «Die Lernenden müssen vorgängig klar und deutlich über den Einsatz des Analysetools sowie über den Umfang der Überwachung informiert werden. Weiter sollten als Alternative schulische Geräte zur Verfügung gestellt werden, die so konfiguriert sind, dass keine Überwachung notwendig ist.» «Das Loggen ist auf die Prüfungsdauer zu beschränken. Wird kein Betrugsfall festgestellt, sind die Logdateien sofort zu löschen. Bei konkreten Hinweisen auf einen Prüfungsbetrug können die Daten bis zum Abschluss eines Verfahrens aufbewahrt werden.»

# Datenschutz

## Zu 1. Generell

Absätze, die auf die Zielgruppen (Mitarbeitende, Lehrpersonen, Lernende) nicht zutreffen, können gelöscht werden.

Falls die Schule gegenwärtig über keine Datenschutzerklärung verfügt, kann dieser Abschnitt gelöscht werden.

Hinweis **Gültigkeit Datenschutzrecht:** In diesem Falle gilt das kantonale Datenschutzrecht und seine weiteren Bestimmungen auch für Privatschulen, die einen kantonalen Leistungsauftrag erfüllen.

## Zu 2. Im Unterricht

Absätze, die auf die Zielgruppen (Mitarbeitende, Lehrpersonen, Lernende) nicht zutreffen, können gelöscht werden.

Hinweis **Datensparsamkeit**: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich

* Auslagerung: «Zu berücksichtigen ist weiter, dass gewisse Dienste verlangen, Daten über sich bekannt zu geben. Werden beispielsweise E-Mail-Adressen mit dem Namen verknüpft, sollte die Schule die Lernenden darüber informieren und bei Bedenken Pseudonyme für die E-Mail-Adressen verwenden.»
* Soziale Medien: «Wird über Messenger kommuniziert, sind vor allem die Verschlüsselung, der Serverstandort und die Möglichkeit der anonymen Nutzung datenschutzrelevant. Es ist von Vorteil, Anbieter zu berücksichtigen, die europäische Standorte und eine Ende-zu-Ende-Verschlüsselung anbieten (beispielsweise Threema).»
* Whatsapp: «Deshalb können Lehrpersonen und andere schulische Mitarbeitende Informationen untereinander oder mit Lernenden nicht über WhatsApp austauschen.
Das Mindestalter für die Nutzung von Messaging-Diensten wurde auf 16 Jahre erhöht.»

Hinweis **Anwendungen**: Beim Einsatz von Anwendungen im Unterricht, die nicht von der Schule freigegeben bzw. empfohlen sind, ist die Lehrperson verpflichtet, die Lernenden über die Datenschutz-Konsequenzen zu informieren (bspw. Speicherort der Daten bei SaaS-Lösungen, Datenaufbewahrungsdauer, Möglichkeit der Löschung der Daten, etc.).

Mit nicht datenschutzkonformen fremden Anwendungen dürfen keine Personendaten der Lernenden bearbeitet werden.

Vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich (Auslagerung): «Produkte, bei denen die datenschutzrechtlichen Anforderungen nicht erfüllt sind, wie Dropbox und Google Drive, können nur für das Bearbeiten von nicht sensitiven Daten eingesetzt werden. Ausgetauscht werden können beispielsweise Unterrichtsmaterialien, Arbeitsblätter und Fotos. Aufsätze, in denen persönliche Erlebnisse beschrieben werden, dürfen nicht mit diesen Produkten bearbeitet werden.»

Hinweis Einsatz Social Media: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Soziale Medien): «Da die Lernenden für die Nutzung sozialer Medien auch eigene Daten bekannt geben müssen, muss das Einrichten eines «Accounts» freiwillig sein. Bei jüngeren Lernenden sind die Eltern zu informieren. Die auf diesem Weg bekannt gemachten schulischen Informationen müssen auch auf andere Weise zugänglich sein. Der interaktive Austausch ist infolge der heiklen umfassenden Datenerfassung, -speicherung und Weiterbearbeitung durch die Betreiber auf ein Minimum zu beschränken. Auf den Austausch sensitiver Informationen wie solche über die Gesundheit oder Ähnliches ist zu verzichten.»

Hinweis **Social Media/ Facebook**: <https://www.privatim.ch/wp-content/uploads/2017/06/privatim_Soziale_Medien_2013_V11.pdf>. Hierbei ist die Quintessenz, dass eine Nutzung der Social Media gestattet werden kann, jedoch die Kommunikation der Lehrperson an die Lernenden und der Lernenden untereinander nicht auf diese Medien verlegt werden darf (Bildung einer eigenen Benutzergruppe zum Austausch über Schulthemen, Aufgaben, Arbeiten).

Sollte eine Lehrperson für eine Klasse einen Kanal auf Social Media eröffnen, ist zu beachten:

* Dass viele Kanäle die Möglichkeit bieten, Benutzergruppen zu unterteilen, Untergruppen nach Themen zu eröffnen und den Zugriff zu steuern. Jede der Chat Foren, Social Media und anderen Kommunikationskanälen gilt es daraufhin zu prüfen;
* Den Teilnehmerkreis klar zu definieren und einzugrenzen;
* Nur Referenzen auf Dateien enthalten und keine sensiblen Daten direkt einbinden;
* Dass die Beiträge nur eine begrenzte Zeit erhalten bleiben, regelmässig kontrolliert und gelöscht werden;
* Der Teams Chat einer Klasse oder schulischen Gruppe ist zu löschen, wenn die Lernende die Schule verlassen. Der Chat kann vorgängig archiviert werden, um spätere Nachfragen zu beantworten;
* Damit bedeutet das Eröffnen eines Austausch-Kanals (Channel, Chat, Blog) vor allem der Beginn einer ständigen Überarbeitung von Austausch-Informationen. (Vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich (Instagram): «Instagram ist eine Plattform, die auf das Teilen von Bildern ausgerichtet ist. Instagram kann nur beschränkt für schulische Zwecke genutzt werden.»)

Hinweis **Datenhaltung der Austausch-Kanäle**: Die Vorhaltung der Austausch-Kanäle ist so lange datenschutzkonform, wie der Bildungszweck es erfordert.

In diesem Zusammenhang muss besonders auf die **Disziplinar Reglemente** der Schulen und des Kantons hingewiesen werden: das Hochladen von Bildern ohne die Erlaubnis der darauf abgebildeten Personen kann strafrechtlich geahndet werden.

Hinweis zu **Auswertungen über die Lernenden**: Gegenwärtig besteht keine genügende Rechtsgrundlage für die Erstellung von Persönlichkeitsprofilen durch die Schule. Diese müsste gemäss unserer Meinung mit einer Gesetzesrevision erst geschaffen werden.
Damit ist die Erstellung von Auswertungen über die Notenentwicklungen nicht erlaubt. Auch dann nicht, wenn sie anonymisiert erfolgt.

Vgl. Das Datenschutzlexikon Grundbegriffe und Definitionen der Datenschutzbeauftragten des Kantons Zürich (Persönlichkeitsprofil): Zum Begriff «Persönlichkeitsprofil» nach Art. 3 lit. d des Bundesdatenschutzgesetzes meint die Eidgenössische Datenschutzkommission: «Der Begriff des Persönlichkeitsprofils kann nicht generell formuliert werden», «[...] Menge und Inhalt der personenbezogenen Daten [sind] ausschlaggebend. Daten, die über einen längeren Zeitraum zusammengetragen werden und so ein biografisches Bild ergeben (Längsschnitt), sind eher als Persönlichkeitsprofil zu qualifizieren als solche, die eine blosse Momentaufnahme darstellen (Querprofil)» (Urteil der Eidgenössischen Datenschutzkommission vom 27.01.2000, VPB 65.48).

(§ 3 Abs. 4 lit. b IDG)

Finden **Auswertungen** **fachspezifisch** statt, z.B. um Schuljahr- oder Lernenden übergreifenden Erfolg der Unterrichtsmaterialien und -methoden zu messen, können diese Statistiken bekannt gegeben werden, soweit aus den Ergebnissen keine individuellen Profile erkennbar sind. (D.h. die Gruppierung der Kennzeichen ist so zu wählen, dass kein Rückschluss auf einzelne Personen möglich ist.)

Hinweis zu **Schul-Veranstaltungen**: Hierzu besteht nach dem Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Fotografieren in der Schule) die Möglichkeit zu **konkludentem Verhalten** oder zum **Opt-out** während der Schul-Veranstaltung: «Die Einwilligung kann grundsätzlich formlos oder durch konkludentes Verhalten erfolgen. Konkludentes Verhalten bedeutet, dass die betroffene Person sich so verhält, dass man daraus schliessen kann, dass sie nichts gegen das Fotografieren einzuwenden hat. Auch ein Opt-out ist möglich. Hier informieren Lehrpersonen, dass an einem Anlass fotografiert wird, und bitten die Personen sich zu melden, die nicht auf Bildern erscheinen wollen.» Zu beachten: in jedem Fall muss die Einwilligung der abgebildeten Personen erfolgen. Dies gilt auch für alle weiteren u.g. Fälle.

Hinweis **Bekanntgabe**: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Schülerdossier): «In das Schülerdossier gehören Unterlagen über Lernende, die im Zusammenhang mit dem Auftrag der Schule relevant sind. Arbeitsmaterial und Unterrichtsunterlagen werden im Normalfall bei der Lehrperson aufbewahrt. Sie können im Einzelfall im Schülerdossier abgelegt werden, wenn sie beispielsweise für die Beurteilung der Betroffenen oder für ein Gespräch mit den Eltern benötigt werden. Lernende respektive ihre gesetzlichen Vertreter haben Anspruch auf Einsicht in ihr Dossier. Sie können die Berichtigung oder Vernichtung unrichtiger Daten verlangen.»

Hinweis **Kontaktangaben oder Fotos**: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Bekanntgabe von Informationen von allgemeinem Interesse): «Private Kontaktangaben oder Fotos dürfen nur mit Einwilligung der Betroffenen veröffentlicht werden. Als Informationsträger kommen hauptsächlich die Schulwebsite, das Intranet oder Printmedien in Frage. Schülerlisten mit Vor- und Nachnamen können im Intranet oder in Printmedien, nicht aber auf der Schulwebsite aufgeführt werden.»

Hinweis zu **Fotos im Intranet Sek II**: Frühere Abklärungen mit dem Rechtsdienst MBA haben ergeben, dass Lernende selber entscheiden müssen, ob sie eine Veröffentlichung ihres Bildes im Intranet SekII wollen oder nicht. Dazu wurde eine Einstellmöglichkeit im persönlichen Profil geschaffen, wer ein Bild einsehen kann und wer nicht. Per Default steht dies für die gesamte Schule auf «Nein». Der Default kann von DSCSII (ex. MBA-IT) geändert werden, wenn von der Schule eine Bestätigung vorhanden ist, dass die Einwilligung aller Lernenden und Lehrpersonen schriftlich vorliegt und die Schule diese Einwilligung künftig auch von allen neuen Lernenden und Lehrpersonen einholt.

Hinweis **Videos**: vgl. das Datenschutzlexikon Mittelschule Berufsfachschule der Datenschutzbeauftragten des Kantons Zürich ( Videokameras): «Videoaufnahmen im Unterricht sind nur zu schulischen Zwecken erlaubt. Es ist darauf zu achten, dass in Rollenspielen oder Vorträgen keine intimen oder andere sensitiven Informationen bekannt gegeben werden. Die Aufnahmen dürfen anderen, nicht am Unterricht oder an Schulprojekten beteiligten Personen nicht zugänglich gemacht und müssen nach Abschluss der Arbeiten gelöscht werden.»

Hinweis **Alter, bis wann Zustimmung der Eltern** einzufordern ist: Hier ist sich die juristische Lehre nicht einig, da die Urteilsfähigkeit von Person zu Person in diesem Alter stark variiert. Sicherheitshalber sollten hier 14 Jahre eingefügt werden.

Hinweis **Datenschutzverletzungen**: es besteht eine Meldepflicht von Datenschutzvorfällen im Zusammenhang mit personenbezogenen Daten, welche im [Merkblatt Meldepflicht bei Datenschutzvorfall](https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_meldepflicht_datenschutzvorfall.pdf) beschrieben ist: «Ein Datenschutzvorfall muss gemeldet werden, wenn er zu einer Gefährdung der Grundrechte auf informationelle Selbstbestimmung beziehungsweise auf Privatsphäre von betroffenen Personen führen kann. Bestehen Zweifel, ob Grundrechte gefährdet sind, ist ebenfalls Meldung zu erstatten.»

# Urheberrechte

Hinweis allgemein: Es sollte sinngemäss ein Paragraf «Daten und Inhalte (Lehrmittel), die im Auftrag der Schule und während der Schulzeit erstellt werden, gehören der Schule. Der Schulkörper kann über diese Daten verfügen.» in den Arbeitsverträgen enthalten sein, daher fehlt dieser Passus in der Nutzungsrichtlinie.

## Zu 2. Im Unterricht

Die Rechte an und die Nutzung von Werken (Musik, Literatur, Kunst etc.) ist im Urheberrechtsgesetz (URG) geregelt. Das URG sieht für gewisse Zwecke gesetzliche Lizenzen, d.h. Nutzungsrechte vor. Im Schulalltag betrifft dies die Nutzung für Unterrichtszwecke oder die interne Dokumentation und Information der Schule. Achtung: Die gesetzliche Lizenz gilt nicht für Computerprogramme.

Für Vervielfältigungen von Werken bzw. deren im Handel erhältliche Exemplare im Rahmen einer gesetzlichen Lizenz schuldet die Schule eine Vergütung. Um den Schulen eine kostengünstige Nutzung ermöglichen, stellt die Verwertungsgesellschaft ProLitteris einen einheitlichen Tarif für gewisse Nutzungsformen zur Verfügung.

Für Nutzungen, welche die gesetzliche Lizenz und/oder der Tarif von ProLitteris nicht vorsieht, muss die Erlaubnis vom Rechteinhaber eingeholt werden.

Wie dürfen Schulen urheberrechtlich geschützte Werke im Alltag nutzen?

Die nachfolgende Tabelle soll hierzu einen groben Überblick verschaffen:

|  |  |
| --- | --- |
| Gesetzliche Lizenz | Erweiterte Lizenz von Pro-Litteris für folgende Werke:  |
| Was | Erlaubter Zweck | Erlaubter Nutzungsumfang |
| Werke und deren Exemplare (literarische Texte, Kunst, Musik, etc.)Im Handel erhältliche Werkexemplare (Bücher, Zeitungen, Ton- und Bildträger, Datenträger etc.) | Verwendung für den eigenen Unterricht durch die Lehrperson oder die interne Information / Dokumentation*--> keine Unterhaltungszwecke (bspw. Film- oder Theatervorführungen in der Schule)* | Vervielfältigung in der Form von Papier- und Digitalkopien sowie ggf. das Speichern auf DatenträgernEs dürfen nur Ausschnitte\* von im Handel erhältlichen Werkexemplare vervielfältigt werden\*Max. 75% (vgl. Glossar) | * + Ganze Sendungen, die direkt aus einem Radio und TV-programm stammen
	+ Werke der bildenden Kunst
	+ Musiknoten
	+ Musikaufführungen
	+ Tagungen von Schulen
 |

Die Tabelle erhebt keinen Anspruch auf Vollständigkeit.

Hinweis **Grundsatz**: Bitte hier die jeweiligen Schulverträge mit ProLitteris oder anderen Verlagen, soweit bestehend, in Betracht ziehen. Hier kommt es auf die schulinterne Regelung an, denn bei der Kopie von ganzen Werken fallen Gebühren von ProLitteris an.

Die aktuellen Gebührenregelungen und Lizenzen von ProLitteris gelten von 2022 bis 2026 und ist unter <https://prolitteris.ch/wp_update2020/wp-content/uploads/GT_7_Schulen_2022-2026.pdf> einsichtbar.

Hinweis zur **vollständigen Aufzeichnung** von Sendungen: Dies ist eine Lizenzerweiterung für Schulen von ProLitteris. Allerdings kommt es hier darauf an, ob es Privatschulen oder öffentliche Schulen sind. Öffentliche Schulen zahlen ProLitteris dafür eine Lizenzgebühr. Private Schulen, die keine ganzen Aufnahmen nutzen, zahlen ggf. keine Lizenzgebühren. Die Veröffentlichung von vollständigen Aufzeichnungen unterliegt ggf. der Ziffer 3 des GT7 und kann gebührenpflichtig sein.

Hinweis **NanooTV:** die Downloads per NanooTV sind per kantonalem Vertrag genehmigt.

Hinweis auf **Mediatheken**: diese bieten oft kostenfreien Zugang.

Hinweis zu **Musikaufführungen** / **Theatralischer Musik:** «Musik, die für den Spielablauf fakultativ ist. Wenn die Musik zum Gelingen einer Bühnenproduktion beiträgt, aber nicht so eng mit dem Text verbunden ist, dass das Stück ohne diese Musik gar nicht aufgeführt werden kann, ist sie nicht-theatralisch.» <https://ssa.ch/de/glossary/nicht-theatralische-musik/>.

Hinweis **Erstellung von Lehrmitteln**: Dazu sagt der Leitfaden von ProLitteris, S. 5: «Das Herstellen von Lehrmitteln unter Verwendung von fremdem Material ist ein Verlagsgeschäft und setzt die individuelle Regelung der Rechte voraus. Ohne diese Genehmigungen sind nur eigene Inhalte, lizenzfreie Inhalte (Schutzdauer abgelaufen oder bestimmte Creative Commons–Lizenzen) und korrekte Zitate im Rahmen des eng begrenzten Zitatrechts (Art. 25 URG) erlaubt.»

Hinweis zur Nutzung **ausserhalb des Unterrichts**: Hierfür sind die Tarife gemäss der Merkblätter G8 und G9 von ProLitteris einschlägig. G7 gilt nur für den Unterricht.

Ergänzender Hinweis zur **Nutzung ganzer Sendungen auf Plattformen**: Unerheblich ist dabei, wer der Betreiber der Plattform ist.

Hinweis **Urheberrecht der Schule**: Die entschädigungslose Übertragung der Urheberrechte und deren Abgeltung mit dem üblichen Lohn muss im Arbeitsvertrag mit der Lehrperson vereinbart werden.

# Massnahmen bei Verstössen

Hinweis zu **gesetzlichen Bestimmungen**: vgl. Personalgesetz des Kanton Zürich §51 Verschwiegenheitspflicht und IDG §23 Einschränkung im Einzelfall (Verweigerung der Herausgabe von Personendaten) und folgende Paragraphen. Die Untersuchung und Beurteilung von Widerhandlungen unterliegt gemäss §40 IDG den Stadthalterämtern.

Hinweis zu **Protokoll und Speicherung** von Vorfällen: hier ist zu beachten, dass die Archivverordnung <https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-413_322-2015_03_05-2015_08_01-089.html> in §6 Absatz b «die Sicherung berechtigter Interessen betroffener Personen oder Dritter» als archivwürdig bezeichnet. Darunter gehören Datensicherheitsvorfälle. Damit können Berichte zu Datenschutz-Vorfällen zwar aus dem direkten Zugriff bzw. der Papierablage entfernt werden, jedoch nur in ein weiterhin verfügbares Archiv.

Hinweis **Dauer der Datenhaltung**: Generell gelten für Daten dieselben Aufbewahrungsvorschriften, wie für die zugehörigen Akten (physischen Ablagen) gelten.
«Die Mittel- respektive Berufsfachschule darf ihre Papier- und elektronischen Akten solange aufbewahren, wie sie diese für das Erfüllen ihrer Aufgaben benötigt (laufende Ablage). Die darauffolgende Aufbewahrungsfrist wird von den Schulen gemäss IDG selbst festgelegt, es sei denn, es existieren spezialgesetzliche Regelungen (ruhende Ablage). Werden keine Fristen festgelegt, gilt die im Gesetz statuierte maximale Frist von zehn Jahren. Wie diese Fristen aussehen, ist in den Musteraktenplänen des Mittelschul- und Berufsbildungsamtes dokumentiert.» (Quelle: <https://www.datenschutz.ch/lexika/mittelschule-berufsfachschule/aktenaufbewahrung>).

Hinweis **Disziplinarreglemente**:

Mittelschulen LS 413.322 , <https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-413_211_1-2015_02_02-2015_08_01-110.html>

Berufsbildung LS 413.322 <https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-413_322-2015_03_05-2015_08_01-089.html>

Zitiert aus dem  [Datenschutzlexikon Mittelschule Berufsfachschule](https://datenschutz.ch/lexika/mittelschule-berufsfachschule):

§ 8. Jede Beeinträchtigung des Schulbetriebs ist untersagt. Dazu gehören insbesondere

1. Verstösse gegen die Hausordnung und schulinterne Erlasse
2. Nichtbefolgen von Anweisungen der Schulleitung, Lehrpersonen und anderen von der Schulleitung ermächtigten Personen.

Da die Nutzungsrichtlinie der Schule **Weisungscharakter** hat, muss sie nicht unterschrieben oder akzeptiert werden.

Hinweis **Strafbares Verhalten durch Schule melden**: Lehrpersonen und andere Mitarbeitende der Schule haben im Fall eines Verdachts auf eine strafbare Handlung grundsätzlich ein Anzeigerecht und keine Anzeigepflicht.

# Ende der Benutzerrolle

Hinweis **Löschen** von Daten: Zur datenschutzkonformen und sicheren Datenlöschung wird das sogenannte Wiping empfohlen, bei dem die Daten mehrfach mit anderen Daten überschrieben werden, und diese damit unwiederbringlich unlesbar sind. Bei Bedarf können hier der schulinterne Service Desk, der IT-Verantwortliche der Schule oder der Digitale Service Center SekII unterstützen.

# Anhänge

Hinweis zur Netiquette / **Messenger**: Vgl. das Merkblatt zu Messenger und Videokonferenzen <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_messenger_videokonferenzsysteme.pdf>

Hinweis **Videos**: Falls das Einverständnis zu Videokonferenzen noch nicht im Anstellungsvertrag generell geregelt ist, muss für jede Sitzung erneut das Einverständnis der Teilnehmer eingeholt werden.

Die genannten Elemente können wahlweise angepasst, gelöscht oder ergänzt werden.