kv business school zürich
mein bildungspartner.

Nutzungsrichtlinien IT für Studierende

gültig ab: 15.08.2025

1. Zweck und Geltungsbereich

Diese Richtlinien gelten für alle Studierenden der KV Business School Zürich. Sie regelt die Nutzung der IT-Infrastruktur und digitalen Dienste der Schule – unabhängig davon, ob diese auf schuleigenen Geräten oder privaten Geräten genutzt werden (sog. **Bring Your Own Device**, BYOD).

Ziel ist es, einen sicheren, verantwortungsbewussten und rechtlich konformen Umgang mit den bereitgestellten IT-Mitteln zu gewährleisten.

2. IT-Dienste der KV Business School Zürich

Studierenden stehen folgende digitalen Dienste zur Verfügung:

- **Moodle**: Lernplattform für Unterrichtsmaterial, Aufgaben und Kommunikation
- **Microsoft 365 (M365)**: Kollaborations- und Office-Tools inkl. Word, Excel, PowerPoint, OneDrive, Teams etc., der Funktionsumfang ist im Einzelfall abhängig von der zugewiesenen Lizenz.
- **WLAN**: Kostenloses WLAN für alle Studierenden, Login erfolgt über persönliche Zugangsdaten

Hinweise zur Datenverarbeitung:

- Die Daten werden nicht lokal auf Servern der Schule gespeichert, sondern in Cloud-Diensten mit Datenstandort Schweiz oder EU gemäss geltendem Datenschutzrecht.
- Mit der Nutzung dieser Plattformen stimmen Studierende der datenschutzkonformen Verarbeitung ihrer Daten gemäss Datenschutzgesetz (nDSG) zu.

Support:
Bei technischen Fragen oder Problemen wenden Sie sich bitte an den IT-Support: helpdesk@kvz-schule.ch.
Der Support bezieht sich auf Schwierigkeiten mit Logins/Passwörtern oder Funktionalitäten von M365. Für technische Probleme mit privaten Geräten im Rahmen von BYOD kann kein Support geleistet werden.

3. Nutzung von Schul-PCs und BYOD

- Schul-PCs stehen in bestimmten Ausbildungsangeboten zur Verfügung und sind mit der M365-Umgebung vollständig ausgestattet.
- Studierende dürfen private Geräte (Laptops, Tablets) mitbringen und im WLAN sowie mit den Cloud-Diensten verwenden (**Bring Your Own Device**).
- Auf Schul-PCs ist es **nicht erlaubt**, private Software zu installieren oder persönliche Daten zu speichern.
- Auf privaten Geräten ist für ausreichenden **Virenschutz und Systemsicherheit** zu sorgen (z. B. aktuelles Betriebssystem, Antivirenprogramm).
- Es dürfen keine Programme zur Netzwerküberwachung, VPN-Tunneling zur Umgehung von Sperren o. ä. eingesetzt werden.

- Es ist nicht möglich, Daten von OneDrive mit privaten Geräten zu synchronisieren. Der Zugriff auf OneDrive erfolgt ausschliesslich über die Weboberfläche.

4. Datenschutz, Datensicherheit und Zugriffsdauer

- Die Verarbeitung personenbezogener Daten unterliegt dem **neuen Datenschutzgesetz (nDSG, 2023)**.
- Persönliche Zugangsdaten (z. B. Passwörter) sind vertraulich zu behandeln und dürfen **nicht weitergegeben** werden.
- Die Schule ergreift angemessene **technische und organisatorische Schutzmassnahmen** zur Sicherung der Datenintegrität und -vertraulichkeit.
- Die Zugänge zu schulischen Systemen (z. B. Moodle, M365) werden **90 Tage nach Ende der Ausbildung automatisch deaktiviert**.
- Nach dieser Frist ist kein Zugriff mehr auf gespeicherte Inhalte möglich. Die Studierenden sind **selbst dafür verantwortlich**, alle benötigten Daten rechtzeitig zu sichern.

5. Verhaltensregeln und Fair Use

- Die bereitgestellten IT-Mittel sind mit **Sorgfalt und Respekt** zu verwenden. Sie dienen **ausschliesslich schulbezogenen Zwecken**.
- Der Zugriff auf oder das Speichern von **unangemessenen oder illegalen Inhalten** (z. B. Gewalt, Pornografie, Hassrede, Raubkopien) ist streng untersagt.
- Es ist **verboten, Konten oder Passwörter mit anderen zu teilen** – auch nicht für Gruppenarbeiten.
- In Plattformen wie Moodle und Teams ist ein **respektvoller und professioneller Kommunikationsstil** einzuhalten (Netiquette).
- Die Nutzung erfolgt stets über persönliche Konten – mit entsprechender Eigenverantwortung für sicheres Verhalten online.

6. Sicherheit und Haftung

- Bei **Verlust oder Verdacht auf Missbrauch** von Zugangsdaten ist umgehend die IT-Abteilung zu informieren.
- Die Studierenden haften **persönlich** für Schäden durch mutwillige Zerstörung, fahrlässige Nutzung oder missbräuchliches Verhalten.
- Die Schule behält sich vor, bei Verdacht auf schwerwiegenden Verstoss:
  - die Nutzung einzuschränken,
  - die betroffenen Konten zu sperren,
  - disziplinarische Massnahmen gemäss Schulreglement zu ergreifen.

7. Schlussbestimmungen

- Mit der Nutzung der IT-Dienste erkennen die Studierenden diese Nutzungsrichtlinie an und verpflichten sich zur Einhaltung.
- Bei Fragen zur Anwendung dieser Richtlinie wenden Sie Sich bitte an Ihre Ansprechperson in der Kursadministration.
- Diese Richtlinie ergänzt ggf. bestehende Regelwerke (Hausordnung, Schulordnung, Datenschutzkonzept) und tritt mit dem oben genannten Datum in Kraft.