SCHULAMT
FÜRSTENTUM LIECHTENSTEIN

Vaduz, 1. Dezember 2020 AK/Di/ij-4043/1-9/Version 2.0

Richtlinie über die Nutzung der Schulinformatik

Gestützt auf Art. 10[1] (in Verbindung mit Art. 24a ff. SchulOV) und Art. 106 Bst. a) ee)[2] des Schulgesetzes bestimmt das Schulamt, was folgt:

1. Geltungsbereich

1.1 Die Richtlinie gilt für alle Nutzerinnen und Nutzer der Schulinformatik

1.2 Die Richtlinie regelt den Gebrauch von Schulinformatikmitteln. Darunter fallen insbesondere Geräte wie Desktops, Notebooks, Tablets oder Convertibles.

1.3 Spezifische Richtlinien des Schulamtes für besondere Informatikmittel und deren Nutzungen bleiben vorbehalten.

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

2. Zweck

2.1 Die Richtlinie bezweckt die Sicherstellung einer rechtmässigen Nutzung und eines störungsfreien Betriebs der Schulinformatik, den Schutz der Datenbestände und den sicheren und wirtschaftlichen Einsatz der Informatikmittel.

3. Datenschutz

3.1 Hinweise zum Datenschutz enthält das Merkblatt über den Datenschutz an öffentlichen Schulen.

4. Allgemeine Grundsätze

4.1 Nutzerinnen und Nutzer tragen die Verantwortung für eine richtlinienkonforme Nutzung der Schulinformatikmittel.

4.2 Lehrpersonen setzen ihre Schülerinnen und Schüler in die Lage, die Schulinformatikmittel richtlinienkonform zu nutzen.

4.3 Erforderlichenfalls gibt die Schule den Eltern und den Schülerinnen und Schüler gestützt auf diese Richtlinie Merkblätter zur Nutzung der Schulinformatik ab.

---

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

[2] Zuständigkeit des Schulamtes für die Schulinformatik.

4.4 Die Informatikmittel stehen grundsätzlich nur für schulische Zwecke zur Verfügung. Jede ausserschulische kommerzielle Verwendung ist ausdrücklich verboten. Private Nutzung ist nur erlaubt, wenn ein noch vertretbarer Rahmen nicht überschritten wird.

4.5 Es ist verboten, die zur Verfügung gestellten Informatikmittel Dritten weiter zu geben.

4.6 Die Informatikmittel sind sorgfältig zu nutzen. Es ist grundsätzlich alles zu vermeiden, was den Betrieb der Schulinformatik beeinträchtigt sowie Schäden am System oder bei anderen Nutzerinnen und Nutzer verursacht.

4.7 Geräte (einschliesslich Peripheriegeräte wie Stifte, Kabel etc.) sind jederzeit sorgfältig aufzubewahren und zu behandeln, auch zu Hause, auf dem Weg zur Schule, auf dem Arbeitsweg oder auf ausserordentlichen Schulveranstaltungen (z.B. Exkursionen).

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

5. Zugang zur Nutzung (Authentifizierung)

5.1 Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Sie dürfen niemand ausgehändigt oder bekannt gemacht werden.

5.2 Der Benutzernamen wird von der zuständigen Stelle vorgegeben, das Passwort muss vom Nutzer und von der Nutzerin gemäss Ziff. 5.3 festgelegt werden.

5.3 Ein Passwort muss aus mindestens acht 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 (Beispiele: !, $, # oder %)

Die Zeichenfolge des Benutzernamens (User-ID) darf im Passwort nicht vorkommen.

5.4 Ein neues Passwort ist maximal 180 Tage gültig und kann frühestens nach einem Tag erneut geändert werden. Die letzten zehn Passwörter können nicht erneut verwendet werden.

5.5 Das Passwort muss umgehend geändert werden, wenn es Dritten bekannt geworden ist oder wenn ein entsprechender Verdacht besteht. Dies gilt auch für Passwörter von Fachapplikationen.

5.6 Nach wiederholter Falscheingabe des Passwortes wird der Computerzugriff gesperrt und muss vom Amt für Informatik freigeschaltet werden.

5.7 Die Nutzerinnen und Nutzer haben die Möglichkeit, sich über biometrische Daten (Fingerabdruck, Gesichtserkennung) zu authentifizieren. Sie müssen diese Art der Authentifizierung gemäss Anleitung selbständig einrichten. Diese Möglichkeit entbindet nicht von der Notwendigkeit und von der Verpflichtung, ein Passwort zu führen

5.8 Benutzernamen, Passwörter und weitere Account-Informationen dürfen nur für schulische und nicht auch für private Zwecke (private Accounts) weiterverwendet werden, z.B. für den Zugang zu digitalen Lehrmitteln oder Lernplattformen. Vorab ist zu klären, ob die betreffende Applikation datenschutzrechtskonform und ihr Anbieter vertrauenswürdig ist.

6. Nutzung des Internet

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. 4.3).

6.2 Verboten ist der Besuch von Internet-Seiten mit pornographischen oder sexistischen Darstellungen oder mit extremistischen, Gewalt verherrlichenden, rassistischen oder sonst strafrechtlich relevanten Inhalten. Ebenso ist der Besuch einschlägiger Spiele-Seiten verboten.

6.3 Nach Möglichkeit werden verbotene Seiten (Ziff. 6.2) und Seiten mit offensichtlich schulfremden Inhalten protokolliert und aufbewahrt..

7. Nutzung des E-Mail-Service

7.1 Es ist die persönliche E-Mail-Adresse (Name.Vorname@schulen.li) zu verwenden.

7.2 Der E-Mail-Service darf für private Zwecke verwendet werden, insofern die Nutzung nicht übermässig ist und den Betrieb nicht stört oder schadet (siehe Ziff. 4.3).

7.3 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, meldet dies der Schulleitung oder dem Schulamt.

7.4 Die Einrichtung einer fixen Weiterleitung von E-Mails an private Mail-Konten ist untersagt. Bei nicht fixen Weiterleitungen sind die Regeln des Datenschutzrechtes einzuhalten (siehe Merkblatt über den Datenschutz an öffentlichen Schulen).

7.5 Authentifizierte Nutzerinnen und Nutzer haben über das Webportal (https://webmail.schulen.llv.li) Zugang zu ihren E-Mails.

7.6 Auf Phising-Mails darf nicht geantwortet werden. Wird Phishing erkannt, ist dies dem Amt für Informatik zu melden. Danach sind die Mails zu löschen.

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 im Rahmen des Lehrplans und unter Beachtung der datenschutzrechtlichen Bestimmungen für schulische Zwecke genutzt werden.

8.2 Technische und organisatorische Sicherheitsmassnahmen bleiben vorbehalten, insbesondere zur Bekämpfung von Cyber Mobbing.

9. Einsatz von Lernapplikationen

9.1 Hinsichtlich der Freigabe digitaler Lehrmittel (inkl. Cloud-Lösungen) gelten die gesetzlichen Zuständigkeiten (Art. 10 Schulgesetz[3]).

9.2 Vor der Freigabe klären die nach Art. 10 Schulgesetz zuständigen Stellen ab, ob die technischen und datenschutzrechtlichen Voraussetzungen dafür erfüllt sind.

---

[3] Art. 10 SchulG lautet: 1) Das Schulamt bestimmt auf der Grundlage des Lehrplanes, welche Lehrmittel in den öffentlichen Schulen vorgeschrieben sind, und beschafft diese Lehrmittel für die einzelnen öffentlichen Schulen. 2) Auf der Grundlage des Lehrplanes können die öffentlichen Schulen im Rahmen ihres Budgets weitere Lehrmittel beschaffen und einsetzen.

10. Nutzung des Outlook-Kalenders

10.1 Es wird empfohlen, die Option „gebucht/frei" gegenüber Nutzerinnen und Nutzern derselben Organisation standardmässig freizugeben.

10.2 Für Termine, welche nicht für die Allgemeinheit bestimmt sind, soll die Option „privat" gewählt werden.

10.3 Bei Abwesenheiten ist der Abwesenheitsassistent zu aktivieren und anzugeben, wer die Stellvertretung übernimmt.

11. Nutzung der Netzlaufwerke und des lokalen Laufwerks

11.1 Die verschiedenen Netzlaufwerke (z.B. G-, S- & P-Laufwerk) sowie das lokale Laufwerk C 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 Für die Netzlaufwerke bestehen spezifische Zugriffsberechtigungen. Auf Antrag kann das Amt für Informatik organisationsübergreifende Zugriffsberechtigungen einrichten.

11.3 Die Daten auf den Netzlaufwerken werden mehrmals täglich gegen Datenverlust gesichert (Backup), und es werden Vorgängerversionen gespeichert. Wiederherstellungen von Vorversionen oder Datensicherungen müssen beim Amt für Informatik in Auftrag gegeben werden.

11.4 Nach dem Austritt werden die Daten auf sämtlichen Laufwerken gelöscht. Nutzerinnen und Nutzern wird empfohlen, diese Laufwerke vor dem Austritt zu bereinigen.

12. Nutzung mittels privater Geräte (BYOD = bring your own device)

12.1 Die Nutzung der Schulinformatik durch private Geräten ist unter Vorbehalt von Ziff. 12.2 ff. erlaubt.

12.2 Die Nutzung durch private Geräte ist beschränkt auf lizenzierte Applikationen.

Derzeit sind dies: Office 365, Outlook Online (Mail, Kalender und Kontakte), Teams, SharePoint online, Adobe Creative Cloud.

12.3 Die Nutzerinnen und Nutzer sind verpflichtet, die Software ihres privaten Gerätes auf dem neusten Stand zu halten (z.B. Windows, iOS, MacOS, Android, etc.) und Updates regelmässig zu installieren.

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

13.1 Werden Daten an externe Partner herausgegeben, so haben diese zwingend ein Non Disclosure Agreement (= Geheimhaltungsvereinbarung) zu unterzeichnen.

14. Clean Desk Policy („sauberer Bildschirm")

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

14.2 Bei längerem Nichtgebrauch sind Endgeräte auszuschalten.

15. Missbräuchliche Nutzung

15.1 Ein Missbrauch liegt vor, wenn einschlägige gesetzliche Bestimmungen und Vorgaben dieser Richtlinie verletzt werden.

15.2 Richtlinienwidrige missbräuchliche Nutzung liegt insbesondere in den folgenden Fällen vor:

- Herunterladen, Speicherung, Verbreitung, Verwertung und jede andere Bearbeitung von rechtswidrigen oder rechtswidrig erlangten Daten, Programmen oder sonstigen Informationen;
- Verteilung von unerwünschten Massenmails (Spam);
- übermässige Privatnutzung des Internets;
- Ausspionieren fremder Passwörter und Daten;
- unbefugtes Verändern, Löschen, Unbrauchbarmachen oder Unterdrücken von Daten;
- unbefugtes Verändern von System- und Netzwerkkonfiguration;
- Bereitstellen von Netzwerkzugängen und/oder Weitergabe von Daten an Dritte;
- unbefugtes Bearbeiten (z.B. Erfassen, Abfragen oder Weitergeben von LLVSA-Daten);
- Veränderung der Konfiguration sowie Installation von nicht freigegebener Zusatz-Software;
- Verletzung der Privatsphäre oder der Persönlichkeit von Personen (z.B. durch Recherchen in Fachinformationssystemen ohne entsprechenden Geschäftsfall oder -vorgang);
- Zugriffe auf privates und/oder urheberrechtlich geschütztes Material;
- Manipulationen an den Endgeräten.

15.3 Ein Missbrauch 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 übereinstimmende Anweisung der Leitungen des Schulamtes und des Amtes für Informatik. Erforderlichenfalls wird auch die Datenschutzstelle miteinbezogen.
- Hinweise (z.B. versehentlicher Falschversand von privaten E-Mails) und Meldungen (Ziff. 15.4).

15.4 Falls Nutzerinnen und Nutzer beim Einsatz von Informatikmitteln oder Dokumenten Unregelmässigkeiten (wie Defekte, Virenbefall oder Missbräuche) feststellen, so sind sie verpflichtet, diese unverzüglich dem technischen Medienkoordinator oder der Schulleitung zu melden.

15.5 Die richtlinienwidrige missbräuchliche Nutzung kann nachstehende Konsequenzen und Sanktionen nach sich ziehen:

- Sperrung des Internet- oder Netzwerkzugangs im Einvernehmen mit dem Schulamt durch das Amt für Informatik; Information der zuständigen Schulleitung;
- Überwachung der Accounts bzw. des E-Mail-Postfachs, einvernehmlich durch das Amt für Informatik und das Schulamt;
- Überwachung der beanspruchten Schulnetzressourcen (speziell Internetauslastung) durch die Benutzer, einvernehmlich durch das Amt für Informatik und das Schulamt;
- weitere disziplinarische oder personalrechtliche Massnahmen nach den einschlägigen gesetzlichen Bestimmungen;
- Strafanzeige durch die Leitung des Schulamtes oder des Amtes für Informatik;
- Schadenersatz gemäss den gesetzlichen Bestimmungen (bei durch Schülerinnen und Schüler verursachten siehe Art. 34 Abs. 4 SchulOV).

15.6 Bei der Beurteilung eines Missbrauchs kommt der Verhältnismässigkeitsgrundsatz zur Anwendung (Beispiel: Ein einzelner misslungener Versuch auf eine durch technische Schutzmassnahmen gesperrte Internetseite zuzugreifen, muss noch keinen Missbrauch darstellen).

16. Schutzmassnahmen

16.1 Es werden organisatorische und technische Schutzmassnahmen gegen Missbrauch und technischen Schaden eingesetzt. Diese Massnahmen werden regelmässig auf den neusten Stand der Technik gebracht.

16.2 Jeglicher Internet- und E-Mail-Verkehr wird protokolliert, ebenso Nutzeraktivitäten mittels Log-Dateien von Windows- und Fachinformationssystemen. Die Protokolle werden in anonymer 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 Auswertungen von Aktivitäten der Schülerinnen und Schüler dürfen nur im Rahmen des Lehrplanes erfolgen (z.B. Lernkontrollen durch elektronische Lernplattformen und Lehrmittel).

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

16.6 Proaktive namentliche Auswertungen ohne konkreten Missbrauchsverdacht sind verboten.

17. Urheber- und Lizenzrechte

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

18. Schlussbestimmungen

18.1 Diese Richtlinie ersetzt die bisherigen Richtlinien und Reglemente.

18.2 Sie tritt am 1. Dezember 2020 in Kraft.

SCHULAMT DES
FÜRSTENTUMS LIECHTENSTEIN

Arnold Kind, Amtsleiter