KANTON
LUZERN

Bildungs- und Kulturdepartement

WEISUNG

an die Lernenden der kantonalen Schulen für die Verwendung von Informatikmitteln in der Schule

1 Vorbemerkung

Diese Weisung ersetzt die *Weisung an die Lernenden der kantonalen Schulen für die Verwendung von Informatikmitteln in der Schule* vom März 2021.

An den kantonalen Schulen werden in verschiedenen Bereichen Informatikmittel (z.B. kantonale und private Geräte, Applikationen) in der Schule eingesetzt. Damit ermöglichen wir den Lernenden, diese Mittel für die Erreichung der Lernziele zu nutzen und einen zielgerichteten Umgang mit diesen Informatikmitteln zu üben und zu vertiefen.

Der Umgang mit diesen Informatikmitteln braucht gewisse Regeln. Die folgende Weisung dient einerseits dem reibungslosen Einsatz der Informatikmittel in der Schule und legt andererseits die persönliche Verantwortung der Lernenden gegenüber ihren Geräten fest. Die Weisung stützt sich auf § 6 Abs. 2 der kantonalen Informatiksicherheitsverordnung (SRL Nr. 26b).

2 Geltungsbereich

Diese Weisung gilt für Lernende, sofern sie kantonale oder private Informatikmittel in der Schule verwenden. Gemäss § 3 des Informatikgesetzes (SRL Nr. 26) sind Informatikmittel Geräte, Einrichtungen und Dienste, wie insbesondere Computersysteme, Computerprogramme, Kommunikationsdienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen.

3 Verwendung von Informatikmitteln

- In der Schule stehen kantonale Informatikmittel zur Verfügung, dazu zählen unter anderem die Netzwerk- und Druckerinfrastruktur, der Internetzugriff oder die Lernenden-Notebooks (LENO-Geräte). Die Nutzung kantonaler Informatikmittel zu privaten Zwecken, insbesondere für datenintensive Dienste (z. B. Audio- und Videostreaming, Onlinespiele), ist nicht gestattet, sofern keine ausdrückliche Bewilligung der Schulleitung vorliegt.
- Private Informatikmittel (BYOD – Bring Your Own Device) können durch die Schule inventarisiert werden.
- Für BYOD-Geräte wird kein schulinterner technischer Support angeboten.

- Zur Umsetzung des Bildungsauftrags kann die Schule bei Bedarf die kostenlose Installation bestimmter Programme oder Dienste (z. B. Safe Exam Browser) auch auf privaten Geräten vorsehen (siehe dazu §§ 27 ff. Informatiksicherheitsverordnung, SRL Nr. 26b). Wird auf eine Installation verzichtet, liegt die Verantwortung für eine geeignete alternative (technische) Lösung zur Teilnahme am Unterricht bei den Lernenden.
- Der Kanton ist für den Schutz der bereitgestellten Informatikmittel verantwortlich und setzt hierfür geeignete Sicherheitsmassnahmen ein (z. B. Multi-Faktor-Authentifizierung). Für deren Nutzung wird das Vorhandensein eines geeigneten Smartphones vorausgesetzt.

4 Persönliche Verantwortung und Sorgfaltspflichten der Lernenden

4.1 Allgemeine Sorgfaltspflichten

Allgemeine Sorgfaltspflichten gelten sowohl für LENO als auch für BYOD-Geräte. Beim Einsatz der Informatikmittel ist das geltende Recht einzuhalten, insbesondere die Bestimmungen zum Datenschutz, zur Datensicherheit, zum Urheberrecht sowie die vorliegende Weisung.

Zugangsschutz und Authentifizierung

- Alle Informatikmittel, Benutzerkonten, Daten und Dokumente sind durch Passwortschutz, PIN oder biometrische Verfahren (z. B. Fingerabdruck, Gesichtserkennung) vor unberechtigtem Zugriff, Verlust und Diebstahl zu schützen.
- Für kantonale und private Benutzerkonten sind unterschiedliche Passwörter zu verwenden (z. B. nicht dasselbe Passwort für Windows/OS und M365 SLUZ).
- Gemäss der Richtlinie R-204 muss das Gerät mit Benutzernamen und Passwort geschützt sein. Dabei gelten folgende Anforderungen: Das Passwort
    a. muss persönlich sein;
    b. wird nur für einen Zugang verwendet (Unikat);
    c. darf nicht weitergegeben werden;
    d. muss mindestens drei der folgenden Zeichengruppen enthalten:
        - Grossbuchstaben
        - Kleinbuchstaben
        - Ziffern
        - Sonderzeichen;
    e. darf nicht trivial sein und keinen Bezug zum User haben, d.h. Attribute wie User-ID, Name, Vorname oder Geburtsdatum dürfen nicht enthalten sein;
    f. hat eine minimale Länge von 12 Zeichen;
    g. muss nach 365 Tagen gewechselt werden.

  Ein Verdacht auf Offenlegung oder Missbrauch des Passworts muss aus Gründen der Nachvollziehbarkeit von Angriffen unverzüglich der Informatik Ansprechperson der jeweiligen Schule gemeldet werden.
- Anfangspasswörter oder gestohlene/geknackte Passwörter müssen durch ein neues, sicheres Passwort ersetzt werden.

Software und Betriebssystem

- Alle installierten Programme müssen ordnungsgemäss lizenziert sein. Der Einsatz von unerlaubt vervielfältigten Programmen oder Raubkopien ist strikt untersagt.

- Das Betriebssystem und alle Programme müssen regelmässig aktualisiert werden. Windows-Updates und Sicherheitspatches sind innerhalb einer Woche zu installieren.
- Es dürfen nur Anwendungen genutzt werden, die vom Hersteller regelmässig mit Sicherheitsupdates versorgt werden.

Umgang mit externen Geräten

- USB-Datenträger (z. B. USB-Sticks) dürfen nicht unbeaufsichtigt bleiben und sind bei Nichtgebrauch sicher aufzubewahren.
- Unbekannte USB-Datenträger (z. B. auf dem Schulgelände gefundene Sticks) dürfen nicht angeschlossen oder verwendet werden.

Kommunikation

- Für die schulische Kommunikation sind ausschliesslich die offiziellen Schul-E-Mail-Adressen zu verwenden.
- Schulische E-Mail-Adressen sind primär für schulische Zwecke vorgesehen. Eine private Nutzung ist nur in beschränktem Umfang zulässig.
- Die schulische E-Mail-Adresse darf nicht für die Registrierung oder Nutzung von Webdiensten zu privaten Zwecken verwendet werden. Dies gilt insbesondere für Foren, Social-Media-Konten und Newsletter-Abonnements.
- Die Nutzung der schulischen E-Mail-Adresse für kommerzielle Zwecke ist untersagt.
- Der E-Mail-Verkehr der M365 Umgebung unterliegt einer sicherheitsbezogenen Überwachung (siehe dazu §§ 27 ff. Informatiksicherheitsverordnung, SRL Nr. 26b). Das Bildungs- und Kulturdepartement (BKD) behält sich je nach Bedrohungslage vor, ergänzende Sicherheitsmassnahmen zu ergreifen.

Netzwerknutzung

- Der Zugriff auf kantonale Informatikmittel darf nicht über private VPNs (z.B. NordVPN, Surfshark) oder anonymisierte Verbindungen (z. B. Tor-Browser) erfolgen.
- Für die kantonale IT-Umgebung ist ein Geoblocking aktiv. Der Zugriff auf M365 und dessen Funktionen ist ausschliesslich aus der Schweiz sowie den umliegenden Ländern zulässig. Die verbindliche Länderliste sowie weiterführende Informationen sind auf dem schulinternen SharePoint abrufbar (Geoblocking M365 BKD). Versuche, diese Ländersperre zu umgehen, gelten als Verstoss gegen die IT-Richtlinien und können disziplinarische Konsequenzen nach sich ziehen. Bei Schulreisen kann die Aufhebung des Geoblockings durch Meldung der Schuladministration an den Informations- und Informatik Sicherheitsbeauftragten (IISB) des BKD veranlasst werden.
- Die Verwendung des Gäste WLAN ist ausschliesslich für Gäste ohne kantonales Login zugelassen.
- Die Verwendung eines "Hotspots" (z.B. Smartphone) auf dem Schulgelände ist lediglich bei einem Ausfall des kantonalen WLAN gestattet.

Automatische Sperrung

- Bei Nichtverwendung des Geräts ist entweder ein automatisches Sperren nach spätestens 15 Minuten oder ein manuelles Sperren beim Verlassen des Raums erforderlich.

Meldepflicht

- Bei Verlust des Geräts, mit dem auf die kantonale Umgebung zugegriffen wurde, ist unverzüglich die IT-Ansprechstelle der Schule zu informieren.
- Cybervorfälle wie der Verdacht auf Schadsoftware (z. B. Malware), kompromittierte Benutzerkonten (z. B. durch unberechtigten Zugriff) oder Erpressungsversuche mittels Ransomware sind umgehend der Schulleitung und der zuständigen IT-Ansprechstelle zu melden.

- Ebenso meldepflichtig sind sicherheitsrelevante Vorkommnisse wie die versehentliche Preisgabe von Zugangsdaten oder der Zugriff Unbefugter auf das Gerät, mit dem auf kantonale Informatikmittel zugegriffen wird.
- Die Meldung hat so früh wie möglich zu erfolgen, damit geeignete Gegenmassnahmen eingeleitet und weitere Schäden verhindert werden können.

4.2 Zusätzliche Sorgfaltspflichten bei der Verwendung eines BYOD-Gerätes

- Private mobile Endgeräte müssen technisch einwandfrei funktionieren.
- Falls mehrere Personen das Gerät nutzen, müssen separate Benutzerprofil eingerichtet werden. Der Zugriff auf das Profil, mit dem auf der kantonalen Umgebung gearbeitet wird, ist Dritten nicht gestattet.
- Ein Viren- und Malwareschutzprogramm mit aktivierter Echtzeitüberwachung und regelmässigen Updates ist zwingend zu verwenden.
- Private Informatikmittel müssen am „KTLU-Internal" WLAN der Schule angemeldet werden.
- Ein Anschluss über Netzwerkkabel (z.B. USB-C oder RJ45) ist an der Schule nicht erlaubt.

4.3 Zusätzliche Sorgfaltspflichten bei der Verwendung von LENO-Geräten

LENO-Geräte sind Lernenden-Notebooks, welche allen Lernenden der Kantonsschulen während der obligatorischen Schulzeit der Gymnasialbildung als Leihgabe abgegeben werden.

- Das LENO-Gerät ist auf einer harten, ebenen Unterlage (z. B. Tisch) zu verwenden. Die Nutzung auf der Schutzhülle ist zu vermeiden, da dadurch die Lüftung beeinträchtigt und das Gerät beschädigt werden kann.
- Das LENO-Gerät wird nach Schulschluss nach Hause mitgenommen, sofern die Schule keine abschliessbare Aufbewahrungsmöglichkeit bereitstellt. Für den Transport ist die mitgelieferte Schutzhülle zu verwenden. Bei Bedarf sind zusätzliche Vorsichtsmassnahmen zu treffen, um das Gerät angemessen zu schützen.
- Auf dem LENO-Gerät dürfen keine Aufkleber angebracht, Bemalungen vorgenommen, Gehäuseteile geöffnet oder sonstige Veränderungen bzw. Beschädigungen vorgenommen werden.
- Sämtliche Schäden am Gerät sind unverzüglich der zuständigen IT-Ansprechstelle der Schule zu melden.
- Das LENO-Gerät inklusive Zubehör ist am Ende der obligatorischen Schulzeit in funktionstüchtigem Zustand an die Schule zurückzugeben.

5 Missbrauch von Informatikmitteln

Die Informatikmittel dürfen nicht missbräuchlich verwendet werden. Als missbräuchlich gilt jede Nutzung, die gegen diese Weisung oder gegen andere Bestimmungen der Rechtsordnung verstösst, Rechte Dritter verletzt oder bestehende Sicherheitsmassnahmen umgeht (§§ 21ff. Informatiksicherheitsverordnung; SRL Nr. 26b).
Dazu gehören insbesondere:

- Weitergeben oder gemeinsames Nutzen von persönlichen Benutzerkonten, Passwörtern oder anderen Zugangsdaten
- Umgehen oder Deaktivieren technischer Schutzmassnahmen (z. B. Firewalls, Jugendschutzfilter, VPNs, Proxies)

- Nutzung, die den Unterricht stört oder vom Bildungsauftrag ablenkt (z. B. Spiele, Chatprogramme, soziale Medien während der Lektion ohne Auftrag)
- Mutwillige Veränderung oder Beschädigung von Informatikmitteln der Schule oder Dritter (z. B. durch Hacken, Cracken)
- Einsatz von Crypto-Minern auf Informatikmitteln der Schule
- Störung des Betriebs von Computern oder Netzwerken (z. B. Portscanner, Sniffing-Tools, Keylogger, Passwort-Cracker)
- Erstellen, Speichern, Ausführen oder Verbreiten von Fernsteuerungs-, Spionage- oder Schadsoftware (z. B. Viren, Trojaner, Würmer, Scripte)
- Versenden von E-Mails zu Täuschungs- oder Belästigungszwecken sowie von privaten Massensendungen
- Zugriff auf, sowie Erfassung, Verarbeitung, Speicherung oder Übermittlung von Daten mit rassistischem, sexistischem oder pornografischem Inhalt
- Illegales Kopieren von Daten oder Software jeglicher Art
- Illegales Bereitstellen oder Verbreiten urheberrechtlich geschützter Werke (z. B. Filme, Musik, Fotos)
- Anfertigen und Verbreiten von Bild- oder Tonaufnahmen ohne ausdrückliche Zustimmung der betroffenen Person

6 Kontroll- und Überwachungsmassnahmen

Zur Gewährleistung der Sicherheit der kantonalen Informatikmittel werden auf der kantonalen Infrastruktur geeignete technische und organisatorische Massnahmen ergriffen. Auf BYOD und LENO-Geräten installiert der Kanton keine Systemüberwachungssoftware.
Zur Kontrolle, ob die Weisung in Bezug auf den Einsatz von privaten Geräten und LENO-Geräten eingehalten wird, ist der IISB des BKD berechtigt, von den Lernenden einen entsprechenden Nachweis einzufordern (z.B. Version Virenschutz, Version Betriebssystem).

7 Disziplinarmassnahmen

Bei Verstoss gegen diese Weisung oder missbräuchlicher Verwendung von Informatikmitteln können disziplinarische Massnahmen ergriffen werden. Anwendbar sind die massgebenden Bestimmungen über die Disziplinarordnung. Die Strafverfolgung und die Geltendmachung allfälliger Schadenersatzforderungen bleiben vorbehalten.

8 Haftung

Wird der Schule oder einem Dritten ein Schaden zugefügt, kann eine Schadenersatzpflicht entstehen (unerlaubte Handlung, Art. 41 OR). Für Verlust und Beschädigung am eigenen Informatikmittel haften die Lernenden selbst. Soweit die Rechtsordnung dies zulässt, schliesst die Schule jede Haftung aus.

9 Beendigung des Ausbildungsverhältnisses

Mit dem Austritt aus der Schule wird das schulische Benutzerkonto gelöscht. Die rechtzeitige Übertragung persönlicher Daten auf ein eigenes Speichermedium oder in einen Cloudspeicher liegt in der Eigenverantwortung des Lernenden.

10 Schlussbestimmungen

Diese Weisung tritt am 20.10.2025 in Kraft.

Luzern, 13. Oktober 2025

Die Departementssekretärin

Qualifizierte Elektronische
Signatur von:
Gabriela Franziska Schmidt

20251013/12:15 UTC+02

Gaby Schmidt

Die Organisations- und Informatikbeauftrage

Qualifizierte Elektronische
Signatur von:
Franziska Wilhelm
Organisations- und Informatikbeauftragte
20251013/11:26 UTC+02

Franziska Wilhelm

Dokumentinformationen

Dokumentenname	Weisung an die Lernenden der kantonalen Schulen für die Verwendung von Informatikmitteln in der Schule
Ablagepfad	

Versionenkontrolle

Version	Datum	Autor	Bemerkung
0.1	10.09.2025	IISB BKD	Erstellung
0.2	16.09.2025	IISB BKD	Verarbeitung Review PID BKD
0.3	30.09.2025	IISB BKD	Verarbeitung Review OpSec DIIN
1.0	13.10.2025	OIB BKD	Veröffentlichte Version