

Informatikcharta

REGLEMENT vom 25. Oktober 2021 über die ICT-Nutzung an der Orientierungsschule von Siders

Alle Personen-, Status- oder Funktionsbezeichnungen in diesem Dokument gelten für die weibliche und die männliche Form.

1. Gesetzliche Grundlagen und Referenzdokumente

Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA) vom 9. Oktober 2008 (SGS/VS 170.2);

Gesetz über das Personal der obligatorischen Schulzeit und der allgemeinen Mittelschule und Berufsfachschule vom 14. September 2011 (GPOS, SGS/VS 400.2);

Gesetz über das Personal des Staates Wallis (kGPers) vom 19. November 2010 (SGS/VS 172.2);

Artikel 29 der Verordnung betreffend das Gesetz über die Primarschule vom 11. Februar 2015 (SGS/VS 411.001);

Art. 29 *Schutz der Persönlichkeit und Datenschutz*

¹ *Im Rahmen der Schule ist der Schüler in seiner Privatsphäre geschützt.*

² *Jede Aufnahme von mündlichen, schriftlichen oder gefilmten Daten durch Dritte, welche nicht Teil der Schule sind, müssen durch die Schuldirektion und die gesetzliche Vertretung bewilligt werden.*

³ *Ohne Zustimmung der Schuldirektion und der Dienststelle für Unterrichtswesen dürfen Lehrpersonen keine Schülerdaten herausgeben.*

⁴ *Die Schule hält sich in allen Fällen an die gesetzlichen Bestimmungen betreffend Datenschutz.*

Weisungen des Departements für Volkswirtschaft und Bildung betreffend ICT für die obligatorische Schule vom 6. Juli 2021;

Muster-Informatikleitbilder vom Juni 2021, die der Kanton Wallis vorgeschlagen hat und die auf der Website des Kompetenzzentrums ICT-VS verfügbar sind (www.ictvs.ch);

Standesregeln der Lehrpersonen des Syndicat des enseignants romands (SER) und des Dachverbands Lehrerinnen und Lehrer Schweiz (LCH);

Filterpolitik des Departements für Volkswirtschaft und Bildung über die Internetnutzung an den Schulen der obligatorischen Schule und der Sekundarstufe II vom 6. Juli 2021;

Pflichtenheft der Lehrperson.

2. Zweck

Dieses Reglement soll die Regeln für die Nutzung der ICT-Tools, den Zugang zu digitalen Ressourcen sowie die Sicherheitsnormen festlegen.

3. Geltungsbereich

¹Das vorliegende Reglement gilt für alle Lehrpersonen, Stellvertreter, administrativen Mitarbeiter und Praktikanten (nachstehend Benutzer), die zur Nutzung der Informatikausstattung, der Plattformen und/oder ICT-Ressourcen der Schule berechtigt sind. Das Reglement gilt ebenfalls für alle anderen Personen, die Zugang zu den Informatikressourcen der Schule haben.

²Jeder Benutzer verpflichtet sich durch seine Unterschrift zur Einhaltung der Bestimmungen des Reglements.

4. Pflichten der Schule

¹Die Schule verpflichtet sich im Rahmen der Massnahmen zur Wahrung ihrer Interessen und zum Schutz bestimmter Informatikausrüstungen, die Persönlichkeit des Benutzers zu achten und zu schützen. Die privaten Daten der Benutzer, sofern sie als solche erkennbar sind, werden weder eingesehen noch verbreitet oder veröffentlicht.

² Die Verantwortlichen für Administration oder Informatik gewähren allen Benutzern ab dem ersten Arbeitstag an der Schule Zugangsrechte.

5. Rechte und Pflichten der Benutzer

a) Sicherheitsregeln: Zugangsrecht

Das Zugriffsrecht auf die Informatiksysteme ist persönlich, nicht übertragbar und zeitlich begrenzt. Sie unterliegen den Bedingungen und Einschränkungen dieses Reglements. Sie sind durch ein persönliches, streng vertrauliches und ausreichend komplexes Passwort zu schützen.

²Die Weitergabe des Passworts ist in keiner Weise zulässig. Der Benutzer darf nur die ihm persönlich zugeteilten Konten benutzen. Er muss das von der Institution eingangs erhaltene Passwort mit der ersten Verbindung/Verwendung und anschliessend regelmässig ändern.

³Der Benutzer hat ausschliesslich mit seinem Benutzernamen und Passwort auf das Informatiksystem und die Informatikressourcen Zugriff.

⁴Der Benutzer darf seinen Benutzernamen und sein Passwort unter keinen Umständen an Dritte weitergeben.

⁵Der Benutzer ist für die Vertraulichkeit und die Aufbewahrung seines Benutzernamens und Passworts verantwortlich.

⁶Der Benutzer überprüft jedes Mal, wenn er einen Arbeitsplatz verlässt, und das auch bei kurzen Unterbrechungen, ob er sich richtig abgemeldet oder den Zugriff gesperrt hat.

⁷Der Benutzer haftet gegenüber dem Staat und/oder den Gemeinden für Schäden durch eine unerlaubte Nutzung seiner Konten. Bei vorsätzlichem Verschulden oder einer groben Fahrlässigkeit haftet er persönlich.

⁸Bei Verdacht auf Betrug oder Identitätsmissbrauch benachrichtigt der Benutzer unverzüglich den Administrator.

b) Vertraulichkeitsverpflichtung

¹Der Zugriff auf Daten, Informationen und Dokumente, die auf den Informatiksystemen und Server gespeichert sind, ist strikt auf die zugelassenen Benutzer beschränkt.

²Das Hinzufügen oder eine Änderung von Daten (Informationen oder Dokumente) auf den Systemen und Servern kann nur von einem Benutzer mit Zugriffsrecht durchgeführt werden.

c) Software: Installation und Kopie

¹Jede Änderung von Einstellungen oder die Installation von Software auf den Arbeitsplätzen kann nur nach vorheriger Genehmigung durch die Schuldirektion durchgeführt werden.

²Das Urheberrecht ist zu beachten. Es ist daher strengstens verboten, Software der Schule zu kopieren.

d) Arbeitsplatz und zugehörige Ausrüstung

¹Änderungen an Geräten, am Netz und an den Konfigurationen werden ausschliesslich von einer von der Schuldirektion beauftragten Person vorgenommen.

²Ein privates Gerät darf nur nach vorheriger schriftlicher Genehmigung durch die Schuldirektion mittels Kabel mit dem Computernetzwerk der Schule verbunden werden. Ein solches Gerät wird umgehend vom Netz getrennt, falls dies als erforderlich erachtet wird.

6. Internet

a) Allgemeine Grundsätze im Rahmen der dienstlichen Tätigkeit

¹Das Internet ist ausschliesslich für dienstliche Zwecke und für die zugewiesenen Aufgaben zu verwenden.

²Die private Internetnutzung wird toleriert, solange es zu keiner missbräuchlichen Nutzung kommt, nämlich insbesondere die IT-Infrastruktur nicht überlastet (Speicherplatz, Bandbreite) und die Sorgfalts- und Treuepflicht des Benutzers nicht verletzt wird.

³Die Verbreitung von persönlichen und politischen Informationen oder Werbeinformationen, die nicht mit der dienstlichen Tätigkeit in Zusammenhang stehen, ist strengstens untersagt.

⁴Die Nutzung von IT-Diensten in der Cloud zu pädagogischen Zwecken bedarf einer vorgängigen Bewilligung durch die Schuldirektion mit Ausnahme der offiziell bewilligten Dienste. Die Daten dürfen nur in der Schweiz gespeichert werden.

b) Missbräuchliche Nutzung

¹Alle Benutzer müssen dafür Sorge tragen, das Internet so zu nutzen, dass keine rechtlichen, technischen oder operativen Risiken für die Schule und die anvertrauten Schüler entstehen und ihr Ruf nicht gefährdet wird.

²Jegliche missbräuchliche oder rechtswidrige Nutzung ist strengstens untersagt. Der Zugriff, das Hochladen oder Herunterladen und die Übertragung von Daten, deren Inhalt gegen das Gesetz, die Ethik oder die Moral verstösst oder beleidigend, verletzend, demütigend oder verunglimpfend ist, ist ausdrücklich untersagt.

c) Elektronische Kommunikation über die dienstliche Adresse

¹Der Benutzer verwendet ausschliesslich seine dienstliche Adresse für Nachrichten in Zusammenhang mit seiner Tätigkeit. Er achtet darauf, fehlerfreie Nachrichten zu verfassen, da es sich um offizielle Mitteilungen handelt.

²Der Massenversand von nicht schulbezogenen Dokumenten oder das Weiterverbreiten von Adressbüchern ist strengstens untersagt. Der Benutzer verwendet die ihm zur Verfügung stehenden Daten nur im schulischen Kontext (untersagt sind namentlich: Werbung, Kettenmails, politische Kampagnen usw.).

³Während der Unterrichtswochen konsultieren die Lehrpersonen die vom Staat bereitgestellte Mailbox in der Regel täglich und bearbeiten die Nachrichten betreffend ihre berufliche Tätigkeit innerhalb einer der jeweiligen Dringlichkeit angemessenen Frist. Ausserhalb dieser Zeit muss der Benutzer seine berufliche Mailbox regelmässig konsultieren.

Jegliche Weiterleitung von beruflichen E-Mails an eine private Mailbox oder umgekehrt ist verboten. Die vom Staat eingerichtete Mailbox ist strikt der beruflichen Nutzung vorbehalten.

7. Technische Fähigkeiten

¹Der Benutzer muss die grundlegenden IT-Tools beherrschen oder sich gegebenenfalls fortbilden, um auf den erforderlichen Stand zu kommen. Es liegt in seiner Verantwortung, sich für die zu diesem Zweck angebotenen Schulungen anzumelden.

²Der Benutzer muss sich schnellstmöglich den Umgang mit der zur Verfügung gestellten IT-Infrastruktur aneignen.

8. Überwachungsmaßnahmen

¹Die Schuldirektion kann beantragen, dass die Nutzung der den Mitarbeitern zur Verfügung gestellten Informatikmittel (insbesondere E-Mail und Internet) anonymisierten statistischen Kontrollen unterzogen wird, um einerseits die Sicherheit und das technische Funktionieren besagter Mittel zu gewährleisten und andererseits die Befolgung der vorliegenden Weisungen durch die Benutzer allgemein zu überprüfen.

²Beeinträchtigt oder gefährdet eine technische Störung das Funktionieren der Informatikmittel, ist der Informatikverantwortliche berechtigt, alle erforderlichen Massnahmen zur Wiederherstellung der Normalsituation zu treffen, ausgenommen die Einsicht privater Daten.

³Die Schuldirektion kann bei Verdacht anonymisierte Kontrollen der Nutzung der Informatikmittel durch ihre Mitarbeiter beantragen. Die Dienstchefs haben dieselbe Befugnis für die ihrer Dienststelle angegliederten Einrichtungen. Die Aufbewahrungsdauer dieser Daten beträgt 10 Tage.

⁴Wird auf der Grundlage der vorerwähnten Kontrollen oder anderer objektiver Anhaltspunkte anhand von Indizien eine Missachtung des vorliegenden Reglements vermutet, kann die Schuldirektion personenbezogene Kontrollen bezüglich der Nutzung der Informatikmittel vornehmen lassen (Angabe der gespeicherten Datenkategorien, Aufbewahrungsdauer und Personen, die Zugang zu den Daten haben). In diesem Fall beträgt die Aufbewahrungsdauer dieser Daten 30 Tage.

⁵Vorbehaltlich des Verdachts auf einen Verstoß ist der Inhalt der Dateien und Nachrichten von diesen Kontrollen ausgeschlossen, da diese rein privater Natur sind.

⁶Beinhaltet das Reglement den Grundsatz und die Einzelheiten für eine personenbezogene Kontrolle und wird die personenbezogene Kontrolle in einem Entscheid des Vorgesetzten festgelegt, beginnt die Durchführung der Kontrolle ohne vorgängige Ankündigung an den vom Entscheid betroffenen Benutzer.

⁷Erweist sich der Verdacht auf Nichtbefolgung der vorliegenden Weisungen als begründet, kann die Kontrolle auf die Zeit vor der Information ausgeweitet werden.

⁸Bei bestätigtem Verdacht auf Nichtbefolgung der vorliegenden Weisungen gelten, unter Vorbehalt von Bagatelldfällen (die vom Arbeitgeber als geringfügige Verstöße angesehen werden), die Bestimmungen von Artikel 29 ff. des Gesetzes über das Personal des Staates Wallis vom 19. November 2010, beziehungsweise für die Lehrpersonen die Artikel 45a ff des Gesetz über das Personal der

obligatorischen Schulzeit und der allgemeinen Mittelschule und Berufsfachschule vom 14. September 2011, welche die Verletzung der Dienstpflichten behandelt, unbeschadet der straf- und zivilrechtlichen Folgen sowie der Haftungsbestimmungen.

⁹Bei Verdacht auf möglicherweise strafrechtlich relevante Taten informiert der Informatikverantwortliche die Schuldirektion, die ihrerseits ihren Dienstchef unterrichtet, welcher über die zu ergreifenden Massnahmen entscheidet. Bei Verdacht einer Straftat können die Daten während 100 Tagen aufbewahrt werden.

¹⁰Wird eine Straftat festgestellt oder besteht ein starker Verdacht auf eine Straftat, die von Amtes wegen verfolgt wird, ist der betreffende Dienstchef verpflichtet, unverzüglich den zuständigen Staatsanwalt, den Vorsteher des Departements und den Staatsrat zu informieren.

¹¹Die Schuldirektion der betroffenen Schule ergreift in Zusammenarbeit mit der Polizei und den Behörden die notwendigen forensischen Massnahmen, um relevante Beweismittel sicherzustellen. Sie behandelt das Ergebnis und die für die Ermittlung erhobenen und aufbewahrten Daten vertraulich.

¹²Wird offiziell (durch Dokumente oder andere sachdienliche Unterlagen) festgestellt, dass die im Rahmen einer personenbezogenen Kontrolle gesammelten und aufbewahrten Daten nicht für allfällige Verfahren dienlich sind, werden sie innert 30 Tagen nach der Feststellung vernichtet.

¹³Bei missbräuchlicher Überwachung eines Benutzers kann auf Gesuch der persönlich kontrollierten Person ein Verfahren eingeleitet werden (auf dem Dienstweg).

¹⁴Der Staatsrat bestimmt das Untersuchungsorgan, das garantiert unparteiisch sein muss.

9. Sanktionen

¹Jegliche missbräuchliche Nutzung und jegliches Verhalten, das gegen die Bestimmungen dieses Reglements verstösst, sind ausdrücklich untersagt.

²Bei Nichtbefolgung des vorliegenden Reglements wird der Zugang des Benutzers zum Informationssystem der Schule beschränkt oder gesperrt.

³Verstösse gegen die Gesetzgebung können strafrechtlich verfolgt werden und administrative Massnahmen nach sich ziehen (Art. 46 des Gesetzes über das Personal der obligatorischen Schulzeit und der allgemeinen Mittelschule und Berufsfachschule vom 14. September 2011, SGS/VS 400.2).

10. Schlussbestimmungen

¹Die Schuldirektion setzt ihr Lehr- und Verwaltungspersonal über die in den vorliegenden Weisungen festgelegten Rechte und Pflichten in Kenntnis. Bei Inkrafttreten dieser Weisungen übermittelt sie diesen gegen Empfangsbestätigung und Unterschrift eine Kopie davon und bewahrt die Empfangsbestätigungen auf. Die gleiche Vorgehensweise gilt bei der Anstellung neuer Mitarbeiter, unabhängig davon wie lange sie an der Schule tätig sind.

²Die Schuldirektion ist in ihrer Leitungsfunktion für die Anwendung der vorliegenden Weisungen verantwortlich, vorbehaltlich der Zuständigkeit anderer Organe.

11. Verpflichtung

Mit seiner Unterschrift bestätigt der Benutzer, das vorliegende Reglement zur Kenntnis genommen zu haben, und verpflichtet sich zur Beachtung der Bestimmungen.

Die Schuldirektion:
Rolf Burgener



Siders, August 2026