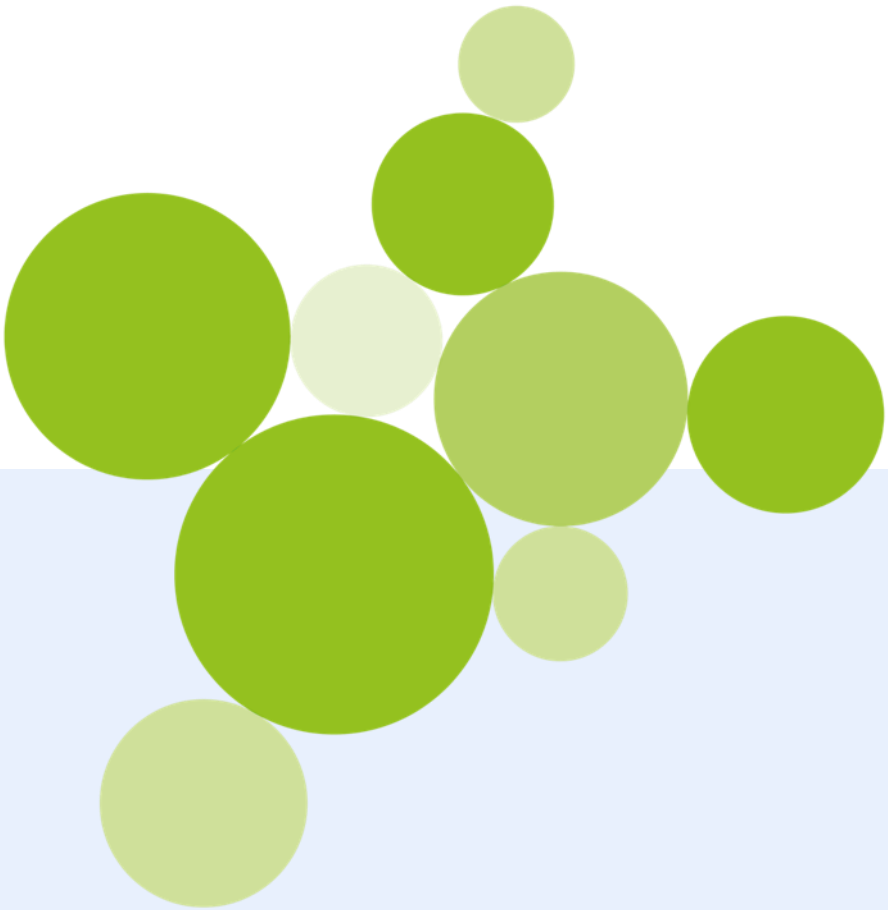
BBW Berufsbildungsschule Winterthur
Rektorat

Nutzungsrichtlinie Informations- und Kommunikations-Technologie

NRL IKT

Version 09.2025



Inhalt

Diese Nutzungsrichtlinie ist nicht als Vertrag zu verstehen, den die Nutzenden aktiv akzeptieren müssen, sondern sie muss lediglich zur Kenntnis genommen werden. Wird die Richtlinie nicht akzeptiert, hat dies keine Auswirkungen auf ihre Wirksamkeit.

Die Schulleitung der Berufsbildungsschule Winterthur (BBW) beschliesst gestützt auf die im Kapitel 8 aufgeführten gesetzlichen Grundlagen:

1 Allgemeine Bestimmungen

1.1 Zweck und Grundlagen

An dieser Schule werden vom Kanton Zürich bereitgestellte Systeme der Informations- und Kommunikationstechnologie (IKT)1 sowie private Geräte (BYOD – Bring Your Own Device) im Unterricht und in der Arbeitsorganisation eingesetzt.

Ziel der Richtlinie ist es, den sicheren Betrieb der IKT-Systeme zu gewährleisten und klare Nutzungsvorgaben in den Bereichen Datenschutz, Datensicherheit und im Umgang mit urheberrechtlich geschützten Inhalten im schulischen Kontext zu definieren.

IKT umfasst alle Technologien, die zur Verarbeitung, Speicherung, Übertragung und Darstellung von Informationen an der BBW verwendet werden. Dazu gehören sowohl Hardware (Bsp. Computer und Netzwerke) als auch Software (Bsp. Anwendungen und Betriebssysteme).

Die IKT-Systeme und Anwendungen sind primär auf schulische oder institutionelle Zwecke ausgerichtet. Ein sorgsamer und verantwortungsvoller Umgang mit diesen Systemen gewährleistet einen störungsfreien Betrieb und kommt allen Benutzenden zugute. Private Nutzung ist zulässig, sofern sie im Rahmen der Lizenzbedingungen bleibt. Ressourcenschwere Aktivitäten (z. B. Mining) sowie kommerzielle Nutzungen sind untersagt.

1.2 Geltungsbereich

Diese Nutzungsrichtlinie betrifft alle Nutzenden von Informations- und Kommunikations-Technologie an der BBW.
Sie richtet sich somit an alle, die in irgendeiner Form IKT an der BBW einsetzen.
Dazu gehören:
- Lernende und Lehrende
- Schulleitung und Schulverwaltung
- Supportorganisationen und Dienste
- Aufsichtsgremien
- Gäste
- weitere

Die in dieser Richtlinie verwendeten Fachbegriffe orientieren sich an den kantonalen Vorgaben.

Eine Nutzung der BBW IKT-Systeme ist gegeben, sobald mindestens ein IKT-System der BBW in eine Nutzung involviert ist. (Bsp. WLAN, Dateiablage, Leihgeräte, Drucker…)
Diese ist insbesondere auch der Fall, wenn private IKT-Systeme im Zusammenspiel mit IKT-Systemen der BBW verwendet werden. (Bsp. Privates Mobile am WLAN der BBW)

1.3 Auswertung von Randdaten

Bei der Nutzung der IKT-Systeme fallen Randdaten in Logfiles verschiedener Komponenten (z. B. Firewall, Server, Anwendungen) an. Zur Erkennung und Rückverfolgung von Sicherheitsvorfällen können die Schule und der Kanton Zürich innerhalb der gesetzlichen Frist auf diese Logfiles zurückgreifen. Standardisierte, anonymisierte Auswertungen werden regelmässig durchgeführt, um die Sicherheit und Verfügbarkeit der Systeme zu gewährleisten. Sollten detaillierte,

[1] Es umfasst alle Technologien, die zur Verarbeitung, Speicherung, Übertragung und Darstellung von Informationen an der BBW verwendet werden. Dazu gehören sowohl Hardware (wie Computer und Netzwerke) als auch Software (wie Anwendungen und Betriebssysteme).

personenbezogene Auswertungen notwendig werden, werden die betroffenen Nutzerinnen und Nutzer informiert.

2 Nutzung von privaten und kantonalen IT-Arbeitsmitteln

2.1 Bestimmungen

Die Nutzenden behandeln die BBW IKT-Systeme mit Sorgfalt und schützen sie vor Beschädigung und Diebstahl.
BBW IKT-Systeme werden, sofern sie unbeaufsichtigt sind, für Unbefugte nicht zugänglich aufbewahrt. (Z.B. in abschliessbaren Schränken oder Räumen).

An den BBW IKT-Systemen dürfen nur Anpassungen oder Änderungen vorgenommen werden, die den ordnungsgemässen funktionierenden, integren und sicheren Betrieb der IKT-Systeme nicht beeinträchtigen.
Die Möglichkeit zur Anpassung oder Änderung hängt von der Kompetenz und der Rolle der nutzenden Person ab.

Eine private Nutzung der BBW IKT-Systeme ist erlaubt.
Die Nutzung der BBW IKT-System für die Zwecke der BBW haben immer Vorrang und dürfen durch die private Nutzung nicht beeinträchtigt werden.

Die Entsorgung ausgedienter oder defekter kantonaler IT-Arbeitsmittel sowie deren Reparatur oder Austausch erfolgt in Abstimmung mit dem technischen IKT-Support der BBW.

Die Nutzung von privaten IKT-Systemen sind an der BBW erlaubt.
Oft werden private IKT-Systeme wie Laptops unter dem Begriff BYOD eingeordnet.
In den meisten der an der BBW zu unterrichtenden Berufen besteht eine BYOD-Vorgabe, wodurch Lernende verpflichtet sind, mit einem eigenen Gerät zu arbeiten.
Zudem definieren diese Berufe technische Mindestanforderungen an die BYOD.
Das Nutzen von privaten IKT-Systemen darf den Betrieb der BBW IKT-Systeme nicht beeinträchtigen.

Es gelten folgende Mindestanforderungen:

- Passwort- oder PIN-Schutz
- regelmässige Updates

2.2 Synchronisation

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

2.3 Support

Für den Support der BBW IT-Systeme sind der didaktisch-pädagogische und der technische IKT-Support der BBW sowie der Service Desk des Digitalen Service Centers SekII zuständig – die entsprechenden Kontaktangaben und Nutzungsvorgaben sind im Intranet der BBW zugreifbar.

Private Geräte (BYOD-Geräte) können von der Schule eingeschränkt betreut werden.

Nutzende der BBW-IKT-Systeme können zu den vorgegebenen Öffnungszeiten das Supportangebot des technischen IKT-Supports der BBW in Anspruch nehmen.

Der Support hat einen eingeschränkten Umfang. Der technische IKT-Support wird die jeweilige Anfrage entsprechend einordnen.

3 Datensicherheit

Datensicherheit umfasst den Schutz aller Daten vor unbefugtem Zugriff, Verlust oder Beschädigung. Sie konzentriert sich auf die technischen und organisatorischen Massnahmen, um die Integrität, Vertraulichkeit und Verfügbarkeit von Daten zu gewährleisten.
Abgrenzung Datenschutz und Datensicherheit:

- Datenschutz:
  - Schutz persönlicher Daten und Privatsphäre (gegenüber Dritten).
  - Schutz der Daten, die nur für schul-internen Gebrauch bestimmt sind (gegenüber Dritten).
- Datensicherheit:
  - Schutz der Daten vor technischen und physischen Bedrohungen.

3.1 Externe Datenablagen

Diese Systeme werden nicht von der BBW zur Verfügung gestellt und nicht durch den TIKTS verwaltet.

Die Nutzung von externen Datenablagen kann für Schule und Lernende **erhebliche Risiken** mit sich bringen. Es ist wichtig, diese Gefahren zu kennen, um bewusst und verantwortungsvoll mit Daten umzugehen.

Mögliche Gefahren:

- Eine unberechtigte Person erhält Zugang zu Daten oder Informationen, die nicht für sie bestimmt sind.
  Schon unscheinbare Geräte (z. B. USB-Kabel mit versteckten Accesspoints) können Dritten Zugang zu Systemen verschaffen.
- Der Anbieter bietet keine oder nur ungenügende Datensicherung.
- Daten werden durch den Anbieter oder Dritte ausgewertet, verarbeitet oder weiterverbreitet.
- Der Anbieter unterliegt nicht dem Schweizer Datenschutzgesetz und erfüllt die Anforderungen an den Datenschutz nicht.
- Eine unberechtigte Person kann ein verbundenes IKT-System beeinträchtigen oder manipulieren.

Besondere Vorsicht gilt bei:

- allen nicht von der BBW betreuten IKT-Systemen (z. B. fremde USB-Sticks, externe Datenspeicher, Tastaturen, fremde WLAN-/LAN-Netze)
- der Nutzung von öffentlichen WLANs

Wenn immer möglich, müssen die Datenablagen der BBW genutzt werden.

3.2 Schutz von Zugangsdaten

Alle Zugangsdaten der schulischen IKT-Systeme und von Lerntechnologien sind streng vertraulich zu behandeln. Bei Verlust oder Verdacht auf Missbrauch ist sofort der technische IKT-Support der BBW zu informieren.

a. Benutzerkonto

Das BBW-Benutzerkonto ermöglicht den Zugriff auf die IKT-Systeme der BBW. Der Zugang erfolgt mit Benutzername und Passwort – bei M365 zusätzlich mit Zwei-Faktor-Authentifizierung.
Das Konto ist persönlich, darf nicht weitergegeben werden und jeder/jede Nutzer/in trägt die Verantwortung für alle Aktivitäten. Bei Verdacht auf Missbrauch kann das Konto ohne Vorwarnung gesperrt werden. Zudem ist ein ordnungsgemässes Abmelden von allen Systemen erforderlich, wenn diese nicht mehr genutzt werden.

b. Passwort

Für jeden Zugang ist ein starkes, individuelles Passwort zu wählen, das ausschliesslich für schulische Zwecke verwendet wird. Eine weitere Möglichkeit sind passwortlose Authentifizierungen mit Schlüsselverfahren oder biometrische Authentifizierung.
Besteht der berechtigte Verdacht, dass ein Passwort kompromittiert wurde, ist es umgehend zu ändern.

c. Mail-Adresse

Lehrpersonen und Lernende loggen sich in die IKT-Systeme der BBW oder in freigegebene Lerntechnologien in der Regel mit ihrer BBW-Schul-E-Mail-Adresse ein. Bei Unklarheiten sind der technische oder didaktisch-pädagogische IKT-Support, interne Informationsquellen oder die Info-Seiten des Digitalen Service Centers (MBA) zu konsultieren. Lernende informieren sich bei der Schulleitung oder den Lehrpersonen über die zu verwendende E-Mail-Adresse und die damit verbundene Datennutzung.

d. Mehr-Faktor-Authentifizierung (MFA)

Bei Anwendungen, die dies ermöglichen, sollte zwingend eine Mehr-Faktor-Authentifizierung eingesetzt werden. Alternativ kann der Zugang durch E-Mail- oder SMS-Verifizierungscodes oder andere passwortlose Authentifizierungsangebote zusätzlich abgesichert werden.

3.3 Schutz von Informationen

Mitarbeitende und Lehrpersonen unterstehen dem Amtsgeheimnis.
Benutzende der IKT-Systeme und Lerntechnologien müssen dafür sorgen, dass schulinterne Informationen – also solche, die den Schulbetrieb und den Unterricht betreffen – nicht offengelegt, entwendet, gelöscht oder unkenntlich gemacht werden.

a. Datensicherung

Die BBW stellt den Nutzenden Systeme für die Datenablage zur Verfügung.
Schulinterne, administrative Informationen (nicht Unterrichtsmaterialien) müssen auf den von der Schule bzw. dem Kanton bereitgestellten Datenablagen (z. B. Schulserver, Nextcloud, OneDrive, Teams, SharePoint, OpenOlat) gespeichert werden, um eine zentrale Sicherung und Verfügbarkeit zu gewährleisten.

Für die Sicherung von Daten, die nicht auf den obigen Systemen abgelegt werden, ist der Nutzende selbst verantwortlich. Beim Nutzen von externen Datenablagen ist das Kapitel 3.1 zu beachten.

Ausnahmen
Im Schulalltag kommt es vor, dass für bestimmte Daten zeitweise Ablagen von **externen Anbietern** genutzt werden.
Langfristig ist es das Ziel, diese durch die **offiziellen Datenablagen der BBW** zu ersetzen.
Ausnahmen können sein, dass bestimmte Programme unter Einhaltung der geltenden Datenschutzbestimmungen für die Datenablage genutzt werden dürfen. Ebenso können Unterrichtsmaterialien schulübergreifend auf externen Datenablagen gespeichert und ausgetauscht werden, sofern dies begründet ist und die datenschutzrechtlichen Vorgaben eingehalten werden.

b. Berechtigungen

Der Zugriff auf nicht öffentliche Daten der BBW ist bei den IKT-Systemen über ein Zugriffsbeschränkung eingeschränkt.
Die BBW definiert in einem Rollenkonzept die Zugriffsbeschränkungen.
Rollen können einzelne Nutzende oder auch Gruppen von Nutzenden innehaben.
Daten werden gemäss diesem Rollenkonzept auf den IKT-Systemen abgelegt. Erhält eine Person

Zugriff auf Informationen, die nicht für sie bestimmt sind, ist dies umgehend dem Ersteller der Daten resp. der vorgesetzten Stelle mitzuteilen.

c. Schutzstufen

Im schulischen Umfeld werden Dokumente erstellt, die unterschiedliche Arten von Informationen enthalten – von allgemeinen Lehrmaterialien bis hin zu sensiblen personenbezogenen Daten.
Die folgende Übersicht zeigt die Kategorien, Klassifizierungen und Schutzstufen sowie eine konsolidierte Tabelle zur besseren Veranschaulichung.

Kategorien:

- **Sachdaten:** z. B. Lehrmittel, Prüfungen, Unterrichtsfolien
- **Personendaten:** z. B. Name, Adresse, Noten, Lernprofile
- **Besondere Personendaten:** z. B. Zeugnisse, Persönlichkeitsprofile, disziplinarische Bewertungen

3.4 Klassifizierung

Klassifizierungen: öffentlich, intern, vertraulich, geheim
Schutzstufen: Grundschutz, Erhöhter Schutz

Wo es sinnvoll erscheint, können Daten mit einer Klassifizierung *öffentlich, intern, vertraulich, geheim* gekennzeichnet werden.
Eine Klassifizierung ist eine Information und keine eigentliche Kontrolle.
Die Kontrolle geschieht durch die Selbstverantwortung der nutzenden Person.
Deshalb ist die Deklaration des Kreises der Nutzenden oder einer Rolle einer Gruppe von Nutzenden der reinen Klassifizierung vorzuziehen oder die Klassifizierung mit dem Kreis der Nutzenden oder einer Rolle einer Gruppe von Nutzenden zu ergänzen.

Dokumente mit Sachdaten sind an den dafür vorgesehenen Orten der IKT-Systeme abzulegen.
Dokumente mit besonderen Personendaten dürfen nicht geteilt oder nur mit einem eingeschränkten Personenkreis geteilt werden.

Wichtig: Bei besonderen Personendaten übernimmt in der Regel die Schulverwaltung, sprich die Abteilungssekretariate, die Organisation und sichere Aufbewahrung.

Konsolidierte Tabelle:

Datenkategorie	**Beispiele**	**Typische Klassifizierung**	**Empfohlene Schutzstzufe**
Sachdaten	Lehrmittel, Prüfungen, Unterrichtsfolien	Öffentlich oder Intern	Grundschutz
Personendaten	Name, Adresse, Noten, Lernprofile	Intern	Grundschutz bis erhöhter Schutz (je nach Sensibilität)
Besondere Personendaten	Zeugnisse, Persönlichkeitsprofile, disziplinarische Bewertungen	Vertraulich bis geheim	Erhöhter Schutz

Definition Schutzstufe:

Kategorie	Zugriff	Speicherung	Übermittlung
Grundschutz *(allgemeine Schul-, Abteilungsdokumente und nicht personenbezogene Sachdaten, z. B. BBW-Informationen, Formulare, Vorlagen, Unterrichtsmittel)*	Leserechte innerhalb der gesamten Schule oder Organisationseinheit. Verantwortlichkeiten sind definiert.	Ablage im offiziellen Cloud-Bereich mit einheitlicher Ordnerstruktur und klaren Dateinamen.	Interne Weitergabe erlaubt. Externe Weitergabe nur bei klarer Zweckbindung, Einhaltung der Datenschutzvorgaben und geklärtem Urheberrecht.
Erhöhter Schutz *(sensiblere Personendaten, z. B. Notenlisten, Teilnehmendenübersichten)*	Zugriff nach Rolle oder Funktion („Need-to-know“); Rechte werden periodisch überprüft.	Separater Bereich für sensible Daten. Lokale Kopien vermeiden. Klare Aufbewahrungs- und Löschregeln.	Weitergabe nur an namentlich bekannte Personen oder Gruppen, idealerweise mit zeitlich eingeschränktem Zugriff (z.B. manuelles Entfernen des Links nach Projektende).
Hoher Schutz *(besondere Personendaten, z. B. Zeugnisse, Disziplinarfälle)*	Zugriff nur für klar definierte Rollen oder Personen; temporäre Freigaben nur bei Bedarf.	Separater Speicherbereich mit beschränktem Zugriff (z.B. interner Server oder geschützter Cloud-Ordner). Lösch- und Aufbewahrungsfristen sind festgelegt.	Keine offenen Links. Weitergabe nur nach Absprache und Dokumentation mit Angabe von Empfänger, Zweck und Umfang.

d) Bekanntgabe von Informationen
Schulinterne Informationen dürfen nur auf einer gesetzlichen Grundlage oder mit ausdrücklicher Einwilligung der betroffenen Person weitergegeben werden. Im Zweifelsfall entscheidet die Schulleitung.

e) Sorgfaltspflichten
Es gilt eine strikte Clean-Desk- und Clear-Screen-Policy (z. B. automatische Bildschirmsperre via Win+L oder [ctrl-cmd-Q] bei Macs). Physische Träger von Informationen wie Wechselmedien oder Papier dürfen nicht unbeaufsichtigt bleiben. Whiteboards und Wandtafeln, auf denen sensible Daten stehen, müssen nach Gebrauch gereinigt werden. Defekte oder Störungen an bereitgestellten IT-Arbeitsmitteln sind sofort dem technischen IKT-Support der BBW zu melden.

Der Zutritt zu nicht-öffentlichen Räumen ist ausschliesslich autorisierten Personen gestattet. Auch herkömmliche Daten und Räume können sensible Informationen offenbaren, wenn sie nicht ausreichend geschützt sind. Daher ist es wichtig, stets aufmerksam zu sein und bei ungewöhnlichen Aktivitäten oder unbefugtem Zutritt umgehend zu melden, um den Schutz aller Daten sicherzustellen.

3.5 Schutz vor Malware

IKT-Systeme müssen mit entsprechend ihren Möglichkeiten mit Schutzsoftware ausgestattet werden.

1. Schutzsoftware darf nicht mutwillig umgangen werden.
2. Soweit die Möglichkeit besteht, müssen immer sämtliche offiziellen Aktualisierungen und Updates installiert werden, insbesondere die des Virenschutzes.
3. Selbst einfache USB-Kabel können als Zugangspunkte für Dritte dienen und sensible Daten offenlegen; daher sollten nur vertrauenswürdige, von der BBW betreute Geräte genutzt, alle Malware-Schutzmassnahmen eingehalten und bei Unsicherheiten der technische IKT-Support der BBW gefragt werden – besonders bei der Nutzung von privaten Geräten (BYOD), USB-Sticks, externen Datenspeichern, Tastaturen, öffentlichen WLAN oder nicht autorisierten bzw. bewilligten Wechselmedien.
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.

Auffälligkeiten und konkrete Verdachte müssen umgehend dem TIKT-Team der BBW gemeldet werden.

3.6 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 ausschliesslich der Korrespondenz im Zusammenhang mit der Schule.

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

Die Benutzenden sind für die Kontrolle und Pflege ihres Postfachs verantwortlich.

Vertraulich und höher klassifizierte Nachrichten müssen verschlüsselt und signiert versendet werden oder die entsprechenden Daten werden auf Systemen mit Zugangssicherung abgelegt.

- E-Mails dürfen nicht an externe (private oder geschäftliche) Postfächer weiter- oder umgeleitet werden.
- Bei E-Mails an grössere Gruppen wird stets das BCC-Feld genutzt, um die Kontaktdaten zu schützen.

b. Collaboration Tools

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

- Die Nutzende verwenden für die Zusammenarbeit und den Austausch nur die von der Schule zur Verfügung gestellten Collaboration Tools.
- Kanäle, die nicht mehr benutzt werden, werden gelöscht.
- 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.

Vertrauliche oder höher klassifizierte Informationen sind– sobald sie den Microsoft EDU-Tenant der BBW verlassen - End-zu-End verschlüsselt auszutauschen, egal ob im Chat, Kanal oder im Videoanruf.

Für Gespräche, die vertrauliche oder höher klassifizierte Informationen enthalten und mit Organisationen ausserhalb des kantonalen Netzwerks geführt werden (z. B. Lehrbetriebe, externe Amtsstellen), muss die externe Organisation den entsprechenden Chatlink erstellen und versenden.

- Collaboration-Tools müssen über einen End-zu-End-Verschlüsselung verfügen.

Chats sind dazu bestimmt, sich auszutauschen. Vertrauliche und höher klassifizierte Daten und Dokumente dürfen nicht dort, sondern in dafür bestimmte Speicher abgelegt und in den Chats und Social Media nur referenziert / verlinkt werden.

- Der Empfängerkreis wird bewusst klein gewählt, sodass nur Personen kontaktiert werden, die betroffen sind.

3.7 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 umfangreichen, nicht unterrichts- oder schulbezogenen Dateien sind zu vermeiden.
   Die Nutzenden der BBW-IKT-Systeme dürfen den Betrieb dieser IKT-Systeme nicht unangemessen beeinträchtigen. Bsp umfangreiche Downloads, Streaming ...
2. Die Sicherheitsmassnahmen des Netzwerkes dürfen nicht bewusst und mutwillig umgangen werden. (Bsp. VPN, Proxy)
3. Der Besuch von Webseiten, ausserhalb des Grundauftrages der Schule, 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.
4. Informationen der Schule dürfen nur anonymisierte auf Internet-Dienste ausserhalb der Schule geladen werden (Bsp. Übersetzung-Tools).

Alle Beteiligten sind verpflichtet, in digitalen Interaktionen stets respektvoll, sachlich und konstruktiv zu agieren, diskriminierende oder beleidigende Inhalte zu vermeiden, den Datenschutz zu wahren und Spam sowie werbende Inhalte zu unterlassen.

3.8 Arbeiten von unterwegs oder zu Hause

Beim Arbeiten von unterwegs muss der Bildschirm vor den Blicken Dritter geschützt sein (Sitzplatz entsprechend wählen, Sichtschutzfolie).
Gespräche über schulinterne Angelegenheiten, Unterrichtsinhalte und sämtliche Informationen, die dem Amtsgeheimnis unterliegen, werden vermieden.

3.9 Meldepflicht

Sicherheitsvorfälle, der Verlust bzw. Defekt von IT-Arbeitsmitteln oder verdächtige Handlungen/Personen sind umgehend dem PIKT- oder TIKT-Team der BBW zu melden.

4 Datenschutz

Der Schutz von Personendaten ist für die Schule besonders wichtig. Werden solche Daten unrechtmässig genutzt oder veröffentlicht, können die Rechte der Betroffenen verletzt und das Vertrauen in die BBW geschädigt werden.

Mögliche Gefahren:

- Eine unberechtigte Person erhält Zugang zu schützenswerten Personendaten. Damit werden die Rechte des betroffenen Nutzenden verletzt.
- Sensitive Daten können veröffentlicht oder in falsche Hände geraten.
- Es werden Daten im Namen der BBW publiziert, die jedoch nicht offiziell von der BBW stammen.

4.1 Generell

Die Benutzenden halten sich im schulischen und organisatorischen Kontext an die hier aufgeführten Punkte zum Datenschutz.

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.

Alle Personen und Stellen innerhalb der Institution haben bei der Verarbeitung von Daten das Prinzip der Datensparsamkeit und Datenminimierung zu beachten. Dies gilt insbesondere für die automatisierte Bearbeitung von Personendaten.

Es ist nicht erlaubt, umfassende Persönlichkeitsprofile über Nutzende zu erstellen. Persönlichkeitsprofile sind gegenüber Lernprofilen zu unterscheiden.

Es dürfen keine schriftlichen Aufzeichnungen, grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen ohne die explizite Zustimmung betroffenen Personen veröffentlicht oder Dritten bekanntgegeben werden.

4.2 Im Unterricht

Der Schutz der Persönlichkeit und die Einhaltung des Datenschutzes liegt während des Unterrichts in der gemeinsamen Verantwortung von Lehrpersonen, Lernenden und der Institution.

Die Lernenden sind betreffend datenschutzrechtliche Themen regelmässig zu sensibilisieren.

a. Lerntechnologien (inklusive Social Media und generative Sprachmodelle)
Anwendungen im Unterricht sind mit Blick auf die datenschutzrechtlichen Vorgaben (Speicherort, Aufbewahrungsdauer, Möglichkeit der endgültigen Löschung, technische Massnahmen wie Verschlüsselung etc.) zu prüfen. Im Zweifelsfall richtet sich die betroffene Person an den IKT-Support der BBW.

b. Auswertungen über die Lernenden
Im schulischen Kontext ist es zur Bewertung der Lernkompetenzen unerlässlich, Lernprofile zu erstellen. Diese enthalten ausschliesslich Daten, die direkt mit der Leistungs- und Kompetenzentwicklung zusammenhängen. Persönlichkeitsprofile hingegen beinhalten umfassendere personenbezogene Informationen, die Rückschlüsse auf das Wesen und die individuelle Persönlichkeit der Lernenden zulassen. Um den Datenschutzprinzipien, insbesondere der Datensparsamkeit und Zweckbindung, gerecht zu werden, dürfen Lernprofile nicht mit zusätzlichen persönlichen Merkmalen kombiniert werden, da dies zur Erstellung von Persönlichkeitsprofilen führen könnte, die den Schutz der Privatsphäre gefährden würden.

Es ist nicht zulässig personenbezogenen Statistiken oder Auswertungen in der Klasse offenzulegen oder anderen Lehrpersonen, Eltern oder Schulmitarbeitenden bekanntzugeben.

In von der Schule definierten Gremien dürfen personenbezogene Statistiken und Auswertungen offengelegt werden.

c. Besondere Personendaten

Schriftliche Aufzeichnungen (Aufsätze, Gedichte, etc.), grafische Darstellungen oder Bild-, Ton- oder Videoaufnahmen von Lernenden, die Angaben über besondere Personendaten enthalten, sind mindestens als vertraulich zu klassifizieren, es gilt die erhöhte Schutzstufe. Sie sind spätestens Ende Ausbildung zu anonymisieren oder zu vernichten. Die Rekursfristen sind einzuhalten.

d. Verhalten und Veröffentlichung

- Es werden keine ehrverletzenden, rassistischen, diskriminierenden oder beleidigenden Beiträge und Kommentare verfasst, verbreitet oder gepostet.
- Es wird nicht zu illegalen oder gefährlichen Handlungen sowie zu Mobbing aufgerufen.
- Themenfremde, kommerzielle oder wiederholende Inhalte (Spam) werden nicht veröffentlicht.
- Öffentliche Beiträge enthalten keine namentliche Nennung und keine persönlichen Daten von Lehrpersonen, Mitarbeitenden oder Lernenden.
- Nutzungsrechte an Inhalte, Aufnahmen Bsp. Bilder, Videos, Audio dürfen nicht an Dritte abgetreten werden.
- Vor jeder Aufnahme wird das Einverständnis aller abgebildeten oder aufgezeichneten Personen eingeholt.
- Ohne ausdrückliche Zustimmung der aufgezeichneten Personen oder der Besitzerinnen werden Aufnahmen nicht versendet, verbreitet oder veröffentlicht.
- Aufzeichnungen und Chatverläufe werden ausschliesslich in abgestimmten Fällen archiviert (z. B. zur Klärung von Vorfällen).
- In Videokonferenzen kann die Kamera ausgeschaltet oder der Hintergrund ausgeblendet werden, um die Privatsphäre zu wahren.
- Die Privatsphäre anderer wird respektiert; niemand wird aufgefordert, private Bereiche oder Räume offenzulegen.
- Persönliche Anliegen werden direkt an die zuständige Stelle der Schule gerichtet, statt sie öffentlich zu adressieren.

e. Bekanntgabe

Da die Lernenden der BBW älter als 14 Jahre sind, muss von den Eltern keine Einwilligung eingeholt werden. Die Einwilligung der Lernenden ist ausreichend.

4.3 Lerntechnologien und KI

Für den Einsatz generativer KI und digitaler Lerntechnologien gelten die folgenden Punkte:

Umgang mit Informationen:

- Bei der Nutzung generativer KI und digitaler Lerntechnologien dürfen keine personenbezogenen Daten eingegeben werden, da auch anonymisierte Daten potenziell Rückschlüsse auf bestimmte Personen zulassen.
- Öffentlich zugängliche Informationen der Schule dürfen eingegeben werden, jedoch ist deren Kombination mit internen, vertraulichen oder geheimen Identifikatoren bzw. Aktenzeichen zu vermeiden, um die Sicherheit und Vertraulichkeit zu gewährleisten.
- Vertrauliche oder als geheim klassifizierte Informationen sind bei der Nutzung generativer KI nicht zu verwenden – im Zweifelsfall ist von der höchsten Schutzklasse auszugehen.

- Daten, die die Schule nicht verlassen dürfen, etwa nicht öffentliche Anfragen von Lernenden oder vertrauliche schulische Inhalte, dürfen bei der Verwendung generativer KI nicht eingegeben werden.

Hinweise für die Registrierung und Nutzung

- Die Registrierung zur Nutzung generativer KI-Tools und digitaler Lerntechnologien erfolgt freiwillig; eine Registrierung darf nicht erzwungen werden.
- Nutzende sind umfassend über den Zweck und die Anwendung generativer KI im Kontext der Anwendung zu informieren. (Bsp. Lernende im Lernkontext)
- Die Angabe persönlicher Daten im Rahmen der Registrierung für generative KI-Anwendungen erfolgt ausschliesslich auf freiwilliger Basis.
- Für Lerntechnologien, die nicht im Schulangebot enthalten sind, dürfen nicht die Logindaten der Schule benutzt werden.
- Bestehen keine offiziellen Vorgaben, welche Logindaten bei einer Registration benutzt werden können, ist das didaktisch-pädagogische IKT PIKT-Team zu konsultieren.

5 Urheberrecht

Die detaillierten Regelungen befinden sich im Tarif 7 von ProLitteris (GT7), der regelmässig überprüft und weiterentwickelt wird und im Zweifelsfall zu konsultieren ist.

5.1 Generell

Die Benutzenden halten sich im schulischen Kontext an das Urheberrecht. Es sind folgende Vorgaben zu beachten:

1. Es dürfen Ausschnitte von urheberrechtlich geschützten Werken («Werke») zum Eigengebrauch der Schule, d.h. zur internen Information und Dokumentation, vervielfältigt werden, sei dies analog oder digital.
2. Erlaubt ist die Nutzung ganzer Radio- und TV-Sendungen auf passwortgeschützten, digitalen Plattformen über die abonnierten Digi- und Mediatheken. Diese Nutzung beinhaltet das Vervielfältigen ganzer Radio- und Fernsehsendungen sowie das unentgeltliche Zugänglichmachen für berechtigte Benutzer, einschliesslich das Abrufen samt Download einzelner Sendungen aus einem schulinternen Netzwerk.
3. Nicht erlaubt ist namentlich:
    a. Das Vervielfältigen von ganzen Werken bzw. deren Exemplare, die im Handel erhältlich sind.
    b. Das Veröffentlichen von Werken oder Werkausschnitten auf der öffentlichen Schulwebseite, sozialen Medien (inkl. geschlossener Gruppen), Videoportalen, etc.
    c. Das Bearbeiten oder Verändern von Werken.
4. Werden für Lehrpersonen, die ganze Schule oder Dritte Lehrmittel erstellt, dürfen diese keine Zusammenstellungen von fremden Werkausschnitten erhalten.

5.2 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. Ton-, Tonbild- und andere Leerträger
Erlaubt ist das Kopieren von Ausschnitten aus Büchern, Filmen, Musikstücken (d.h. auch Musiknoten) und auch Werken der bildenden Kunst sowie das vollständige Aufzeichnen von Radio- und Fernsehsendungen (exkl. im Handel erhältlicher Filme) durch eine einzelne Lehrperson für ihre eigenen Unterrichtszwecke. Beim Bereitstellen solcher Kopien für mehrere Lehrpersonen aus Quellen, die nicht Radio- oder Fernsehsendungen sind, muss die Erlaubnis des Rechteinhabers eingeholt werden.

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

d. Musikaufführungen
Das Aufführen von Werken der nicht-theatralischen Musik und geschützter Leistungen an klassenübergreifenden 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.

e. 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.

5.3 Generative KI

Wer KI-Inhalte veröffentlicht, trägt die Verantwortung bei Rechtsverletzungen.

6 Massnahmen bei Verstössen

Bei einer missbräuchlichen Nutzung der IKT-Systeme – also bei Verstössen gegen diese Nutzungsrichtlinie, gegen weitergehende schulinterne Vorgaben oder geltende gesetzliche Bestimmungen sowie bei der Beeinträchtigung der Rechte Dritter – behält sich die Schule vor, angemessene Massnahmen zu ergreifen.

Diese Regelung gilt für alle Benutzenden, also sowohl für Mitarbeitende, Lehrpersonen, Mitglieder von Schulkommissionen, Gäste als auch für Lernende. Zur Klärung von Vorfällen können technische Protokolle ausgewertet werden. In der Regel wird zunächst das Gespräch gesucht und den Betroffenen die Möglichkeit zur Stellungnahme eingeräumt.

Je nach Schwere und Wiederholung des Verstosses können Massnahmen von einer mündlichen Verwarnung über eine schriftliche Abmahnung bis hin zu disziplinarischen Massnahmen reichen.

Bei Lernenden erfolgt – je nach Schwere des Verstosses – auch eine Information der Inhaber der elterlichen Sorge, weiterer Erziehungsberechtigter und des Lehrbetriebs.

Sollte sich ein Verstoss als gravierend erweisen, behält sich die Schule zudem vor, Schadenersatzforderungen zu stellen und gegebenenfalls die zuständigen Behörden zu informieren.

7 Haftungsausschluss

Soweit die Rechtsordnung dies zulässt, schliesst die Schule jede Haftung für Schäden durch Benutzerhandlungen aus. Die Schule haftet ausserdem nicht für Schäden, die den Benutzenden aus ihrer Missachtung dieser Nutzungsrichtlinie und des anwendbaren Datenschutzrechts sowie der Missachtung der kantonalen AISR und anwendbaren BISR entstehen. (vgl. auch «Richtlinien» unter Kap. 8)

8 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

Richtlinien

- Allgemeine Informationssicherheitsrichtlinie des Regierungsrates AISR für die kantonale Verwaltung vom 3. September 2019 Link

- Besondere Informationssicherheitsrichtlinien für die kantonale Verwaltung BISR vom 17. Juni 2020, Inkrafttreten am 17. Juni 2022 Link
- Richtlinien für die Informationsverwaltung an den kantonalen Mittel- und Berufsfachschulen sowie an den vom Kanton beauftragten Berufsfachschulen vom 4. April 2016 Link
- Richtlinien Informationsschutz des MBA; Link

Merkblätter

Leitfaden Datenschutzlexikon Mittelschule und Berufsfachschule vom September 2020; Link

- Leitfaden Einsatz von mobilen Geräten in der Verwaltung vom August 2022; Link
- ProLitteris Tarif 7 Gültigkeit 2022-2026; Link
- Pro Litteris Merkblatt Schulen (GT 7), Link