



SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Richtlinie

Richtlinie zur Nutzung der Schulinformatik



SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Herausgeber

Schulamt (SA)
Giessenstrasse 3
Postfach 684
9490 Vaduz
T +423 236 67 70
www.sa.llv.li

 Schulamt auf Facebook

 Schulamt auf LinkedIn

Kontakte

Zentrum für Schulmedien
Pädagogisches Medienmentorat
Technische IT-Koordination
Pflugstrasse 28
9490 Vaduz
T +423 236 7685
dms@llv.li

Datenschutzkoordination Schulamt/Daten-
schutzbeauftragte der öffentlichen Schulen
Giessenstrasse 3
Postfach 684
9490 Vaduz
T +423 799 63 98
datenschutz@schulen.li

Version 4.0
Stand, 01.08.2026

Copyright

Wiedergabe unter Angabe
des Herausgebers gestattet.
©Schulamt

Präambel

Ziel dieser Richtlinie ist es, den Nutzerinnen und Nutzern im Sinne von Ziff. 1.1. dieser Richtlinie der Schulinformatik den Umgang mit den Informatikmitteln und die entsprechenden Regelungen näher zu bringen und einen Überblick zum Thema eines sicheren und rechtskonformen Umgangs mit der Schulinformatik darzulegen.

Die offizielle und letztgültige Version ist auf der Internetseite des Schulamtes via <https://www.llv.li/de/landesverwaltung/schulamt/datenschutz> abrufbar.

Für Fragen zu dieser Richtlinie stehen der Technische IT-Koordinator (SIK) und der Pädagogische Medienmentor (PMM) beim Zentrum für Schulmedien sowie der/die Datenschutzkoordinator/in / Datenschutzbeauftragte der öffentlichen Schulen unter den oben angeführten Adressen zur Verfügung.

Erziehungsberechtigten von Schülerinnen und Schülern an den öffentlichen Schulen im Fürstentum Liechtenstein ist diese Richtlinie und weitere Handreichungen mit Einschulung ihres Kindes bzw. bei Änderungen in geeigneter Form durch die zuständige öffentliche Schule zur Kenntnis zu bringen.

Soweit Verweise auf gesetzliche Bestimmungen enthalten sind, sind diese in ihrer jeweils gültigen Fassung anzuwenden.

Inhalt

Präambel	3
Inhalt.....	4
Rechtsgrundlage.....	4
1. Geltungsbereich	5
2. Zweck	6
3. Datenschutz	6
4. Allgemeine Grundsätze	6
5. Zugang zur Nutzung (Authentifizierung).....	7
6. Nutzung des Internets.....	8
7. Nutzung des E-Mail-Service	8
8. Nutzung von Social Media	8
9. Einsatz von Lernapplikationen	8
10. Nutzung des Outlook-Kalenders	8
11. Nutzung der Netzlaufwerke und des lokalen Laufwerks	8
12. Nutzung privater Geräte im Schulunterricht (BYOD = bring your own device).....	9
13. Herausgabe von Daten an externe Partner (z.B. Dienstleister, IT-Berater, usw.)	10
14. Clean Screen Policy («sauberer Bildschirm»)	11
15. Missbräuchliche Nutzung und sonstige sicherheitsrelevante Vorfälle	11
16. Massnahmen zur Feststellung von Missbrauch.....	15
17. Massnahmen bei sicherheitsrelevanten Vorfällen	14
18. Sanktionen.....	15
19. Urheber- und Lizenzrechte	16
20. Schlussbestimmungen	14

Rechtsgrundlage

Gestützt auf Art. 10¹ (i.V.m Art. 24a Schulorganisationsverordnung²) und Art. 106 Bst. a UBst. ee³ des Schulgesetzes erlässt das Schulamt folgende Richtlinie zur Nutzung der Schulinformatik.

1. Geltungsbereich

- 1.1. Die Richtlinie gilt für alle Nutzerinnen und Nutzer der Schulinformatik. Darunter sind insbesondere die Schülerinnen und Schüler, das Lehr-, Assistenz- und Schulpersonal sowie das Verwaltungspersonal der öffentlichen Schulen des Fürstentums Liechtenstein zu verstehen.
- 1.2. Die Richtlinie regelt den Gebrauch von Schulinformatikmitteln sowie des Schulnetzwerkes⁴. Darunter fallen insbesondere Geräte wie Tablets oder Convertibles. Als Schulinformatikmittel gelten sowohl die an den Schulen eingesetzten physischen Endgeräte und die eingesetzten digitalen Lehrmittel (Software, Lernplattformen, webbasierte Dienste sowie Cloud-Dienste) als auch anderweitige technische, elektronische und digitale Schulmaterialien, die im Schulunterricht eingesetzt werden.
- 1.3. Die vom Schulamt und vom Amt für Informatik zur Verfügung gestellten Schulinformatikmittel sind grundsätzlich nur für schulspezifische Zwecke einzusetzen. Sie dürfen nicht an Dritte weitergegeben werden, weder kurzfristig noch für einen längeren Zeitraum.
- 1.4. Spezifische Richtlinien und Handreichungen des Schulamtes und des Amtes für Informatik und deren Nutzungen bleiben vorbehalten. Darunter fallen insbesondere das IT-Anwender-Reglement, die [Handreichung «Datenschutz an Schulen»](#), die Wegleitung «Informationssicherheit & Datenschutz» sowie sinngemäss das «Remote Work Reglement» usw. in ihrer jeweils gültigen Fassung (abrufbar über das Intranet der Liechtensteinischen Landesverwaltung, kurz LLV).

¹ Art. 10 SchulG, LGBI. 1972.007 idF LGBI. 2007.098 lautet:

1) Das Schulamt bestimmt auf der Grundlage des Lehrplans, welche Lehrmittel in den öffentlichen Schulen vorgeschrieben sind, und beschafft diese Lehrmittel für die einzelnen öffentlichen Schulen.

2) Auf der Grundlage des Lehrplans können die öffentlichen Schulen im Rahmen ihres Budgets weitere Lehrmittel beschaffen und einsetzen.

² Art. 24a SchulOV, LGBI. 2004.154 idF LGBI. 2007.362 unter Kapitel VIIa (Lehrmittel und Schulmaterial) lautet:

1) Als Lehrmittel gelten die aufgrund des Lehrplanes im Unterricht eingesetzten Medien, insbesondere Printmedien (z.B. Bücher, Arbeits- und Lösungshefte), elektronische Medien (z.B. Compact Discs, Digital Versatile Discs) und elektronische Lernplattformen.

2) Als Schulmaterial gilt, vorbehaltlich Abs. 3, das aufgrund des Lehrplanes für den Unterricht zwingend benötigte Material (z.B. Reprographien, Taschenrechner, Zirkel).

3) Nicht als Schulmaterial gelten insbesondere persönliche Kleidung (z.B. für den Sportunterricht) und persönliche Utensilien (z.B. Schreibzeug und -material, Schultasche).

³ Art. 106 Bst. a UBst. ee SchulG, LGBI. 1972.007 idF LGBI. 2011.553 lautet: Dem Schulamt obliegen folgende Aufgaben: [...]

a) Aufrechterhaltung und Weiterentwicklung des Schulbetriebs in den öffentlichen Schulen, insbesondere: [...]
ee) Führung von zentralen Diensten, insbesondere in den Bereichen Schulpsychologie, Pädagogik, Schulsozialarbeit, Schulinformatik, Schulmedien, Administration des Schulleitungs- und Lehrpersonals, Verwaltung von Lehrer- und Schülerdaten sowie Sachadministration;

⁴ Ein Schulnetzwerk ist ein speziell für den Unterricht und den Schulalltag eingerichtetes Computernetzwerk, das von Schulpersonal und Lernenden genutzt wird. Es ist die technische Grundlage, damit Schülerinnen, Schüler und Lehrkräfte digital arbeiten können – mit sicheren Logins, Zugriff auf Unterrichtsmaterial, geteilten Ordnern, Internetfiltern und klar geregelten Rechten.

- 1.5. Schulorganisatorische Zuständigkeiten sind in der Richtlinie über die Anrechenbarkeit von Tätigkeiten sowie in Pflichtenheften geregelt.

2. Zweck

Die Richtlinie bezweckt die Sicherstellung einer rechtmässigen Nutzung und eines störungsfreien Betriebs der Schulinformatik, der Datensicherheit und den sicheren und wirtschaftlichen Einsatz der Informatikmittel durch die Nutzerinnen und Nutzer.

3. Datenschutz

- 3.1 Detaillierte Hinweise und Empfehlungen zum Datenschutz an den öffentlichen Schulen enthält die [Handreichung über den Datenschutz an öffentlichen Schulen](#).
- 3.2 Weitere allgemeine Hinweise zum Datenschutz sind auf der Website des Schulamtes, der [Datenschutzstelle des Fürstentums Liechtenstein](#) sowie der [Fachstelle Datenschutz](#) zu finden.

4. Allgemeine Grundsätze

- 4.1 Nutzerinnen und Nutzer tragen die Verantwortung für eine richtlinienkonforme Nutzung der vom Schulamt zur Verfügung gestellten Schulinformatikmittel.
- 4.2 Die Schulleitung sowie das Lehr- und Schulpersonal setzt seine Schülerinnen und Schüler in die Lage, die Schulinformatikmittel richtlinienkonform zu nutzen und berücksichtigt dabei die einschlägigen Handreichungen und Leitlinien des Schulamtes.
- 4.3 Erforderlichenfalls gibt die Schule den Eltern bzw. den Erziehungsberechtigten und den Schülerinnen und Schülern gestützt auf diese Richtlinie Merkblätter zur Nutzung der Schulinformatik ab.
- 4.4 Die Informatikmittel stehen grundsätzlich nur für schulische Zwecke zur Verfügung, ausgenommen sind «Bring Your Own Device - Geräte (BYOD-Geräte)» ausserhalb der Schule. Jede ausserschulische kommerzielle Verwendung ist ausdrücklich verboten. Private Nutzung ist ohne Zustimmung der zuständigen Lehrperson oder der vorgesetzten Stelle nur für unaufschiebbare, unbedingt erforderliche Angelegenheiten und in zeitlich eingeschränktem, geringfügigem Ausmass erlaubt, sofern es dadurch zu keiner Vernachlässigung der schulischen oder dienstlichen Pflichten kommt. In keinem Fall darf dadurch der Betrieb gestört werden, zusätzliche Sicherheitsrisiken geschaffen werden oder Kosten entstehen. Der jederzeitige Widerruf der ausnahmsweisen erlaubten privaten Nutzung, vor allem bei missbräuchlicher Verwendung, bleibt vorbehalten.
- 4.5 Die Informatikmittel sind sorgfältig zu nutzen und zu verwahren. Es ist grundsätzlich alles zu vermeiden, was den Betrieb der Schulinformatik beeinträchtigt sowie Schäden am System oder bei anderen Nutzerinnen und Nutzern verursacht. Die Schulinformatikmittel sind sicher zu verwahren und erforderlichenfalls zu versperren.
- 4.6 Bei Reparaturen von beschädigten Geräten wird eine Reparaturpauschale von 100 CHF eingefordert. Wird nachgewiesen, dass der Schaden ohne eigenes Verschulden entstanden ist, wird von der Pauschale abgesehen.
- 4.7 Im Falle von Diebstahl oder schweren Schäden, die nicht durch den erweiterten Garantievertrag abgedeckt sind, wird der entsprechende Betrag (Neuwert bzw. Restwert) für Ersatz oder Reparatur den Erziehungsberechtigten des Kindes in Rechnung gestellt.

Wird nachgewiesen, dass der Schaden ohne eigenes Verschulden entstanden ist, wird von einer Kostenbeteiligung abgesehen.

- 4.8 Das Schulgerät ist mit einem sicheren Passwort zu schützen (siehe 5.3). Das Passwort muss an sicherer Stelle aufbewahrt werden und darf keinesfalls auf dem Endgerät notiert werden.
- 4.9 Geräte (einschliesslich Peripheriegeräte wie Stifte, Kabel etc.) sind jederzeit sorgfältig aufzubewahren, vor Fremdzugriffen zu schützen und sorgsam zu behandeln. Verstösse können durch das Schulamt geahndet werden.
- 4.10 Die Geräte sind aufgeladen und betriebsbereit zur Schule zu bringen.
- 4.11 Schuleigene Geräte und Materialien sowie die im Pflichtschulbereich ausgegebenen Endgeräte der Liechtensteinischen Landesverwaltung müssen über das Amt für Informatik erworben sowie ersetzt werden (bspw. defekte Netzgeräte, Adapter, Stifte, Anschlusskabel).
- 4.12 Schuleigene Geräte und Materialien sowie die im Pflichtschulbereich ausgegebenen Endgeräte der Liechtensteinischen Landesverwaltung dürfen nicht beklebt oder anderweitig verändert werden.
- 4.13 Schul- und Lehrpersonal sowie Eltern sind verantwortlich für regelmässige Gespräche mit den Kindern und Jugendlichen über die sichere und verantwortungsbewusste Nutzung der Geräte. Dadurch wird ein besseres Verständnis für die Nutzung und das Bewusstsein für die digitale Sicherheit gefördert.

5. Zugang zur Nutzung (Authentifizierung)

- 5.1 Benutzername und Passwörter sind persönlich und nicht übertragbar. Passwörter dürfen weder ausgehändigt noch bekannt gegeben werden; das gilt auch gegenüber Vorgesetzten, Stellvertretungen, anderen Mitarbeitenden, Lehr- und Schulpersonal usw. Es gilt auch gegenüber Mitarbeitenden des Amts für Informatik (z.B. Helpdesk) oder anderen Personen, welche für die einwandfreie Verwendung der Schulinformatikmittel und für den Support zuständig sind.
- 5.2 Der Benutzername und die entsprechenden Pseudonyme (die...@schulen.li-Adressen der Lehrpersonen sowie der Schülerinnen und Schüler haben ein automatisch generiertes Pseudonym) werden vom Schulamt respektive dem Amt für Informatik vorgegeben und zugeteilt.
- 5.3 Das Passwort muss von dem Nutzer bzw. der Nutzerin festgelegt und in vorgegebenen Zyklen erneuert werden. Es muss aus mindestens zehn Zeichen bestehen und folgende Kriterien erfüllen:
 - Grossbuchstaben (A-Z)
 - Kleinbuchstaben (a-z)
 - Ziffern (0-9)
 - Sonderzeichen (bspw. !, %, \$ oder #)
- 5.4 Für die Festlegung eines sicheren Passworts wird ein sogenannter Merksatz (Passphrase) empfohlen. Beispielsweise: «Mir wird am 1.5. ein Stern (*) am Hollywood Boulevard verliehen!» ergibt das sichere Passwort: Mw1.5.e*aHBv! Diese Passphrase ergibt ein 14-stelliges Passwort mit Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen. Dies entspricht den Vorgaben des Amts für Informatik. Passwörter müssen nach Anweisung des Amts für Informatik einmal pro Jahr geändert werden.

Falls der Verdacht besteht, dass das Passwort Dritten bekannt ist (zum Beispiel, wenn eine Person die Passworteingabe beobachtet hat), muss das Passwort unverzüglich geändert werden. Betrifft der Verdacht Passwörter von Fach-Applikationen, ist unverzüglich das Amt für Informatik zu informieren.

- 5.5 Zur Authentifizierung von Nutzern des Schulnetzes wurde vom Amt für Informatik eine Multi-Faktor-Authentifizierung (MFA) eingeführt. Schülerinnen und Schüler sowie das Lehr- und Schulpersonal sowie Schulamtsmitarbeitende haben einmalig eine MFA für den Zugriff auf Microsoft-365-Systeme (SharePoint, Outlook, Teams, OneDrive etc.) einzurichten. Diese Massnahme erfolgt zur Gewährleistung eines dem Stand der Technik entsprechenden Datenschutzes und aus Gründen der Informationssicherheit. Innerhalb des Schulnetzwerks erfolgt die Authentifizierung anhand der Gerätekennung, ausserhalb (etwa bei Zugriff auf MS-365 aus dem Heimnetzwerk) kann die Authentifizierung über unterschiedliche Faktoren (Benutzername und Passwort plus Authenticator App, TOTP-Token, Windows-Hello) erfolgen.

6. Nutzung des Internets

- 6.1 Grundsätzlich ist die Nutzung des Internets nur erlaubt, wenn sie schulischen Zwecken dient. Für die private Nutzung gilt Ziff. 4.4 sinngemäss.
- 6.2 Verboten ist der Besuch von Internetseiten mit pornographischen oder sexistischen Darstellungen oder mit extremistischen, gewaltverherrlichenden, rassistischen oder sonst strafrechtlich relevanten Inhalten. Ebenso ist der Besuch einschlägiger Spieleseiten verboten. Der Besuch verbotener Seiten und Seiten mit offensichtlich schulfremden Inhalten wird gegebenenfalls vom Amt für Informatik protokolliert und aufbewahrt.
- 6.3 Für einen datenschutzkonformen und den Vorgaben des Jugendschutzes entsprechenden Internetzugang wurde vom Amt für Informatik flächendeckend für sämtliche vom Schulamt und AI ausgegebenen Endgeräte ein sogenannter Web Proxy eingeführt. Dieser verhindert, dass eine den Endnutzenden zuordenbare IP-Adresse an externe Webdienstanbieter übermittelt wird und blockiert verschiedene Websitekategorien. Eine Umgehung dieser Schutzfunktionen stellt eine missbräuchliche Verwendung der zur Verfügung gestellten Schulinformatikmittel dar (vgl. Ziff. 15).

7. Nutzung des E-Mail-Service

- 7.1 Zur schulinternen Kommunikation (z.B. via Teams oder Outlook) ist die persönliche E-Mail-Adresse (name.vorname@schulen.li) zu verwenden. Private E-Mail-Adressen (z.B. GMX, Gmail, Hotmail u.v.a.) dürfen nicht zu schulischen Zwecken und zur schulischen Kommunikation zwischen Lehrpersonen bzw. dem Schulpersonal und Schülerinnen und Schülern verwendet werden.
- 7.2 Schülerinnen und Schülern sowie dem Lehrpersonal werden zusätzlich zur persönlichen E-Mail-Adresse, die eine Kennung im Klarnamen aufweist, eine pseudonymisierte E-Mail-Adresse zugewiesen, die sich zufallsgeneriert aus einem Dialektwort und einer Ziffernfolge zusammensetzt. Diese E-Mail-Adresse ist für eine Anmeldung oder Registrierung zur Nutzung externer Webdienste oder Applikationen zu verwenden. Ausgenommen hiervon ist die Plattform schulen.li.
- 7.3 Für die private Nutzung des E-Mail-Service gilt Ziff. 4.4 sinngemäss.

- 7.4 Es ist verboten, E-Mails mit pornographischen, sexistischen, extremistischen, Gewalt verherrlichenden, rassistischen oder sonst strafrechtlich relevanten Inhalten zu versenden. Wer E-Mails mit solchen Inhalten erhält, muss dies der Lehrperson oder der Schulleitung oder dem Schulamt melden.
- 7.5 Die Einrichtung einer dauerhaften Weiterleitung von E-Mails an private Konten ist untersagt.
- 7.6 Authentifizierte Nutzerinnen und Nutzer haben über das Webportal der Schulen (<https://outlook.office.com>) Zugang zu ihren E-Mails.
- 7.7 Mit dem Schul- bzw. Dienstaustritt wird das E-Mail-Konto im Auftrag des Schulamtes vom Amt für Informatik deaktiviert. Die Löschung des E-Mail-Kontos geschieht im Auftrag des Amtes für Informatik drei Monate nach dem Schul- bzw. Dienstaustritt. Abweichungen von diesen Vorgaben müssen beim Schulamt beantragt werden.

8. Nutzung von Social Media

- 8.1 Social Media dürfen nur im Rahmen des Lehrplans und unter Beachtung der rechtlichen Bestimmungen, insbesondere jugendschutz- sowie datenschutzrechtlicher Bestimmungen, für schulische Zwecke genutzt werden.
- 8.2 Technische und organisatorische Sicherheitsmassnahmen bleiben vorbehalten, insbesondere zur Bekämpfung von Cybermobbing.

9. Einsatz von Lernapplikationen

- 9.1 Hinsichtlich der Freigabe digitaler Lehrmittel (inkl. Cloud-Lösungen) gelten die gesetzlichen Zuständigkeiten (Art. 10 Schulgesetz).
- 9.2 Vor der Freigabe klären die nach Art. 10 Schulgesetz zuständigen Stellen ab, ob die technischen und datenschutzrechtlichen Voraussetzungen dafür erfüllt sind. Hierfür haben die Pädagogischen Medienkoordinatoren und -koordinatorinnen der Schulen einen Antrag beim Zentrum für Schulmedien einzubringen. Das Schulamt hat hierzu eine Checkliste für das Lehr- und Schulpersonal ausgegeben.
- 9.3 Für den datenschutzkonformen Einsatz digitaler Lehrmittel ist der [konsolidierte Leitfaden](#) vom Schulamt zu berücksichtigen.

10. Nutzung des Outlook-Kalenders

- 10.1 Es wird empfohlen, die Option «alle Details» gegenüber Nutzerinnen und Nutzern innerhalb der eigenen Organisationseinheit (Schule) standardmässig freizugeben.
- 10.2 Für Termine, welche nicht für die Allgemeinheit bestimmt sind, soll jeweils die Option «privat» gesetzt werden.
- 10.3 Bei Abwesenheiten ist der Abwesenheitsassistent zu aktivieren und anzugeben, wer die Stellvertretung übernimmt und – soweit möglich – ab wann der Empfänger erneut verfügbar und erreichbar ist.

11. Nutzung der Netzlaufwerke und des lokalen Laufwerks

- 11.1 Die verschiedenen Netzlaufwerke stehen ausschliesslich für schulbezogene Dokumente zur Verfügung. Für die Speicherung von privaten Daten gilt Ziff. 4.4. sinngemäss. Bei ausnahmsweise erlaubter privater Nutzung im Sinne von Ziff. 4.4 hat eine Kennzeichnung im Dateinamen oder in einem Dateiordner mit «PRIVAT» zu erfolgen und sind diese Daten ausschliesslich im P-Laufwerk, sofern ein solches zur Verfügung steht, abzuspeichern.

Die LLV haftet weder für den Verlust noch für die Beschädigung von persönlichen Daten, welche auf Informatikmitteln der LLV verarbeitet werden.

- 11.2 Für die Netzlaufwerke bestehen spezifische Zugriffsberechtigungen. Auf Antrag und in Rücksprache mit der festgelegten vorgesetzten Stelle kann das Amt für Informatik organisationsübergreifende Zugriffsberechtigungen einrichten.
- 11.3 Soweit für die digitale Aktenablage und -verwaltung eine eigenständige Software bzw. Fachapplikationen zur Verfügung gestellt wurde (z.B. LiSA oder für Schulamts-mitarbeitende (LiVE), ist diese zu verwenden. Aktendoppel und Aktenkopien sind zur Wahrung des Grundsatzes der Datenminimierung und Datensparsamkeit zu vermeiden bzw. zu löschen, wenn das erstellte Doppel nicht länger benötigt wird.
- 11.4 Daten auf den Netzlaufwerken werden mehrmals täglich gegen Datenverlust gesichert und es werden Vorgängerversionen gespeichert. Wiederherstellungen von Vorversionen oder Datensicherungen müssen beim Amt für Informatik in Auftrag gegeben werden.
- 11.5 Nach dem Austritt werden die Daten auf sämtlichen Laufwerken gelöscht. Nutzerinnen und Nutzern wird empfohlen, diese Laufwerke vor dem Austritt zu bereinigen, indem relevante Dateien in die entsprechenden Dateiordner abgelegt werden und allfällige persönliche Dateien auf eigenen Medien gesichert werden.

12. Nutzung privater Geräte im Schulunterricht

- 12.1 «Bring your own device» (BYOD) bezeichnet den Einsatz privater mobiler Endgeräte im Schulunterricht durch Lehr- und Schulpersonal sowie durch Schülerinnen und Schüler. Auf der Sekundarstufe II ist die Nutzung privater Geräte durch Schülerinnen und Schüler im Schulunterricht verpflichtend vorgesehen, da nicht wie im Pflichtschulbereich Endgeräte unentgeltlich zur Verfügung gestellt werden und vom Amt für Informatik zentral verwaltet werden.
- 12.2 Um einen störungsfreien Einsatz der Geräte zu Schulunterrichtszwecken zu gewährleisten, sind die Geräte aufgeladen und betriebsbereit zur Schule zu bringen.
- 12.3 Die Nutzung der Schulinformatik durch private Geräte ist unter Vorbehalt von Ziff. 12.4.-12.8. erlaubt.
- 12.4 Die verpflichtende Nutzung von Webanwendungen sowie Applikationen durch private Geräte ist auf lizenzierte Anwendungen beschränkt. Derzeit sind dies beispielsweise: Office 365, Outlook Online (E-Mail, Kalender, Kontakte), MS-Teams, SharePoint. Diese Anwendungen sind verpflichtend zu nutzen.
- 12.5 Eine darüberhinausgehende Nutzung nicht lizenzierter Webanwendungen oder Applikationen oder Internetseiten ist freiwillig. Bei Verwendung solcher Software bzw. digitaler Lehrmittel ist darauf zu achten, dass Schülerinnen und Schüler angeleitet werden, sich mit der zur Verfügung gestellten pseudonymisierten E-Mail-Adresse anzumelden (sofern eine Anmeldung oder Registrierung vom Softwareanbieter gefordert wird).
- 12.6 Informationen und Datensätze, welche dem Dienstgeheimnis des Lehr- und Schulpersonals unterliegen und/oder personenbezogene Daten Dritter enthalten und somit dem Datenschutz unterstehen, dürfen nur in begründeten und dokumentierten Ausnahmefällen auf private Geräte übertragen, verarbeitet oder abgespeichert werden. In diesen Fällen hat das Schul- und Lehrpersonal eine erweiterte Sorgfaltspflicht und Verantwortung für den Schutz der Daten und eine Übertragung sollte vorgängig mit der vorgesetzten Schulleitung oder dem Schulamt geklärt werden.

- 12.7 Die Nutzerinnen und Nutzer sind verpflichtet, die Software ihres privaten Gerätes auf dem neuesten Stand zu halten (z.B. Windows, iOS, MacOS, Android etc.), regelmässig Updates vorzunehmen und eine Sicherheitssoftware (zB Endpoint Protection) zu installieren. Die Verantwortung für eine datenschutzkonforme Verwaltung und Konfiguration von BYOD-Geräten liegt bei den Erziehungsberechtigten bzw. den volljährigen Schülerinnen und Schülern.
- 12.8 Bei der Verwendung privater Datenträger und Peripheriegeräte, wie USB-Sticks, Kameras, Plug- and Play Drucker, Ladegeräte, ist auch auf BYOD-Geräten Vorsicht geboten. Es wird dringend empfohlen, auf die Nutzung von Werbegeschenken (z.B. USB-Sticks oder ähnliche Artikel mit USB-Stecker) zu verzichten, um ein unbeabsichtigtes Hochladen von Malware und Spyware zu verhindern.

13. Herausgabe von Daten an externe Partner (z.B. Dienstleister, IT-Berater usw.) durch das Schulpersonal und das Schulamt

Ist es erforderlich und zweckmässig, Daten an externe Partner herauszugeben, beispielsweise im Rahmen eines Dienstleistungsauftrags zu schulspezifischen Zwecken, so haben die Empfänger zwingend ein Non-Disclosure Agreement (Geheimhaltungsvereinbarung entsprechend dem Template des Amts für Informatik) und gegebenenfalls einen Auftragsverarbeitungsvertrag gemäss Art. 28 Abs. 3 DSGVO zu unterzeichnen.

14. Clean Screen Policy («sauberer Bildschirm»)

- 14.1 Bei einem bloss vorübergehenden Verlassen des Arbeitsplatzes bzw. des Endgeräts ist die Bildschirmsperre zu aktivieren. Eine automatische Sperre bei Nicht-Aktivität ist auf höchstens 10 Minuten eingestellt.
- 14.3 Bei Verlassen des Arbeitsplatzes hat sich jeder Endnutzer von den Endgeräten abzumelden.
- 14.4 Bei längerem Nichtgebrauch und vor dem Verstauen in den Schutzhüllen sind Endgeräte auf Standby zu stellen oder ganz auszuschalten.

15. Missbräuchliche Nutzung und sonstige sicherheitsrelevante Vorfälle

- 15.1 Ein Missbrauch liegt vor, wenn einschlägige gesetzliche Bestimmungen (etwa des Strafrechts) und die Vorgaben dieser Richtlinie verletzt werden. Ein Verdacht einer nicht sachgemässen Nutzung und/oder der Begehung solcher vorschriftswidrigen Handlungen ist umgehend der Schulleitung, respektive dem Schulamt zu melden, das die weiteren Abklärungen gemäss Ziff. 16, Ziff. 17 oder Ziff. 19 prüft.
- 15.2 Den Anweisungen des Schulamtes bzw. der Schulleitung sowie des Amts für Informatik zur Verhinderung missbräuchlicher Nutzung der Schulinformatikmittel oder zur Abhilfe bereits erfolgter Verstösse oder eines Missbrauchs ist zu folgen.
- 15.3 Verboten im Sinne dieser Richtlinie oder aufgrund rechtlicher Bestimmungen sind insbesondere:
 - das Herunterladen, das Speichern, das Verbreiten, die Installation, die Ausführung oder die Verwertung als auch jegliche andere Verarbeitung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder anderen Informationen,

- jeglicher Einsatz der Schulinformatikmittel bzw. von Informatikmitteln allgemein, der die Privatsphäre oder die Persönlichkeit von Personen verletzen könnte,
 - die Nutzung von Fachinformationssystemen ohne entsprechenden Geschäftsfall durch das Schulpersonal,
 - die Verwendung der Schulinformatikmittel für Angriffe auf andere Systeme, zur Verteilung von unerwünschten Massen-E-Mails (Spam) sowie für jede weitere nicht zweckgemässe Tätigkeit wie z.B. übermässige, private Nutzung des Internets oder komplette Zweckentfremdung dessen,
 - das Ausspionieren fremder Passwörter und Daten,
 - widerrechtliches Kopieren, Verändern, Löschen oder Unbrauchbarmachen von Daten,
 - die Bereitstellung von Netzwerk- und Applikationszugängen und/oder Weitergabe von Daten für Dritte,
 - die Verbindung privater Hardware mit der Informatikinfrastruktur der LLV oder die Installation und Verwendung privater Software auf derselben (ausgenommen BYOD auf der Sekundarstufe II),
 - Unbefugtes Verändern der Konfiguration von Hard- und Software der Informatikmittel,
 - die Beanspruchung von Ressourcen (insbesondere Arbeitszeit, Bandbreite, Datenmenge, Speicherplatz etc.) für private Zwecke entgegen Ziff. 4.4.,
 - die geschäftliche Nutzung der Schulinformatikmittel (z.B. im Rahmen eines Nebenerwerbs),
 - die Benutzung der Infrastruktur für Hacking oder Cracking anderer oder eigener Systeme, insbesondere das Kopieren oder Einsetzen von entsprechender Software,
 - das Verbreiten von Meinungsäusserungen auf Chat-Foren, in Newsgroups, in sozialen Netzwerken und ähnlichem, die dem Ansehen des Landes oder seinen Bediensteten, dem liechtensteinischen Schul- und Bildungswesen, den öffentlichen Schulen, dem Schul- und Lehrpersonal und Schülerinnen und Schülern im Fürstentum Liechtenstein schaden können,
 - die Synchronisation dienstlicher Daten auf private Informatikmittel.
- 15.4 Falls Nutzerinnen und Nutzer beim Einsatz von Informatikmitteln oder Dokumenten Unregelmässigkeiten (wie Defekte, Virenbefall oder Missbräuche) feststellen, sind sie verpflichtet, diese dem technischen Medienkoordinator oder dem Amt für Informatik zu melden.
- 15.5 Sicherheitsrelevante Vorfälle im Sinne des Art. 33 DSGVO sind vom Schulpersonal dem oder der schulischen Datenschutzbeauftragten / Datenschutzkoordinator/in **unverzüglich** zu melden.

16. Massnahmen zur Feststellung von Missbrauch

Bei Verdacht oder Feststellung einer missbräuchlichen Nutzung der Schulinformatikmittel sind die erforderlichen Massnahmen umgehend und verhältnismässig zu ergreifen. Dabei sind insbesondere der Schutz von Personen, Daten, Systemen sowie der ordnungsgemässe Schulbetrieb sicherzustellen. Die einschlägigen gesetzlichen Bestimmungen, insbesondere zum Datenschutz und zum Persönlichkeitsschutz, sind einzuhalten.

Es werden organisatorische und technische Schutzmassnahmen gegen Missbrauch und technischen Schaden durch das Schulamt und das Amt für Informatik getroffen. Diese Massnahmen werden regelmässig auf den neuesten Stand der Technik geprüft und erforderlichenfalls angepasst.

- 16.1 Abklärung und Dokumentation: Die Schulleitung und / oder das Schulamt stellt sicher, dass der Vorfall sachgerecht geklärt und dokumentiert wird. Dazu gehören insbesondere:
- Ermittlung von Art, Umfang und Ursache des Vorfalls;
 - Prüfung möglicher Verstösse gegen gesetzliche Vorschriften oder interne Richtlinien;
 - Zusammenarbeit mit dem Amt für Informatik und der oder dem schulischen Datenschutzbeauftragten / Datenschutzkoordinator/in sowie, falls erforderlich, mit der Datenschutzstelle;
 - Protokollierung der getroffenen Massnahmen und Feststellungen.
- 16.2 Sofortmassnahmen: Je nach Art und Schwere des Vorfalls können insbesondere folgende Sofortmassnahmen getroffen werden:
- vorübergehende oder dauerhafte Sperrung von Benutzerkonten, Zugängen oder einzelnen Diensten;
 - Sicherung relevanter Daten, Logfiles und Beweismittel zur weiteren Abklärung;
 - Trennung betroffener Geräte vom Netzwerk;
 - Anordnung technischer Schutzmassnahmen zur Verhinderung weiterer Schäden.
- Weitere Massnahmen:
- schriftliche Ermahnungen oder Verwarnungen;
 - gezielte Sensibilisierungs- und Schulungsmassnahmen zur sicheren und verantwortungsvollen Nutzung der Informatikmittel;
 - Einschränkung der Nutzungsmöglichkeiten einzelner Dienste oder Systeme.
- Bei schwerwiegenden oder wiederholten Verstössen können – abhängig von der betroffenen Personengruppe und der geltenden Rechtsgrundlage – weitere Massnahmen ergriffen werden, wie
- schulische oder dienstrechtliche Disziplinarmassnahmen;
 - arbeitsrechtliche Massnahmen;
 - Ausschluss von der Nutzung bestimmter Informatikmittel;
 - Geltendmachung von Schadenersatzansprüchen;
 - Anzeige bei den zuständigen Strafverfolgungsbehörden
 - Eine namentliche Auswertung der vom Amt für Informatik gemäss dem IT-Anwender-Reglement geführten Protokolldaten ist nur ausnahmsweise zulässig. Sie bedarf der vorgängigen Zustimmung der Leitung des Schulamtes und der Leitung des Amtes für Informatik und darf nur erfolgen, wenn sie zur Abklärung eines konkreten Sachverhalts bzw. Verdachts zwingend erforderlich ist. Die Auswertung ist auf diejenigen Daten und denjenigen Zeitraum zu beschränken, die für den verfolgten Zweck unerlässlich sind.
- 16.3 Erforderlichenfalls wird auch die Datenschutzstelle und die / der schulische Datenschutzbeauftragte / Datenschutzkoordinator/in miteinbezogen.

- 16.4 Im Rahmen der pädagogischen Begleitung und Aufsicht im digitalen Raum kann eine Lehrperson aus wichtigen Gründen, insbesondere bei einem konkreten Verdacht auf einen Verstoss gegen Ziff. 4.4 dieser Richtlinie, die Einhaltung dieser Richtlinie kontrollieren. Dabei sind folgende Fälle zu unterscheiden:

a) Verdacht auf private Nutzung während der Unterrichtszeit

Besteht der konkrete Verdacht, dass das Gerät während der Unterrichtszeit entgegen den Vorgaben dieser Richtlinie privat genutzt wird (insbesondere für Teams-Chats, Internetnutzung oder Installation von Apps), kann eine Lehrperson im Beisein der betroffenen Schülerin oder des betroffenen Schülers sowie einer weiteren, möglichst unabhängigen Person des Schulpersonals (z. B. einer Lehrperson einer anderen Klasse, einer schulischen Heilpädagogin bzw. einem schulischen Heilpädagogen oder einer Schulasistenz) Einsicht in diejenigen auf dem Bildschirm sichtbaren Informationen nehmen, die zur Feststellung eines Verstosses erforderlich sind. Dazu gehören insbesondere die Metadaten von Kommunikationsverläufen (z. B. beteiligte Personen sowie Zeitpunkt von Nachrichten), die aktuell geöffnete Chatansicht, soweit deren Einsicht zur Überprüfung der Nutzung unvermeidbar ist, der Browserverlauf sowie die sichtbaren Hinweise auf installierte Anwendungen (z.B. App-Symbole oder App-Listen). Die Kontrolle beschränkt sich auf die Feststellung, ob eine unzulässige private Nutzung vorliegt. Eine darüberhinausgehende inhaltliche Auswertung privater Kommunikation oder sonstiger persönlicher Daten ist unzulässig.

b) Verdacht auf eine Nutzung mit möglicher Schädigung Dritter oder auf rechtlich relevante Verstösse

Besteht ein konkreter Verdacht, dass das Gerät während der Unterrichtszeit für Handlungen genutzt wird, durch die Dritte beeinträchtigt oder geschädigt werden könnten (insbesondere Cybermobbing, Belästigungen, Drohungen oder andere Persönlichkeitsrechtsverletzungen), oder liegen Anhaltspunkte für einen rechtlich relevanten Verstoss vor, kann die Lehrperson im Beisein der betroffenen Schülerin oder des betroffenen Schülers sowie eines Mitglieds der Schulleitung und gegebenenfalls eines Erziehungsberechtigten Einsicht in die zur Abklärung des Sachverhalts erforderlichen Inhalte auf dem Bildschirm nehmen. Soweit zur Klärung des konkreten Verdachts unbedingt erforderlich, kann hierbei ausnahmsweise auch eine inhaltliche Einsichtnahme in die betroffene Kommunikation erfolgen. Die Einsichtnahme ist zwingend auf diejenigen Inhalte zu beschränken, die mit dem konkreten Verdacht in Zusammenhang stehen.

Vorgehen in beiden Fällen:

- Sofern dies zur Aufrechterhaltung eines ungestörten Unterrichts angezeigt ist, kann die Kontrolle zeitlich auf einen späteren Zeitpunkt verschoben werden. Zu diesem Zweck kann das Gerät vorübergehend sichergestellt werden.
- Jede Kontrollmassnahme hat dem Grundsatz der Verhältnismässigkeit zu entsprechen. Insbesondere sind Art, Umfang und Dauer der Kontrolle auf das zur Erreichung des Kontrollzwecks erforderliche Mass zu beschränken. Stehen gleich geeignete, aber weniger eingriffsintensive Massnahmen zur Verfügung, sind diese vorzuziehen.

- Zur Durchführung der genannten Massnahmen kann die Schule unter Beachtung des Grundsatzes der Verhältnismässigkeit geeignete technische und organisatorische Massnahmen einsetzen, insbesondere Bildschirmfreigaben, Zugriffsbeschränkungen, Protokollierungen oder vergleichbare Kontrollinstrumente.
Die betroffenen Schülerinnen und Schüler sowie deren Erziehungsberechtigte werden über solche Massnahmen und deren Zweck in geeigneter Weise informiert, soweit dadurch der Kontrollzweck nicht vereitelt wird.
 - Der Zugriff auf im Rahmen von Kontrollen erhobene Informationen ist auf die mit der Abklärung betrauten Personen beschränkt. Anlass, Umfang, Durchführung und Ergebnis der Kontrolle sind angemessen zu dokumentieren.
- 16.5 Protokollierungen dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle der Nutzerinnen und Nutzer ausgewertet werden.

17. Massnahmen bei sicherheitsrelevanten Vorfällen

Sicherheitsrelevante Vorfälle, wie etwa der versehentliche Fehlversand von E-Mails und die Verletzung des Schutzes personenbezogener Daten, aber auch die Bekanntgabe von Passwörtern etc. über Phishing und andere illegale Fremdzugriffe sind unverzüglich dem Amt für Informatik sowie der zuständigen Schulaufsicht und der oder dem schulischen Datenschutzbeauftragten / Datenschutzkoordinator/in zu melden, welche/r die Meldung des Vorfalles, wenn Art. 33 DSGVO dies erfordert, an die Datenschutzstelle und, falls erforderlich, gemäss Art. 34 DSGVO an die betroffene Person veranlasst.

18. Schutzmassnahmen

- 18.1 Im Sinne des Kinder- und Jugendschutzes haben Eltern von Primarschülerinnen und Primarschülern die Möglichkeit, JAMF Parent zu verwenden und mit dem iPad ihres Kindes zu koppeln. Damit können sie die Gerätenutzung ausserhalb der vom Schulamt festgelegten Zeitfenster klar regulieren.
- 18.2 Das Lehrpersonal befähigt die Schülerinnen und Schüler im Rahmen des Lehrauftrags zu einem verantwortungsbewussten datenschutzkonformen Umgang mit den digitalen Medien, insbesondere in der Nutzung der Schulinformatiksysteme.
- 18.3 Lehrpersonen sind verpflichtet, die Schülerinnen und Schüler während des Unterrichts bei der Nutzung von Schulinformatikmitteln angemessen zu beaufsichtigen, um sie vor jugendgefährdenden und/oder rechtswidrigen Inhalten zu schützen.

19. Sanktionen

Ein Verstoß gegen eine oder mehrere Bestimmungen dieser Richtlinie kann, unbeschadet anderer rechtlicher Bestimmungen, je nach Schwere und Art zu dienst- oder disziplinarrechtlichen sowie schulrechtlichen Konsequenzen führen.

20. Urheber- und Lizenzrechte

Falls für bestimmte Software und Dokumente Urheber-, Lizenz- oder andere Rechte bestehen, so unterliegen deren Verwendung, Kopie und Weitergabe den entsprechenden rechtlichen Bestimmungen und Vereinbarungen.

21. Schlussbestimmungen

- 21.1 Diese Richtlinie ersetzt die bisherige Richtlinie vom August 2024.
- 21.2 Diese Richtlinie tritt am 01.08.2026 in Kraft und gilt bis auf Widerruf.

SCHULAMT DES FÜRSTENTUMS LIECHTENSTEIN

Eva Meirer
Amtsleiterin ad interim