

Benutzungsordnung für die IT-Infrastruktur der HTL Villach



Teil der Hausordnung gemäß § 44 Abs. 1 SchUG

Fassung 2 · Gültig ab 14.09.2026

Diese Benutzungsordnung ist Teil der Hausordnung der HTL Villach und ergänzt diese. Regelungen, die bereits in der Hausordnung enthalten sind – insbesondere zu Datenschutz, zu Foto-, Video- und Tonaufnahmen sowie zur Nutzung von Mobiltelefonen – werden hier nicht wiederholt; es gilt die Hausordnung.

Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

Das Wichtigste in Kürze

Diese Kurzfassung dient dem Überblick und der Besprechung im Unterricht. Rechtlich verbindlich ist der ausführliche Text ab Punkt 1.

- Dein Schul-Account gehört dir allein. Passwort geheim halten, Multifaktor-Authentifizierung aktivieren, nie weitergeben.
- Die Schul-IT und dein Microsoft-365-Konto sind für die Schule da, nicht für Privates.
- Sei anständig – online wie offline. Mobbing, Belästigung und Diskriminierung sind auch im Chat verboten.
- Fremde Konten, fremde Daten und fremde Systeme sind tabu – auch „nur zum Ausprobieren“.
- Wenn du eine Sicherheitslücke findest: melde sie, nutze sie nicht aus. Wer meldet, wird dafür nicht bestraft.
- Lade nichts herunter und verbreite nichts, was in Österreich verboten ist.
- Halte dich ans Urheberrecht – bei Software, Musik, Filmen, Bildern und Texten.
- Für Fotos, Videos und Tonaufnahmen gelten die Regeln der Hausordnung – ohne Zustimmung geht nichts.
- KI-Werkzeuge nur dort, wo die Lehrperson sie erlaubt – ohne personenbezogene Daten und mit Offenlegung.
- Beim Betrieb der Systeme fallen Protokolldaten an. Was gespeichert wird und wie lange, steht im Anhang.
- Probleme, Schäden, verlorene Geräte: sofort dem IT-Management melden.

1. Geltungsbereich, Zweck und Rechtsgrundlagen

- 1.1** Diese Benutzungsordnung regelt die Nutzung der IT-Infrastruktur der Höheren Technischen Bundeslehr- und Versuchsanstalt Villach (HTL Villach) durch Schülerinnen und Schüler. Erfasst sind insbesondere EDV-Räume, schulische Endgeräte, das schulische Netzwerk einschließlich WLAN, der Internetzugang, die schulischen Microsoft-365-Dienste (Domain edu.htl-villach.at) sowie sonstige von der Schule bereitgestellte Anwendungen und Cloud-Dienste.
- 1.2** Sie ist Teil der Hausordnung (§ 44 Abs. 1 SchUG). Ergänzend gelten die übrigen Bestimmungen der Hausordnung, insbesondere jene zum Datenschutz, zu Foto-, Video- und Tonaufnahmen sowie zur Nutzung von Mobiltelefonen. Diese Regelungen werden hier nicht wiederholt.

Tschinowitscher Weg 5
A-9500 Villach

Tel 04242 / 37061-0

office@htl-villach.at
www.htl-villach.at
DVR 64343 (202417)

- 1.3** Zweck der Ordnung sind der geordnete, sichere und rechtskonforme Betrieb der schulischen IT, der Schutz der Nutzerinnen und Nutzer sowie die Erfüllung des Unterrichts- und Erziehungsauftrags.
- 1.4 Verhältnis zum Datenschutzrecht.** Bereitstellung und Betrieb der IT-Infrastruktur erfolgen zur Erfüllung der der Schule gesetzlich übertragenen Aufgaben (Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit SchUG, SchOG und Bildungsdokumentationsgesetz) und beruhen **nicht** auf einer Einwilligung. Die Kenntnisnahme dieser Benutzungsordnung ist daher keine datenschutzrechtliche Einwilligung. Für Einwilligungen – insbesondere zu Foto- und Videoaufnahmen – gilt die Hausordnung.
- 1.5** Die Benutzungsordnung wird bei Ausgabe des Schul-Accounts ausgehändigt und im Unterricht besprochen. Die Kenntnisnahme wird dokumentiert; bei minderjährigen Schülerinnen und Schülern werden auch die Erziehungsberechtigten informiert.



2. Benutzerkonto und Zugangsdaten

- 2.1** Die Nutzung der IT-Infrastruktur ist ausschließlich über das persönliche Benutzerkonto (lokales Konto und Microsoft-365-Konto) gestattet.
- 2.2** Zugangsdaten sind geheim zu halten und dürfen nicht an Dritte weitergegeben werden. Kennwörter müssen den geltenden Mindestanforderungen der Schule entsprechen (siehe Anhang) und dürfen nicht für private Dienste wiederverwendet werden.
- 2.3** Wo technisch verfügbar, ist die Mehrfaktor-Authentifizierung (MFA) zu aktivieren und zu verwenden.
- 2.4 Verantwortlichkeit.** Jede Schülerin und jeder Schüler ist für Handlungen verantwortlich, die unter dem eigenen Konto gesetzt werden, soweit sie oder er die Pflichten nach 2.2 und 2.3 verletzt oder die Nutzung durch Dritte sonst zu vertreten hat. Eine Verantwortlichkeit besteht nicht, wenn das Konto trotz Einhaltung dieser Sorgfaltspflichten missbraucht wurde.
- 2.5** Ein Verdacht auf Missbrauch des eigenen Kontos (vergessenes Abmelden, Kenntnis Dritter vom Kennwort, Verlust eines angemeldeten Gerätes, Phishing-Verdacht) ist unverzüglich dem IT-Management zu melden; das Kennwort ist zu ändern. Eine unverzügliche Selbstmeldung wird nicht sanktioniert.
- 2.6** Die Verwendung fremder Konten sowie das Ausprobieren oder Umgehen von Zugangs- und Berechtigungskontrollen sind untersagt (vgl. § 118a StGB).

3. EDV-Räume und schulische Endgeräte

- 3.1** Die EDV-Räume dürfen nur in Anwesenheit einer aufsichtsführenden Lehrperson oder mit ausdrücklicher Erlaubnis genutzt werden; ausgenommen sind ausgewiesene Schüler-Internetbereiche innerhalb der ausgehängten Öffnungszeiten.
- 3.2** Arbeitsplatz und Geräte sind ordnungsgemäß und sauber zu hinterlassen; vor dem Verlassen ist abzumelden. Essen und Trinken sind in den EDV-Räumen nicht gestattet.
- 3.3** Mit der gesamten Ausstattung ist schonend, mit Verbrauchsmaterial (Toner, Tinte, Papier) sparsam umzugehen.

- 3.4 Systemkonfigurationen sowie Netzwerk- und Sicherheitseinstellungen dürfen nicht verändert werden, soweit dies nicht ausdrücklich Teil einer Unterrichtsaufgabe ist. Das Einbringen oder Ausführen funktionsschädigender Programme (Malware) ist untersagt (vgl. §§ 126a, 126b, 126c StGB).
- 3.5 Software einschließlich Spielen, Browser-Erweiterungen und Apps darf nur mit Erlaubnis des IT-Managements installiert oder im Netzwerk gespeichert werden. In Laborumgebungen gelten die dort erteilten Freigaben.
- 3.6 Störungen, Schäden und sicherheitsrelevante Auffälligkeiten sind unverzüglich dem IT-Management zu melden (mündlich, schriftlich oder per E-Mail).
- 3.7 Vorsätzliche Beschädigung oder Entwendung von Ausstattung kann zivil- und strafrechtliche Folgen haben; die Schule behält sich in solchen Fällen eine Anzeige vor. Für den Schadenersatz gelten die allgemeinen gesetzlichen Bestimmungen (§§ 1293 ff. ABGB, für Minderjährige insbesondere § 1310 ABGB).



Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

4. Eigene Geräte (BYOD) und Schul-WLAN

- 4.1 Private Geräte dürfen im Unterricht nur mit Erlaubnis der Lehrperson verwendet werden.
- 4.2 Für die Nutzung des Schul-WLAN gelten dieselben Regeln wie für schulische Geräte. Die Anmeldung erfolgt mit dem persönlichen Schul-Account; eine Weitergabe des Zugangs an schulfremde Personen ist untersagt.
- 4.3 Private Geräte sind auf einem aktuellen Sicherheitsstand zu halten. Geräte, von denen eine Gefahr für das Schulnetz ausgeht, können ohne vorherige Ankündigung vom Netzzugang getrennt werden.
- 4.4 Die Schule haftet nicht für Verlust oder Beschädigung privater Geräte und übernimmt keine Wartung. Ein Anspruch auf Zugang zum Schulnetz mit privaten Geräten besteht nicht.
- 4.5 Bei der Verbindung mit dem Schulnetz fallen Verbindungsdaten an, die nach dem Anhang verarbeitet und nach Ablauf der dort genannten Fristen gelöscht werden.

5. Schulische Microsoft-365-Umgebung

- 5.1 **Zweckbindung.** Das Konto und alle darüber zugänglichen Dienste (Outlook, Teams, OneDrive, SharePoint, Office-Apps) sind ausschließlich für unterrichts- und schulbezogene Zwecke bestimmt. Eine private Nutzung ist nicht gestattet. Nutzerinnen und Nutzer dürfen daher nicht darauf vertrauen, dass im Schulkonto abgelegte private Inhalte vertraulich bleiben; private Inhalte sind außerhalb des Schulkontos zu speichern.
- 5.2 **Datenablage.** Schulische Dokumente werden in OneDrive oder in den Teams der jeweiligen Klasse bzw. Gruppe abgelegt. Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO (etwa Gesundheitsdaten) sowie private Fotos und Dokumente dürfen im Schulkonto nicht gespeichert werden.
- 5.3 **Kommunikation.** E-Mails und Chats sind in höflichem, sachlichem Ton zu verfassen. Cybermobbing, Belästigung, Bedrohung und diskriminierende Inhalte sind untersagt – auch in Einzel- und Gruppenchats über das Schulkonto – und werden als schwerwiegender Verstoß behandelt. Sie können strafrechtliche Folgen haben (z. B. §§ 107, 107c, 111, 115 StGB).

5.4 Videokonferenzen (Teams-Meetings).

- Aufzeichnungen sind grundsätzlich nicht zulässig. Ausnahmen setzen einen konkreten Unterrichtszweck, eine vorherige Ankündigung, die vorherige ausdrückliche und freiwillige Einwilligung aller Beteiligten – bei minderjährigen Schülerinnen und Schülern zusätzlich jene der Erziehungsberechtigten – sowie eine im Vorhinein festgelegte Speicherdauer voraus.
- Wer nicht einwilligt, darf daraus keinen Nachteil erleiden; es ist eine gleichwertige Teilnahmemöglichkeit ohne Aufzeichnung anzubieten.
- Es besteht keine Verpflichtung, die Kamera einzuschalten. Lehrpersonen können darum ersuchen; die Entscheidung liegt bei der Schülerin oder dem Schüler beziehungsweise den Erziehungsberechtigten. Für Leistungsfeststellungen im Distanzunterricht gelten gesonderte Regelungen.
- Meeting-Links und Zugangsdaten dürfen nicht an schulfremde Personen weitergegeben werden.
- Eigenmächtige Mitschnitte, Bildschirmaufnahmen und Fotos des Bildschirms sind untersagt (§ 120a StGB, § 78 UrhG).



Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

5.5 Geräteverlust. Geht ein Gerät mit aktivem Zugang zum Schulkonto verloren oder wird es gestohlen, ist dies unverzüglich dem IT-Management zu melden, damit das Konto gesperrt werden kann.

5.6 Verarbeitung durch den Auftragsverarbeiter. Die Verarbeitung erfolgt im Rahmen des Schul-Tenants auf Grundlage eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO zwischen dem Schulerhalter beziehungsweise der zuständigen Stelle des Bundes und Microsoft. Die Daten werden grundsätzlich innerhalb der EU-Datengrenze (EU Data Boundary) verarbeitet und gespeichert. Soweit im Einzelfall Übermittlungen in Drittländer stattfinden, erfolgen diese auf Grundlage eines Angemessenheitsbeschlusses (EU-US Data Privacy Framework) oder der Standardvertragsklauseln.

5.7 Beendigung des Kontos. Nach Beendigung des Schulbesuchs wird das Konto innerhalb von acht Wochen deaktiviert und spätestens zwölf Monate nach Beendigung samt Inhalten gelöscht. Betroffene werden mindestens sechs Wochen vorher informiert, damit sie relevante Daten sichern können. Eine längere Aufbewahrung erfolgt nur, soweit gesetzliche Aufbewahrungspflichten bestehen.

6. Internetnutzung

6.1 Der Internetzugang dient schulischen Zwecken. Downloads, die nicht dem Unterrichtszweck dienen oder die Netzwerkkapazität erheblich belasten, sind zu unterlassen.

6.2 Untersagt sind das Abrufen, Speichern, Weiterverbreiten und Anbieten von Inhalten, die nach österreichischem Recht verboten sind, insbesondere nationalsozialistische Wiederbetätigung (Verbotsgesetz), Verhetzung (§ 283 StGB), Darstellungen sexuellen Missbrauchs Minderjähriger (§ 207a StGB), gewaltverherrlichende und pornografische Inhalte sowie Inhalte, die gegen Jugendschutzbestimmungen verstoßen. Verstöße können strafrechtliche Folgen haben.

6.3 Bedenkliche oder belastende Inhalte sowie Kontaktversuche unbekannter Personen sind der aufsichtsführenden Lehrperson, dem Klassenvorstand oder dem IT-Management zu melden.

Personenbezogene Bezeichnungen gelten jeweils auch in ihrer weiblichen Form

- 6.4** Persönlichkeitsrechte sowie Urheber- und Publikationsrechte Dritter sind zu respektieren.
- 6.5** Der Internetzugang darf nicht für parteipolitische Werbung oder kommerzielle Zwecke genutzt werden. Die Tätigkeit der schulischen Interessenvertretung und die Meinungsäußerung der Schülerinnen und Schüler im Rahmen der Schulgemeinschaft bleiben davon unberührt.
- 6.6** Wer über schulische Kanäle kommuniziert (Schul-E-Mail, offizielle Konten der Schule), muss sich bewusst sein, dass diese Kommunikation der Schule zugerechnet werden kann. Untersagt ist die Verbreitung rechtswidriger, beleidigender, wahrheitswidriger oder ehrenrühriger Inhalte. Sachliche Kritik – auch an der Schule – ist davon nicht erfasst und ausdrücklich zulässig. Für den Inhalt eigener Nachrichten ist jede Nutzerin und jeder Nutzer selbst verantwortlich.
- 6.7** Zum Schutz der Nutzerinnen und Nutzer sowie des Schulnetzes werden am Internetzugang technische Schutzmaßnahmen eingesetzt (Firewall, Malware- und Inhaltsfilter). Die dabei anfallenden Daten werden nach dem Anhang verarbeitet und nach Ablauf der dort genannten Fristen gelöscht. Das Umgehen dieser Schutzmaßnahmen, etwa über Proxys, VPN oder Tunnel, ist außerhalb ausdrücklich freigegebener Unterrichtsübungen untersagt.
- 6.8** Die Schule wählt die über ihren Zugang erreichbaren fremden Inhalte nicht redaktionell aus und übernimmt für diese keine Verantwortung.



Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

7. Einsatz von KI-Werkzeugen

- 7.1** Der Einsatz von KI-Werkzeugen (Chatbots, Bild- und Codegeneratoren, in Anwendungen integrierte Assistenzfunktionen) ist nur mit den von der Schule freigegebenen Diensten und in dem von der Lehrperson festgelegten Rahmen zulässig. Eine aktuelle Liste der freigegebenen Dienste führt das IT-Management.
- 7.2** In KI-Werkzeuge dürfen keine personenbezogenen Daten Dritter – etwa von Mitschülerinnen und Mitschülern, Lehrpersonen oder Praktikumsbetrieben – und keine vertraulichen Schul- oder Betriebsdaten eingegeben werden.
- 7.3** Bei Schularbeiten, Projekten und Diplomarbeiten ist der Einsatz von KI-Werkzeugen nach den Vorgaben der Lehrperson beziehungsweise den Regelungen zur Diplomarbeit offenzulegen. Die Abgabe unveränderter KI-Ausgaben als eigene Leistung ist unzulässig.
- 7.4** Für Ergebnisse von KI-Werkzeugen besteht keine Richtigkeitsgewähr; sie sind eigenständig zu prüfen.

8. Umgang mit Sicherheitslücken (Responsible Disclosure)

- 8.1** Wer eine Schwachstelle oder Fehlkonfiguration in schulischen Systemen entdeckt, meldet dies unverzüglich und ausschließlich dem IT-Management (support@htl-villach.at) und behandelt die Information bis zur Behebung vertraulich.

- 8.2** Untersagt sind das Ausnutzen, Ausweiten, Weitergeben und Veröffentlichen einer Schwachstelle, der Zugriff auf fremde Daten sowie jede Veränderung oder Beeinträchtigung von Systemen. Solche Handlungen können strafbar sein (§§ 118a, 126a, 126b, 126c StGB) – auch dann, wenn keine Schädigungsabsicht besteht.
- 8.3 Schutz für Meldende.** Wer eine Schwachstelle entdeckt, sie nicht ausnutzt und sie nach Punkt 8.1 meldet, hat allein wegen der Entdeckung und der Meldung keine Maßnahmen nach Punkt 10 zu erwarten. Das gilt auch, wenn die Entdeckung durch eine versehentliche Fehlbedienung erfolgt ist.
- 8.4** Sicherheitsuntersuchungen wie Portscans, Kennwort- oder Penetrationstests sind ausschließlich in den dafür vorgesehenen Laborumgebungen und nur nach ausdrücklicher Beauftragung durch eine Lehrperson in Absprache mit dem IT-Management zulässig.



Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

9. Urheberrecht und Software

- 9.1** Das Vervielfältigen, Verbreiten und Zugänglichmachen urheberrechtlich geschützter Werke – Software, Musik, Filme, Bilder, Texte – ohne Erlaubnis ist untersagt und kann zivil- und strafrechtliche Folgen haben (§§ 86 ff. und § 91 UrhG).
- 9.2** Es dürfen ausschließlich lizenzierte beziehungsweise von der Schule freigegebene Programme verwendet werden. Lizenzbedingungen, auch jene von Open-Source-Lizenzen, sind einzuhalten.
- 9.3** Über die Schule bezogene Lizenzen dürfen nur im zulässigen Umfang und nur während des aufrechten Schulbesuchs genutzt werden.
- 9.4** Fremde Inhalte in Referaten, Projekten und Diplomarbeiten sind zu kennzeichnen und zu zitieren.

10. Verstöße und Maßnahmen

- 10.1** Vor jeder Maßnahme ist der Schülerin oder dem Schüler Gelegenheit zur Stellungnahme zu geben. Bei Minderjährigen werden die Erziehungsberechtigten eingebunden.
- 10.2** Maßnahmen sind nach Schwere, Verschulden und Wiederholung abgestuft und verhältnismäßig zu wählen. In Betracht kommen insbesondere:
- das pädagogische Gespräch sowie die Erziehungsmittel nach § 47 SchUG;
 - die Mitwirkung an der Behebung eines Schadens im zumutbaren Ausmaß;
 - die befristete Einschränkung oder der befristete Entzug einzelner Nutzungsrechte, etwa des Internetzugangs oder der Nutzung außerhalb des Unterrichts;
 - bei Gefahr für die Systeme die sofortige vorläufige Sperre des Kontos; diese ist unverzüglich zu überprüfen und aufzuheben, sobald der Grund weggefallen ist.
- 10.3 Sicherstellung des Unterrichts.** Maßnahmen nach 10.2 dürfen die Teilnahme am Unterricht und an Leistungsfeststellungen nicht verhindern. Ist für den Unterricht ein IT-Zugang erforderlich, wird ein betreuter oder eingeschränkter Zugang bereitgestellt. Ein dauerhafter, vollständiger Entzug der Nutzungsberechtigung ist ausgeschlossen; der Ausschluss von der Schule richtet sich ausschließlich nach § 49 SchUG.

- 10.4** Weitergehende schulrechtliche Maßnahmen richten sich nach dem SchUG. Zivil- und strafrechtliche Folgen bleiben unberührt. Bei strafrechtlich relevanten Sachverhalten entscheidet die Schulleitung über eine Anzeige unter Bedachtnahme auf das Jugendgerichtsgesetz.
- 10.5** Punkt 8.3 (Meldung von Sicherheitslücken) und Punkt 2.5 (Selbstmeldung eines Missbrauchsverdachts) gehen diesem Punkt vor.



Höhere Technische
Bundeslehr- und
Versuchsanstalt Villach

Anhang – Protokolldaten, Speicherfristen und Kennwortvorgaben

Die folgenden Angaben werden vom IT-Management mit den tatsächlichen Systemeinstellungen abgeglichen und bei Bedarf aktualisiert. Eine über die genannten Fristen hinausgehende Speicherung ist nur zur Aufklärung eines konkreten Vorfalls und nur für dessen Dauer zulässig.

System / Quelle	Protokollierte Daten	Zweck	Speicherdauer
Anmeldung Windows / Active Directory	Benutzerkonto, Zeitpunkt, Arbeitsplatz, Erfolg oder Fehlschlag	Sicherheit, Fehleranalyse	90 Tage
Netzwerk und WLAN	Benutzerkonto, Geräteerkennung, Zeitpunkt, zugewiesene Adresse	Sicherheit, Störungsbehebung	90 Tage
Internetzugang, Firewall und Inhaltsfilter	Zeitpunkt, Benutzerkonto bzw. Adresse, Ziel, Kategorie, Blockierung	Sicherheit, Jugendschutz, Störungsbehebung	90 Tage
E-Mail-Transport	Absender, Empfänger, Zeitpunkt, Zustellstatus, Spam- und Malware-Befund	Zustellung, Malwareschutz	90 Tage
Microsoft 365 (Audit- Log)	Kontoaktivitäten laut Tenant- Konfiguration	Sicherheit, Nachvollziehbarkeit	90 Tage (laut Tenant- Konfiguration)
Datensicherung	systemabhängig	Wiederherstellbarkeit	90 Tage

Kennwortvorgaben: Mindestlänge 14 Zeichen, keine Wiederverwendung für private Dienste. Die Multifaktor-Authentifizierung ist zu aktivieren, sobald sie von der Schule freigegeben wird; der verpflichtende Einführungstermin wird den Nutzerinnen und Nutzern rechtzeitig per E-Mail bekanntgegeben. Die jeweils gültige Fassung dieser Vorgaben macht das IT-Management kund.