TBZ
Technische Berufsschule Zürich

D5.4-03F
(Stand: Dezember 25)

Nutzungsrichtlinie für Informatikmittel an der Technischen Berufsschule Zürich

Gültig ab 08.12.2025

Inhaltsverzeichnis

1 Allgemeine Bestimmungen 3
2 Geltungsbereich 3
3 Nutzung von Informatikmittel 3
3.1 Lizenzbestimmungen für Software 3
3.1.1 Microsoft 365 4
4 Datensicherheit 4
4.1 Schutz von Zugangsdaten 4
4.2 Schutzsoftware 5
4.3 Schutz vor Kommunikation 5
5 Persönliche Geräte / BYOD 6
5.1 Grundsatz 6
5.2 Geräteanforderungen 6
5.3 Support 7
6 Nutzung 7
6.1 Nutzung im Unterricht 7
6.2 Private Nutzung von TBZ-Informatikmitteln 7
6.3 Sorgfaltspflicht 7
6.4 Netzwerk- und Internetnutzung 7
7 Unerlaubte Handlungen und Massnahmen bei Verstössen 8
8 Haftung und Haftausschluss 9
9 Anhang I – Glossar 9
10 Anhang II – Netiquette 11

1 Allgemeine Bestimmungen

An der Technischen Berufsschule Zürich werden in verschiedenen Bereichen vom Kanton Zürich bereitgestellte Informatikmittel 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 Informatikmittel zu geben. Diese Vorgaben regeln die Datensicherheit, den Datenschutz und den Umgang mit Informatikmitteln im schulischen Kontext.

2 Geltungsbereich

Die nachfolgenden Regelungen gelten für die gesamte Schule (TBZ) und für alle Benutzenden unabhängig ob mit TBZ-Geräten oder privaten Geräten gearbeitet und allenfalls ein fremdes Netz verwendet wird. Diese Nutzungsrichtline gilt für Mitarbeitende, Lehrpersonen, Lernende, Studenten, die Zugang zu Informatikmittel der TBZ haben. Die Benutzenden sind persönlich dafür verantwortlich, diese Richtlinie einzuhalten.

Mit der ersten Anmeldung oder der Nutzung der zur Verfügung gestellten Informatikmittel nehmen die Benutzenden die Nutzungsrichtline zur Kenntnis und bestätigen, über die Konsequenzen bei deren Nichtbeachtung informiert worden zu sein.

3 Nutzung von Informatikmittel

An der Technischen Berufsschule Zürich (TBZ) werden Informatikmittel verwendet, die von der Schule und / oder vom Kanton Zürich bereitgestellt bzw. verwaltet werden. Die Informatikmittel umfassen alle Systeme, inkl. Netzwerk und Zugang zum Internet sowie Programme oder Applikationen, die von der Schule zur Verfügung gestellt werden. Darüber hinaus werden Bring Your Own Devices (BYOD) gemäss Absatz 5 zur Nutzung an der Schule zugelassen. Andere Informatikmittel, welche diesen Kriterien nicht entsprechen, sind zur Nutzung an der Schule nicht zugelassen.

Die Benutzenden behandeln die Informatikmittel mit Sorgfalt und schützten sie vor Diebstahl und Beschädigung. Räume, die Informatikmittel enthalten, sind beim Verlassen, wenn es der Schulalltag erlaubt, abzuschliessen.

Diese Nutzungsrichtlinie bezweckt, den Benutzenden verständliche und nachvollziehbare Vorgaben zum korrekten Umgang mit den Informatikmittel zu geben.

3.1 Lizenzbestimmungen für Software

Jede an der TBZ eingesetzte kommerzielle Software ist für Schulzwecke lizenziert. Diese darf ohne rechtmässige Autorisierung weder kopiert noch weitergegeben werden. Im Weiteren ist es untersagt, zusätzliche Software ohne ausdrückliche Einwilligung der Lehrperson auf den TBZ-Systemen zu installieren. Nach Austritt aus der TBZ darf die zur Verfügung gestellte Software nicht mehr weiterverwendet werden.

3.1.1 Microsoft 365

Microsoft 365 Anwendungen werden von der Schule kostenlos zur Verfügung gestellt. Nach Austritt aus der TBZ wird das Benutzerkonto sowie die E-Mail-Adresse (*.tbz.ch) gelöscht und die Programme können nicht mehr genutzt werden. Die Daten welchen auf OneDrive, MS-Teams usw. gespeichert wurden, werden mit dem Austritt ebenfalls unwiderruflich gelöscht. Die persönlichen schulischen Unterlagen müssen deshalb vorgängig privat abgespeichert werden.

4 Datensicherheit

4.1 Schutz von Zugangsdaten

Sämtliche Zugangsdaten für Informatikmittel sind geheim zu halten. Gehen Zugangsdaten verloren oder besteht ein Verdacht auf Missbrauch, muss der/die betroffene(n) Benutzer/-in umgehend eine Meldung beim Informatikdienst (helpdesk@tbz.ch) vornehmen.

a. Benutzerkonto

Der Zugang zur Nutzung der Informatikmittel erfolgt über einen Benutzernamen und ein Passwort. Wenn möglich, wird als zusätzlichen Schutz eine Zwei-Faktor-Authentifizierung angewendet.

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 ihr Gerät verlassen.

b. Passwortschutz

Die Benutzenden sind verpflichtet, für sämtliche Geräte und Zugänge starke Passwörter zu wählen. Für jeden Zugang ist ein separates, starkes und einzigartiges Passwort zu wählen.

Beim Festlegen eines neuen Passworts sind folgende Vorgaben einzuhalten:

Passwortanforderungen

- Das Passwort muss **mindestens 12 Zeichen** lang sein.
- Es muss **vier verschiedene Zeichenarten** enthalten:
  - **Grossbuchstaben** (A, B, C, …)
  - **Kleinbuchstaben** (a, b, c, …)
  - **Ziffern** (0, 1, 2, …)
  - **Sonderzeichen** (+, =, %, …)

Gültigkeit und Wiederverwendung

- Das Passwort muss **alle 365 Tage** gewechselt werden.
- Es darf **nicht mit einem der letzten zehn Passwörter identisch** sein.

Verbotene Authentifizierungsmerkmale

Folgende Arten von Passwörtern sind **nicht zulässig**:

- **Kompromittierte Merkmale** (z. B. aus Datenlecks bekannte Passwörter)
- **Einfache Muster** (z. B. *abcdefgh*, *123456*)
- **Kontextspezifische Begriffe** (z. B. *Kanton*, *Zürich*, *Verwaltung*)
- **Personenbezogene Angaben** (z. B. Geburtsdatum)
- **Benutzer- oder servicebezogene Daten** (z. B. eigene Anmeldedaten)

Damit Passwörter sicher verwaltet werden können, stehen verschiedene Programme, sogenannte Passwortmanager, zur Verfügung. Weitere Informationen und Empfehlungen können dem Merkblatt des DSB entnommen werden. Die an der Schule verwendeten Passwörter dürfen nicht für private Zugänge verwendet werden.

4.2 Schutzsoftware

Die TBZ bzw. der Informatikdienst (ID) schützt alle Systeme, welche in der Verantwortung des ID liegen vor Malware und vor Computerviren. Werden private Informatikmittel - BYOD-Geräte - mit dem TBZ-Netz verbunden, sind die Benutzenden gehalten, die ergänzenden Schutzvorschriften zu berücksichtigen:

1. Schutzsoftware darf nicht umgangen oder deaktiviert werden.
2. Es muss sichergestellt sein, dass die eingesetzten Informatikmittel vom Hersteller unterstützt (supported) und sämtliche offiziellen Aktualisierungen / Updates installiert werden.
3. Persönliche Geräte müssen grundsätzlich über eine aktive und aktuelle Schutzsoftware verfügen.
4. Verdächtige E-Mails müssen umgehend gelöscht und als Spam gemeldet werden, bei einer Häufung solcher Fälle hat eine Meldung beim Informatikdienst (helpdesk@tbz.ch) 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, unbekannte Wechselmedien an die Systeme der Schule angeschlossen werden.
8. Auffälligkeiten und konkrete Verdachte müssen umgehend an den Informatikdienst (helpdesk@tbz.ch) gemeldet werden.

4.3 Schutz vor Kommunikation

a. E-Mail

Die Benutzenden erhalten ein eigenes E-Mail-Konto mit einer E-Mail-Adresse der Schule. Das E-Mail-Konto dient für:

- Die Korrespondenz im Zusammenhang mit dem Schulbetrieb.
- Empfang von allgemeinen Informationen und Weisungen der Schule bzw. des Kantons.
- Organisation des Klassenbetriebs

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

1. Die Benutzenden sind für die Bewirtschaftung ihres Postfachs verantwortlich.

2. Vertraulich und höher klassifizierte Nachrichten müssen verschlüsselt und falls möglich, signiert versendet werden.
3. E-Mails dürfen grundsätzlich 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-Mail-Adresse darf nicht für private Korrespondenz oder nicht schulbezogene Angebote und Online-Services (Newsletter, Abonnemente, Streamingdienste, Onlineshopping, etc.) genutzt werden.

b. Collaboration Tools

Im Zusammenhang mit der Nutzung von Anwendungen zur Zusammenarbeit wie bspw. Microsoft Teams (sog. Collaboration Tools) gelten folgende Bestimmungen / 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 Informationen sind End zu End verschlüsselt auszutauschen.
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 Persönliche Geräte / BYOD

5.1 Grundsatz

Das Mitführen und Verwenden von persönlichen Informatikmittel bspw. von Notebooks und mobilen Geräten an der Schule ist grundsätzlich gewollt und erlaubt.

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. Für die Trennung von geschäftlichen, schulischen und privaten Daten sind die Benutzenden selbst verantwortlich.

5.2 Geräteanforderungen

Es gelten folgende Mindestanforderungen:

- Passwort- oder PIN-Schutz
- Installation eines aktuellen Virenschutzes
- Aktuelle Firewall
- Aktuelle und durch den Hersteller unterstützte Betriebssysteme (Sicherheitsupdates und Support muss gewährleistet sein)
- Regelmässige Updates (Firewall, Betriebssystem, Virenschutz und Applikationen)

- Verschlüsselung vertraulicher Daten bei der Speicherung und Übermittlung

Für den Unterricht darf auch auf privaten Geräten nur lizenzierte Software verwendet werden. Die Benutzenden sind selbst für ihre Geräte verantwortlich (Diebstahlschutz, Versicherung, etc.).

5.3 Support

Für persönliche Geräte besteht grundsätzlich kein Supportanspruch. Bei Problemen kann der Informatikdienst (helpdesk@tbz.ch) kontaktiert werden und dieser versucht den Benutzenden - soweit dies möglich ist - Hilfestellung zu leisten. Für fachgerechte Entsorgung (u.a. korrekte Datenlöschung) und Reparatur von persönlichen Geräten sind die Benutzenden selbst zuständig. Datenträger können beim Informatikdienst zur fachgerechten Entsorgung, abgegeben werden.

6 Nutzung

6.1 Nutzung im Unterricht

Im Unterricht dürfen Informatikmittel (TBZ und private) ausschliesslich für den Unterricht gebraucht werden und die Anweisungen der Lehrperson sind strikte zu befolgen. Private Geräte dürfen im Unterricht auch die Infrastruktur der TBZ verwenden. Das betrifft insbesondere Netzwerk, Drucker, WLAN und Internet.

6.2 Private Nutzung von TBZ-Informatikmitteln

Eine Nutzung der TBZ-Informatikmittel für private Anwendungen ist nur mit ausdrücklicher Erlaubnis der Lehrperson gestattet.

6.3 Sorgfaltspflicht

Störungen von Informatikmitteln können den Unterricht massiv behindern. Bei allen Informatikmitteln wird darum ein sorgfältiger Umgang verlangt. Private Geräte dürfen keine Störungen verursachen. Werden Beschädigungen an TBZ-Informatikmitteln festgestellt, so sind diese sofort der Lehrperson zu melden. Die Benutzenden sind selbst für ihre Daten verantwortlich.

6.4 Netzwerk- und Internetnutzung

Das Schulnetzwerk steht den Benutzenden via einem 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:

- Streaming Dienste sowie Up- und Downloads von grossen Dateien sind zu verhindern, insbesondere die Installationen von Spielen und grossen Audio- und Videodateien aus dem Internet.
- Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden.

7 Unerlaubte Handlungen und Massnahmen bei Verstössen

Als unerlaubte Handlungen gelten insbesondere (nicht abschliessend):

- Besuch des Darknets oder von Webseiten mit folgenden Inhalten: 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.
- Illegales Kopieren und Downloads von Software (Verletzung von Urheberrecht, Lizenzbestimmungen).
- Belastung des Schulnetzes durch die Nutzung von Streaming Diensten sowie Up- und Downloads von grossen Dateien.
- Störung des Betriebes durch unerlaubte Manipulationen an Informatikmittel.
- Störung des Betriebes durch Malware oder andere schädliche Programmelemente (Scripts, etc.).
- Eindringen in geschützte Bereiche und Diebstahl von Daten.
- Bild- und Tonaufnahmen im Schulbereich ohne Bewilligung und deren Publikation.

Bei unerlaubten Handlungen oder bei einer missbräuchlichen Nutzung der Informatikmittel 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.

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

Die Schule kann unter anderem folgende Massnahmen bei Verstössen 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. Bei gravierenden oder wiederholten Verstössen kann die Schule direkt Disziplinarmassnahmen gemäss der anwendbaren Schulordnung bzw. dem anwendbaren Disziplinarreglement oder Personalrecht ergreifen.
5. Die Schule kann nebst Schadenersatz auch, sofern rechtlich zulässig, die Wiederherstellung des ursprünglichen Zustands verlangen.
6. Stellt die Schule strafbares Verhalten fest, kann sie ohne Vorwarnung eine Strafanzeige einreichen bzw. eine Meldung bei der zuständigen Behörde vornehmen.

8 Haftung und Haftausschluss

Die Benutzenden haften für von ihr/ihm vorsätzlich oder grobfahrlässig verursachte Schäden oder Veränderungen an Informatikmitteln der TBZ oder für mit Informatikmitteln der TBZ verursachte Schäden innerhalb und ausserhalb der Schule. Die Schäden, beziehungsweise deren Beseitigung, werden dem Verursacher in Rechnung gestellt. Soweit die Rechtsordnung dies zulässt, schliesst die Schule jede Haftung für Schäden durch Benutzerhandlungen aus. Die Schule haftet ausserdem nicht für Schäden, die den Benutzenden aus ihrer Missachtung dieser Nutzungsrichtlinie und des anwendbaren Datenschutzrechts sowie der Missachtung der kantonalen AISR (Allgemeine Informationssicherheitsrichtlinie) und anwendbaren BISR (Besonderen Informationssicherheitsrichtlinien) entstehen.

9 Anhang I – Glossar

AISR: Allgemeine Informationssicherheitsrichtlinie des Regierungsrates Link

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, Fachapplikationen, Kantonsapplikationen.

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

BISR: Besondere Informationssicherheitsrichtlinien für die kantonale Verwaltung Link

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.

Informatikmittel: IT-Infrastruktur (Soft- und Hardwaresysteme z.B. Clients, Server, Netzwerkkomponenten, Betriebssysteme, Treiber, mobile Endgeräte; BYOD) und Plattformen/Middleware sowie von der Schule zur Verfügung gestellte Geräte (statische Geräte wie Drucker, Bildschirme, PCs und mobile Geräte) inklusive Software und Anwendungen.

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.

Passwortmanager: Anwendung, mit deren Hilfe Zugangsdaten verschlüsselt gespeichert und verwaltet werden können.

Starkes Passwort: Starke Passwörter sind mindestens 8 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. Unter http://www.passwortcheck.ch kann die Sicherheit eines Passworts überprüft werden.

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, externe Festplatten (HDD/SSD), welche kabelgebunden, kabellose, physischen und logischen mit Informatiksystemen verbunden werden können.

Zugang: Mit Zugang wird die Nutzung von Informatikmittel, insbesondere System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person oder einem System, bestimmte Ressourcen zu nutzen.

Zugangsdaten: Zugangsdaten erlauben es den Benutzenden, Zugang zu den Informatikmittel zu erhalten. Es kann sich dabei um Benutzernamen, Zahlen-PINs, Passwörter und weitere Angaben handeln.

10 Anhang II – Netiquette

Die Schule TBZ 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 sich die Benutzenden mit der vorliegenden Netiquette einverstanden.

Die Schule TBZ 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 Kontakt-daten 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.