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 SA/Datenschutz-
beauftragter der öffentlichen Schulen FL
Giessenstrasse 3
Postfach 684
9490 Vaduz
T +423 799 63 98
datenschutz@schulen.li

Version 3.0
Stand, August 2024

Präambel

Ziel dieser Richtlinie ist es, den Nutzerinnen und Nutzern 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 abrufbar.

Für Fragen zu dieser Richtlinie stehen der Technische IT-Koordinator (SIK) und der Pädagogische Medienmentor (PMM) beim Zentrum für Schulmedien sowie der/die 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.

Vaduz, August 2024

Inhalt

Rechtsgrundlage

Gestützt auf Art. 10[1] (i.V.m Art. 24a ff. SchulOV[2]) und Art. 106 Bst. a UBst. ee[3] 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 sowie des Schulamts zu verstehen.

1.2. Die Richtlinie regelt den Gebrauch von Schulinformatikmitteln. Darunter fallen insbesondere Geräte wie Desktop-Computer, Notebooks, Tablets oder Convertibles. Als Schulinformatikmittel gelten sowohl die an den Schulen eingesetzten physischen Endgeräte, die eingesetzten digitalen Lehrmittel (Software, Lernplattformen, webbasierte Dienste, sowie Cloud-Dienste) und 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. Die Informatikmittel dürfen nicht an Dritte weitergegeben werden, weder kurzfristig noch für einen längeren Zeitraum.

1.4. Spezifische Richtlinien und Handreichungen des Schulamtes und des Amts 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 (beide abrufbar über das Intranet der LLV).

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, den Schutz der Datenbestände und den

---

[1] Art. 10 SchulG, LGBl. 1972.007 idF LGBl. 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, LGBl. 2004.154 idF LGBl. 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, LGBl. 1972.007 idF LGBl. 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;

sicheren und wirtschaftlichen Einsatz der Informatikmittel durch das Schul- und Lehrpersonal sowie die Schülerinnen und Schüler.

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 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 BYOD-Geräte ausserhalb der Schule. Jede ausserschulische kommerzielle Verwendung ist ausdrücklich verboten. Private Nutzung ist nur innerhalb eines vertretbaren Rahmens zulässig. Ein vertretbarer Rahmen ist beispielsweise dann gegeben, wenn Musik zum Lernen abgespielt wird oder die Schulinformatikmittel für eine private Recherchen genutzt werden.

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 notfalls zu versperren.

4.6. 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.

4.7. 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.

4.8. Die Geräte sind aufgeladen und betriebsbereit zur Schule zu bringen.

4.9. Schuleigene Geräte und Materialen sowie die im Pflichtschulbereich ausgegebene Endgeräte der Liechtensteinischen Landesverwaltung dürfen nicht beklebt oder anderweitig verändert werden.

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 (Schulleitung), Stellvertretung, anderen Mitarbeitenden, Lehr- und Schulpersonal usw. Dies 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 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 vorgegeben Zyklen erneuert werden. Es muss aus mindestens zehn Zeichen bestehen, wobei das Passwort Zeichen aus mindestens drei der folgenden vier Kategorien enthalten muss:

- Grossbuchstaben (A-Z)
- Kleinbuchstaben (a-z)
- Ziffern (0-9)
- Sonderzeichen (bpsw. !, %, $ oder #)

Für die Festlegung eines sicheren Passworts wird ein sogenannter Merksatz (Passphrase) empfohlen. Beispielsweise:
«***M**ir **w**ird **a**m **1.5. e**in Stern (*) **a**m **H**ollywood **B**oulevard **v**erliehen**!***» ergibt das sichere Passwort: **Mwa1.5.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 periodisch 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.

5.4. 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 je nach Schulstufe, 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. Eine private Nutzung ist ausnahmsweise erlaubt, insoweit sie nicht übermässig ist und den Betrieb nicht stört (siehe Ziff. 4.4.).

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 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 wird 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 Der E-Mail-Service darf für private Zwecke verwendet werden, insofern die Nutzung nicht übermässig ist und den Betrieb nicht stört oder schadet (vgl. Ziff. 4.4).

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 bzw. 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://webmail.schulen.llv.li) 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 gelöscht.

8. Nutzung von Social Media

8.1 Social Media dürfen nur im Rahmen des Lernplans und unter Beachtung der datenschutzrechtlichen 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 beim Zentrum für Schulmedien einen Antrag einzubringen. Das Schulamt erlässt 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 die Option «privat» jeweils gesetzt werden.

10.3 Bei Abwesenheiten ist der Abwesenheitsassistenz 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 und datenschutzrechtskonforme Dokumente zur Verfügung. Private Daten dürfen darauf nicht gespeichert werden. Es ist auf eine massvolle Nutzung zu achten.

11.2 Persönliche Daten sollen im Dateinamen oder in einem Dateiordner mit «persönlich» gekennzeichnet werden und sind ausschliesslich im P-Laufwerk abzuspeichern. Die LLV haftet weder für den Verlust noch für die Beschädigung von persönlichen Daten, welche auf Informatikmitteln der LLV verarbeitet werden.

11.3 Für die Netzlaufwerke bestehen spezifische Zugriffsberechtigungen. Auf Antrag und in Rücksprache mit der festgelegten vorgesetzten Stelle kann das Amt für Informatik organisationsübergreifende Zugriffsberechtigungen einrichten.

11.4 Soweit für die digitale Aktenablage und -verwaltung eine eigenständige Software bzw. Fachapplikationen zur Verfügung gestellt wurde (z.B. LiSA oder für Schulamtsmitarbeitende LiVE) ist diese zu verwenden. Aktendoppel und -kopien sind zur Wahrung des Grundsatzes der Datenminimierung und -sparsamkeit zu vermeiden bzw. zu löschen, wenn das erstellte Doppel nicht länger benötigt wird.

11.5 Die 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.

11.6 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 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 keine Endgeräte unentgeltlich zur Verfügung gestellt werden und vom Amt für Informatik zentral verwaltet werden.

12.2 Die Nutzung der Schulinformatik durch private Geräte ist unter Vorbehalt von Ziff. 12.3.ff erlaubt.

12.3 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.
Eine darüber hinausgehende 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).

12.4 Informationen und Datensätze, welche dem Dienstgeheimnis des Lehr- und Schulpersonals unterliegen und/oder personenbezogene Daten 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.

12.5 Die Nutzerinnen und Nutzer sind verpflichtet, die Software ihres privaten Gerätes auf dem neuesten Stand zu halten (z.B. Windows, iOS, MacOS, Android etc.) und Updates regelmässig zu installieren. Die Verantwortung für eine datenschutzkonforme Verwaltung und Konfiguration von BYOD-Geräten liegt bei den Erziehungsberechtigten bzw. den volljährigen Schülerinnen und Schülern.

12.6 Um einen störungsfreien Einsatz der Geräte zu Schulunterrichtszwecken zu gewährleisten sind die Geräte aufgeladen und betriebsbereit zur Schule zu bringen (siehe Ziff. 4.8.).

12.7 Bei der Verwendung privater Datenträger und Peripheriegeräte, wie USB-Sticks, Kameras, Plug- and Play Druckern, Ladegeräten ist auch auf BYOD-Geräten Vorsicht geboten. Auf die Nutzung von Werbegeschenken (z.B. USB-Sticks oder ähnliche Artikel mit USB-Stecker) sollte verzichtet werden, um ein unbeabsichtigtes Hochladen von Malware und Spyware zu verhindern.

13. Herausgabe von Daten an externe Partner (z.B. Dienstleister, IT-Berater, usw.)

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) zu unterzeichnen. Hierfür sollte das Template des Amts für Informatik verwendet werden**.**

14. Clean Screen Policy («sauberer Bildschirm»)

14.1 Bei einem bloss vorübergehenden Verlassen des Arbeitsplatzes bzw. des Endgeräts ist die Bildschirmsperre zu aktivieren.

14.2 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

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 strafrechtsrelevanten Handlungen ist umgehend der Schulleitung, respektive dem Schulamt zu melden, das die weiteren Abklärungen entsprechend Ziff. 15.4 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 Als richtlinienwidrig gilt insbesondere:

- jeglicher Einsatz der Schulinformatikmittel bzw. von Informatikmitteln allgemein, der die Privatsphäre oder die Persönlichkeit von Personen verletzen könnte; eine Verletzung der Privatsphäre oder der Persönlichkeit von Personen ist zu verhindern (z.B. durch Recherchen in Fachinformationssystemen ohne entsprechenden Geschäftsfall oder -vorgang); Verstösse gegen den Datenschutz sind dem Datenschutzkoordinator bzw. der Datenschutzkoordinatorin respektive dem oder der schulischen Datenschutzbeauftragten zu melden.
- das Herunterladen, das Speichern und/oder Verbreiten, die Installation, die Ausführung oder die Verwertung als auch jegliche andere Verarbeitung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder anderen Informationen.
- Des Weiteren dürfen die Schulinformatikmittel nicht verwendet werden 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.
- Weitere Beispiele richtlinienwidriger missbräuchlicher Nutzung der Schulinformatikmittel bestehen insbesondere in den folgenden Fällen:
  - Ausspionieren fremder Passwörter und Daten;
  - Widerrechtliches Kopieren, Verändern, Löschen oder unbrauchbar machen von Daten;
  - Bereitstellen von Netzwerk- und Applikationszugängen und/oder Weitergabe von Daten für Dritte;
  - Verbindung privater Hardware mit der Informatikinfrastruktur der LLV oder Installation und Verwendung privater Software auf derselben (ausgenommen BYOD auf der Sekundarstufe II);
  - Unbefugtes Verändern von der Konfiguration von Hard- und Software der Informatikmittel;
  - Herunterladen, speichern, verbreiten, verwerten und jede andere Verarbeitung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder sonstigen Informationen;
  - Beanspruchung von Ressourcen (insbesondere Arbeitszeit, Bandbreite, Datenmenge, Speicherplatz etc.) für private Zwecke, die einen Umfang einnimmt, der in einem Missverhältnis zur dienstlichen oder schulischen Verwendung der Informatikmittel steht;
  - Geschäftliche Nutzung der Schulinformatikmittel (z.B. im Rahmen eines Nebenerwerbs);
  - Benutzen der Infrastruktur für Hacking oder Cracking anderer oder eigener Systeme, insbesondere das Kopieren oder Einsetzen von entsprechender Software;

- 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;
- Synchronisation dienstlicher Daten auf private Informatikmittel und Verteilen von unerwünschten Massen-E-Mails (Spam).

15.4 Ein Missbrauch der Schulinformatikmittel kann beispielsweise durch folgende Mittel festgestellt werden:

- Anonyme oder pseudonyme Überwachung der Protokolle (siehe Ziff. 16), z.B. bei der Suche nach einer Virusquelle oder bei der Verifizierung eines Hacking-Versuches.
- Eine namentliche Auswertung der Protokolle geschieht im Verdachtsfall auf Anweisung der Staatsanwaltschaft oder auf übereistimmende Anweisung der Leitungen des Schulamtes und des Amts für Informatik.
- Erforderlichenfalls wird auch die Datenschutzstelle miteinbezogen.

15.5 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 zu melden.

15.6 Falls Nutzerinnen und Nutzer beim Einsatz von Informatikmitteln oder Dokumenten Unregelmässigkeiten (wie Defekte, Virenbefall oder Missbräuche) feststellen, so sind sie verpflichtet, diese dem technischen Medienkoordinator oder dem Amt für Informatik zu melden.

16. Schutzmassnahmen

16.1 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.

16.2 Jeglicher Internet- und E-Mail-Verkehr wird protokolliert, ebenso Nutzeraktivitäten mittels Log-Dateien von Windows- und Fachinformationssystemen. Die Protokolle werden in anonymisierter oder pseudonymer Form ausgewertet. Pseudonyme Auswertungen erfolgen stichprobenartig.

16.3 Protokollierungen nach Ziff. 16.2 dürfen vorbehaltlich Ziff. 16.4 und Ziff. 16.5 grundsätzlich nicht zu Zwecken der Verhaltens- oder Leistungskontrolle der Nutzerinnen und Nutzer ausgewertet werden.

16.4 Weitere Auswertungen sind nur dann zulässig, wenn sonst ein Missbrauch und/oder ein Schaden nicht abgewendet werden kann.

16.5 Personenbezogene Auswertungen ohne konkreten Missbrauchsverdacht sind verboten.

17. 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.

18. Schlussbestimmungen

18.1 Diese Richtlinie ersetzt die bisherige Richtlinie vom 1. Dezember 2020.
18.2 Diese Richtlinie tritt am 19. August 2024 in Kraft und gilt bis auf Widerruf.

SCHULAMT DES

FÜRSTENTUMS LIECHTENSTEIN

Rachel Guerra, Amtsleiterin