Schule für Gestaltung Zürich

Nutzungsrichtlinien zur Verwendung von Informatik-mitteln an der SfGZ

Lernende, Studierende und Kursteilnehmer/innen

Inhalt

Einleitung 3
I. Allgemeine Bestimmungen 3
1. Zweck 3
2. Grundlagen 3
3. Geltungsbereich 3
4. Begriffe 4
5. Verwendungszweck 4
6. Auswertungen von Randdaten 4
II. Nutzung von schulinternen IT-Arbeitsmitteln (nicht BYOD) 4
1. Änderungen 5
2. Anwendungen 5
3. Supportorganisation 5
4. Weitere Hilfestellungen 5
III. Datensicherheit 5
1. Schutz von Zugangsdaten 5
2. Schutz von Informationen 6
3. Schutz vor Malware 6
4. Schutz von Kommunikation 7
5. Netzwerk- und Internetnutzung 8
6. Meldepflicht 9
IV. Persönliche Geräte / BYOD 9
1. Grundsatz 9
2. Geräteanforderungen 9
3. Synchronisation 9
4. Support 9
5. Onlineprüfungen 10
V. Datenschutz 10
1. Generell 10
2. Im Unterricht 10
VI. Urheberrechte 10
1. Im Unterricht 10
VII. Massnahmen bei Verstössen 12

VIII. Ende der Benutzerrolle 12
IX. Haftungsausschlus 13
Anhang I – Rechtliche Grundlagen 14
Anhang II – Glossar 16
Anhang III – Netiquette (alle) 19

Einleitung

Für die Schule für Gestaltung Zürich ist die Förderung kreativer Kompetenzen zentral. Dies zeigt sich in der vertieften Auseinandersetzung mit Themenbereichen, in der Vernetzung von Wissen, der Mitgestaltung des Unterrichts und in der gestalterischen Arbeit z.B. in den verschiedenen Werkstätten der Schule. Dabei ist es uns wichtig, dass unsere Lernenden das Handwerk, von bewährten analogen, bis hin zu aktuellen digitalen Techniken kennenlernen und deren Gestaltungspotenzial erfahren. Dies führte in den letzten Jahren zu einem markanten Ausbau der IKT-Umgebung, sowohl im Hard- als auch im Softwarebereich. Um die Nutzung aller an der Schule sich im Einsatz befindlichen IKT-Systeme zu regeln und zu gewährleisten, beschliesst die Schulleitung der Schule für Gestaltung Zürich, gestützt auf das Personalgesetz, das Gesetz über Information und Datenschutz (IDG) sowie zugehörige Verordnungen, die Informatiksicherheitsverordnung etc., folgendes:

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

2. Grundlagen

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

Als unselbständige Anstalt ist sie ausserdem an die Allgemeine Informationssicherheitsrichtlinie vom 3. September 2019 und die ergänzenden Besonderen Informationssicherheitsrichtlinien des Kantons gebunden.

3. Geltungsbereich

Diese Nutzungsrichtlinie gilt für Lernende, Studierende sowie Kursteilnehmende, die Zugang zu IKT-Systemen der Schule für Gestaltung Zürich (nachfolgend genannt «Schule») haben («Benutzende»). Die Benutzenden sind persönlich dafür verantwortlich, diese Richtlinie einzuhalten.

Mit dem ersten Login oder der Nutzung der zur Verfügung gestellten IT-Infrastruktur nehmen die Benutzenden 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 befinden sich im Glossar im Anhang.

5. Verwendungszweck

Die IKT-Systeme und Anwendungen sind auf schulische oder institutionelle Zwecke ausgerichtet. Der sorgsame und verantwortungsvolle Umgang mit allen IKT-Systemen garantiert einen störungsfreien Betrieb und dient allen Benutzenden.

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 Nutzung zu kommerziellen Zwecken ist nicht erlaubt, ausser die Schulleitung erteilt hierfür eine Bewilligung.

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

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

6. Auswertungen von Randdaten

Bei der Nutzung der IKT-Systeme fallen Randdaten an, die in Logfiles unterschiedlicher Komponenten (Firewall, Server, Anwendung, etc.) gespeichert werden. Zur Erkennung und Rückverfolgung von Sicherheitsvorfällen können die Schule und der Kanton Zürich innert der gesetzlichen Frist auf diese Logfiles zurückgreifen.

II. Nutzung von schulinternen IT-Arbeitsmitteln (nicht BYOD)

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.5 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. Räume, die IT-Arbeitsmittel enthalten, sind beim Verlassen, wenn es der Schulalltag erlaubt, 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.

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

3. Supportorganisation

Für den Support sind der schulinterne Vor-Ort-Support und der Service Desk des Digitalen Service Center SekII zuständig. Die Kontaktangaben sind auf der Homepage der Schule auffindbar. Der schulinterne Vor-Ort-Support dient als erste Anlaufstelle.

4. Weitere Hilfestellungen

Für gewisse IT-Arbeitsmittel existieren separate Nutzungsvorgaben und Anleitungen. Hilfestellungen der Schule unterstützen die Benutzenden beim Setup und der Nutzung der IT-Arbeitsmittel im Schulalltag. Die Hilfestellungen sind im internen Bereich SfGZ auffindbar.

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

a. Benutzerkonto

Erhält der Benutzende ein Benutzerkonto, dient dies für: die Nutzung der MS-365 Anwendungen, die Nutzung der Adobe Creative Cloud Produkte, dem Zugang zur internen Mailadresse.

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 Benutzenden tragen für alle mit ihrem Benutzerkonto ausgeführten Aktivitäten die volle Verantwortung. Beim Verdacht auf Missbrauch kann das Benutzerkonto ohne Vorwarnung durch die Schule bzw. den Kanton gesperrt werden.

Die Benutzenden melden sich von allen Systemen ordnungsgemäss ab, wenn sie ihre Arbeitsstation definitiv verlassen.

b. Passwortschutz

Die Benutzenden sind verpflichtet, für sämtliche Zugänge ein starkes Passwort zu wählen.

Für jeden Zugang ist ein separates, einzigartiges Passwort zu wählen. Das Passwort ist alle 90 Tage zu ändern.

Die für die an der Schule verwendeten Passwörter dürfen nicht für private Zugänge verwendet werden.

2. Schutz von Informationen

Die Benutzenden haben Vorsichtsmassnahmen zu ergreifen, damit Informationen, die den Schulbetrieb, den Unterricht betreffen (nachfolgend «schulinterne Informationen»), nicht unbeabsichtigt offengelegt, entwendet oder gelöscht bzw. unkenntlich gemacht werden.

a. 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.

Störungen oder Defekte an bereitgestellte IT-Arbeitsmitteln sind umgehend dem schulinternen Vor-Ort-Support oder der Lehrperson/dem/der Dozierenden zu melden.

3. Schutz vor Malware

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

1. Schutzsoftware darf nicht umgangen oder deaktiviert werden;

2. Es müssen immer sämtliche offiziellen Aktualisierungen und Updates installiert werden, insbesondere die des Virenschutzes;
3. Persönliche Geräte müssen, soweit sie an der Schule zugelassen sind, auf Malware gescannt werden, wenn sie zuvor an einem anderen Netzwerk angeschlossen waren oder Dritte mit dem Gerät gearbeitet haben;
4. Verdächtige E-Mails müssen umgehend gelöscht und als Spam gemeldet werden, bei einer Häufung solcher Fälle hat eine Meldung bei der zuständigen Supportorganisation zu erfolgen;
5. Es dürfen keine Anhänge, die von unbekannten oder verdächtigen Absendern stammen, geöffnet werden;
6. Generell dürfen Werbungen oder Pop-Ups in Nachrichten oder im Internet nicht angeklickt werden, bei externen Links ist Zurückhaltung geboten;
7. Es dürfen keine fremden, nicht autorisierten bzw. bewilligten Wechselmedien an die IT-Infrastruktur der Schule angeschlossen werden;
8. Auffälligkeiten und konkrete Verdachte müssen umgehend gemeldet werden (vgl. Ziff. 7).

4. Schutz von Kommunikation

a. 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; etc..]

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

1. Die Benutzenden sind für die Kontrolle und Pflege ihres Postfachs verantwortlich. Auf E-Mails ist an Werktagen und in der letzten Woche der Sommerferien in der Regel innerhalb von 48 Stunden zu reagieren.
2. Vertraulich und höher klassifizierte Nachrichten müssen verschlüsselt und signiert versendet werden.
3. E-Mails dürfen nicht an externe (private oder geschäftliche) Postfächer weiter- oder umgeleitet werden.
4. Das E-Mail-Konto darf 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 benutzt werden.
5. Die E-Mailadresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshop-ping, etc.) genutzt werden.

b. Collaboration Tools

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

1. Die Benutzenden verwenden Collaboration Tools für die schulinterne Kommunikation;
2. Die Anzahl neuer Kanäle ist auf das Nötige zu limitieren;
3. 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;
4. Vertrauliche oder höher klassifizierte Informationen sind End zu End verschlüsselt auszutauschen, egal ob im Chat, Kanal oder im Videoanruf.
   (Hinweis: dies erfolgt im EDU-Tenant automatisch);
5. 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.

5. 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:

1. Up- und Downloads von grossen Dateien sind zu verhindern, insbesondere die Installationen von Spielen und grossen Audio- und Videodateien aus dem Internet;
2. Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden;
3. Der Besuch des Darknets ist verboten;
4. Der Besuch von Webseiten mit folgenden Inhalten ist verboten: pornografische, sexistische, rassistische oder gewaltverherrlichende Äusserungen bzw. Darstellungen; Glücks- und Geldspiele; Pyramiden- und Schneeballsysteme; Terrorismusförderung und -Finanzierung, sonstige, rechtswidrige oder gegen die guten Sitten verstossende Inhalte;
5. Während des Unterrichts ist der Besuch von Social Media und sonstige Unterhaltungsseiten verboten, ausser dies gehört zum Unterrichtsstoff;
6. Schulinterne, administrative Informationen dürfen nicht ins Internet hochgeladen werden, z.B., um Übersetzungen in Gratistools zu erwirken;
7. Die Netiquette gemäss Anhang III ist einzuhalten.

Sämtliche Webseitenzugriffe werden automatisch protokolliert. Die Protokolldaten können von der Schule bzw. vom Kanton im begründeten Verdachtsfall personenbezogen ausgewertet werden.

6. Meldepflicht

Sicherheitsvorfälle, der Verlust bzw. Defekt von IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem schulinternen Vor-Ort-Support / IT-Verantwortlichen zu melden.

IV. Persönliche Geräte / BYOD

1. Grundsatz

Das Mitführen von persönlichen mobilen Geräten an der Schule ist grundsätzlich erlaubt.

Eine Verbindung mit dem Schulnetzwerk ist zulässig.

Die Nutzung im Unterricht erfolgt in Absprache mit der Lehrperson und der zuständigen Supportorganisation. Die Schule behält sich vor, die Nutzung im Unterricht nur zuzulassen, wenn die Geräte den kantonalen oder schulischen Vorgaben entsprechen.

2. Geräteanforderungen

Es gelten folgende Mindestanforderungen:

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

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

3. Synchronisation

E-Mails und Termine können synchronisiert werden, sofern das Gerät den kantonalen oder schulischen Vorgaben genügt.

Bei Verlust von persönlichen Geräten wird der Benutzer gesperrt. Wählen sich Dritte über dieses Gerät ins Internet ein, werden die letzten Änderungen (z.B. in SharePoint) übertragen.

4. Support

Persönliche Geräte können von der Schule eingeschränkt betreut werden, d.h. ein Vor-Ort-Support kann dafür genutzt werden. Anspruch auf weiteren Support besteht nicht.

5. Onlineprüfungen

Onlineprüfungen können gemäss den Weisungen der Schule durchgeführt werden.

V. Datenschutz

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.

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

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.

a. Bilder

Lernende und Lehrpersonen 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.

f. Bekanntgabe

Es dürfen keine schriftlichen Aufzeichnungen, grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen ohne die explizite Zustimmung der/des betroffene/n Lernenden oder Lehrperson veröffentlicht oder Dritten bekanntgegeben werden. Ebenso dürfen ohne explizite Einwilligung keine Porträts von Lernenden, Lehrpersonen oder Mitarbeitenden auf der öffentlich zugänglichen Schulwebseite veröffentlicht werden.

VI. Urheberrechte

1. Im Unterricht

a. 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.

b. Bilder

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

c. Musikaufführungen

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

1. die Aufführung durch Schulangehörige erfolgt;
2. der Anlass sich ausschliesslich an die Schüler- und Lehrerschaft sowie deren Familienangehörige richtet; und
3. der Anlass unentgeltlich ist.

d. Neukreationen

Lernende dürfen Teile von Werken zur Herstellung eigener Kreationen, seien es Texte, Bilder, Darbietungen oder Theaterstücke verwenden. Die neuen Werke dürfen der Klasse präsentiert werden.

VII. Massnahmen bei Verstössen

Bei einer missbräuchlichen Nutzung der IKT-Systeme, inkl. Urheberrechtsverletzungen, drohen den Benutzenden Massnahmen. Missbräuchlich ist die Nutzung dann, wenn sie gegen diese Nutzungsrichtlinie, weitergehende schulinterne Richtlinien und Weisungen 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 Benutzenden die Möglichkeit zur Äusserung gegeben.

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

Die Schule kann unter anderem folgende Massnahmen ergreifen:

1. Zuerst erfolgt ein persönliches Gespräch mit der Möglichkeit der Parteien, ihre Beweggründe zu nennen.
2. In der Regel erfolgt dann eine Abmahnung bzw. Verwarnung, bevor weitere Massnahmen ergriffen werden;
3. Bei Lernenden erfolgt je nach Schwere des Verstosses eine Meldung an die Inhaber der elterlichen Sorge, weitere Erziehungsberechtigte und den Lehrbetrieb;
4. Dossiereintrag
5. Bei gravierenden oder wiederholten Verstössen kann die Schule direkt Disziplinarmassnahmen gemäss der anwendbaren Schulordnung bzw. dem anwendbaren Disziplinarreglement oder Personalrecht ergreifen.
6. Die Schule kann nebst Schadenersatz auch, sofern rechtlich zulässig, die Wiederherstellung des ursprünglichen Zustands verlangen.
7. Stellt die Schule strafbares Verhalten fest, kann sie ohne Vorwarnung eine Strafanzeige einreichen bzw. eine Meldung bei der zuständigen Behörde vornehmen.

VIII. Ende der Benutzerrolle

Die Rolle als Benutzerin oder Benutzer der IKT-Systeme kann aus verschiedenen Gründen enden: 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.

Ihr Benutzerkonto wird bei Austritt deaktiviert.

Vor Ende der Benutzerrolle wird in ausreichender Frist 1 Monat 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. Der Unterstützungsbedarf sollte spätestens einen Monat vor Ende der Benutzerrolle angemeldet werden.

IX. Haftungsausschlus

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 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

Anhang II – Glossar

Amtsgeheimnis: Das Amtsgeheimnis untersagt das Offenbaren von schulischen Angelegenheiten, die im Rahmen der amtlichen oder dienstlichen Stellung wahrgenommen werden, es sei denn, es liegt ein gesetzlicher Rechtfertigungsgrund vor. Diese Schweigepflicht bleibt nach Beendigung des Arbeitsverhältnisses bestehen. Die Verletzung des Amtsgeheimnisses ist strafbar.

Anonymisierte Personendaten: Daten, die keinen Personenbezug mehr aufweisen und bei denen eine Re-Identifizierung nicht möglich ist. Bei der Schule vorhandene Personendaten dürfen für nicht personenbezogene Zwecke wie Statistiken bearbeitet werden, wenn sie anonymisiert werden.

Anwendungen: Als Anwendungssoftware (englisch «application software», kurz App) werden Computerprogramme bezeichnet, die genutzt werden, um eine nützliche oder gewünschte nicht system-technische Funktionalität zu bearbeiten oder zu unterstützen. z.B. Geschäftsanwendungen, Clouddienste, gem. IKT-Strategie Fachapplikationen, Kantonsapplikationen.

Ausschnitt eines Werkexemplars: Als Faustregel gilt, dass der zu vervielfältigende Ausschnitt 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 Einsichtgewähren, Weitergeben oder Veröffentlichen.

Benutzende: Mitarbeitende, Lehrpersonen, Lernende sowie Dritte (bspw. Kursbesuchende, Bibliotheksbenutzende, Mieter von Schulräumen, etc.), welche die Informatik-Infrastruktur der Schule benutzen.

Besondere Personendaten: Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht. Beispiel: Gesundheitsdaten, Zeugnis.

BYOD: Bring-your-own-device bezeichnet persönliche mobile Geräte, die nicht von der Schule zur Verfügung gestellt, aber zur Nutzung an der Schule zugelassen sind.

Clean Desk und Clear Screen: Grundsätze des aufgeräumten Schreibtischs («clean desk») und des leeren Bildschirms («clear screen»), d. h., bei jedem Verlassen des Arbeitsplatzes sind vertrauliche und wichtige Dokumente und Informationsträger wegzuschliessen sowie eine passwortgeschützte Bildschirmsperre (Windows: L + Windowstaste bzw. Mac: Tastenkombination [ctrl – cmd – Q]) zu aktivieren.

Ereignisprotokoll: Die Protokollierung aller Ereignisse, die Software auf dem Betriebssystem betreffen: Starten und Stoppen, Zugriff auf Dateien, Änderungen von Berechtigungen.

Grundeinstellungen: Basiskonfigurationen und Parametrisierung von IKT-Systemen, Anwendungen und Zugängen.

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

Informationen: Alle Aufzeichnungen betreffend die Ausübung einer öffentlichen Tätigkeit, ausgenommen Notizen zum persönlichen Gebrauch.

Informationssicherheit: Verantwortliche der Schule müssen dafür sorgen, dass die Informationen, die im Schulbereich bearbeitet werden, durch angemessene Massnahmen geschützt werden. Dies bedeutet beispielsweise, dass nur berechtigte Personen Zugriff und Kenntnis von Informationen erhalten. Dazu gehören auch Massnahmen, die sicherstellen, dass die Informationen zur Verfügung stehen oder verhindern, dass sie verloren gehen.

IT-Arbeitsmittel: Die den Benutzenden von der Schule zur Verfügung gestellten Geräte (statische Geräte wie Drucker, Bildschirme, PCs und mobile Geräte) und Anwendungen.

IT-Infrastruktur: Die IT-Infrastruktur umfasst Soft- und Hardwaresysteme z.B. Clients, Server, Netzwerkkomponenten, Betriebssysteme, Treiber, mobile Endgeräte.

Malware: Der Begriff Malware steht für MALicious SoftWARE – also bösartige Software. Malware dient als Oberbegriff für die Gesamtheit von Schadsoftware. Viren, Würmer, Trojaner, Adware und Spyware sind zum Beispiel 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.

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.

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.

Anhang III – Netiquette (alle)

Die Schule für Gestaltung Zürich und ihre Organisationseinheiten/Fachschaften sind im Internet und auf unterschiedlichen Social Media Kanälen präsent. Die Schule freut sich auf einen konstruktiven und respektvollen Austausch, spannende Diskussionen und Kommentare. Auch kritische Meinungen sind erwünscht. Bei der Interaktion mit der Schule im Internet und auf Social Media erklären Sie sich mit der vorliegenden Netiquette einverstanden. Sie ergänzt die Nutzungsbedingungen der Schule, die Sie akzeptiert haben.

Die Schule für Gestaltung Zürich behält sich vor, im Fall von Verstössen einzelne Beiträge ohne Angaben von Gründen zu löschen oder bei schweren und wiederholten Verstössen Benutzende von ihren Kanälen auszuschliessen.

Allgemein

1. Ich verfasse, verbreite oder poste:
    a. keine ehrverletzenden, rassistischen, diskriminierenden oder beleidigenden Beiträge oder Kommentare;
    b. keine themenfremden Beiträge oder Kommentare bzw. solche mit kommerziellen oder werbenden Inhalten (Spam);
    c. keine Beiträge von politischen und gewerkschaftlichen Organisationen;
    d. keine Beiträge oder Kommentare mit sich wiederholenden und identischen Inhalten;
    e. keine Beiträge oder Kommentare mithilfe von Bots;
2. Ich verzichte auf namentliche Nennungen von schulischen Mitarbeitenden, Lehrpersonen sowie Lernenden in öffentlichen Beiträgen;
3. Persönlichen Anfragen richte ich direkt an die zuständige Stelle der Schule;
4. Ich rufe nicht zu illegalen oder gefährlichen Handlungen oder Mobbing auf:
5. Wenn ich Mobbing bemerke, schreite ich dagegen ein oder informiere den/die Klassenlehrer/-in oder eine dafür zuständige Stelle innerhalb der Schule.

SMS/Messangerdienst/E-Mail

1. Ich versende Nachrichten nicht im Affekt, sondern lese sie noch einmal durch, um verletzende oder unangebrachte Äusserungen zu vermeiden;
2. Ich bleibe stets höflich und vermeide Beleidigungen;
3. Ich vermeide es, Konflikte online auszutragen, sondern bespreche sie mit den involvierten Personen persönlich;
4. Ich versuche, den Empfängerkreis von Nachrichten gering zu halten und richte Nachrichten nur an Personen, die tatsächlich davon betroffen sind;
5. Ich versuche, Nachrichtenverteiler regelmässig zu reduzieren;
6. Ich leite keine Kettenbriefe weiter;
7. Für grössere Empfängerkreise verwende ich stets das BCC-Feld, um die Kontaktdaten der Empfänger zu schützen.

Social Media Nutzung

1. Ich verbreite persönliche Informationen über mich mit Vorsicht;
2. Mir ist bewusst, dass ich beim Hochladen von Bildern und sonstigen Inhalten (Content) den Social Media Anbieter ggf. zur beliebigen Nutzung der Bilder/des Contents berechtige;
3. Ich bleibe auch in hitzigen Diskussionen sachlich;
4. Ich gehe nicht auf Beschimpfungen und Beleidigungen ein;
5. Ich setze Ironie und Sarkasmus mit Vorsicht ein, um Missverständnisse zu vermeiden;
6. Ich bin mir stets bewusst, an wen sich meine Mitteilung richtet, und passe meine Sprache der privaten und öffentlichen Kommunikation an;
7. Ich leite keine gefährlichen oder illegalen «Challenges» weiter.

Foto- und Videoaufnahmen

1. Ich frage vorgängig immer sämtliche abgebildeten Personen, ob sie mit einer Aufnahme einverstanden sind;
2. Ich versende, verbreite oder veröffentliche keine Aufnahme ohne vorgängige Zustimmung der abgebildeten Personen;
3. Falls mir Gewaltdarstellungen oder Aufnahmen mit verbotenem Inhalt weitergeleitet/geteilt werden, lösche ich diese und melde den Vorfall der Schule;
4. Ich beachte bei meinen Aufnahmen stets das Urheberrecht;
5. Ich versende keine Aufnahmen von mir oder von anderen an unbekannte Personen.

Videokonferenzen

1. Ich zeichne Videokonferenzen nur auf, wenn alle Beteiligten einverstanden sind;
2. Ich speichere die Videokonferenzen nur ab, wenn es notwendig und abgestimmt ist;
3. Ich zeichne nur dann Videokonferenzen auf, wenn ich als Lehrperson an der Konferenz teilnehme;
4. Mir ist bewusst, dass Chatverläufe ggf. gespeichert werden, um Mobbingvorfälle und strafbare Handlungen aufzuklären;
5. Ich nehme keine Videokonferenzen mit dem Handy auf und kopiere – ausser bei berechtigtem Anlass gemäss Ziff. 4 – keine Chatverläufe;
6. Ich darf meine Videokamera im Rahmen von Aufnahmen in Absprache ausschalten und jedenfalls meinen Hintergrund ausblenden, und ich weise andere Teilnehmende daraufhin, dass sie das ebenfalls dürfen;
7. Mir ist bewusst, dass das Einschalten der Kamera von allen Teilnehmern aus pädagogischer Sichtweise angefordert werden kann;
8. Ich respektiere die Privatsphäre von Videokonferenzteilnehmern und fordere niemanden dazu auf, mir seine/ihre privaten Räumlichkeiten zu zeigen.