Informatik-Nutzungsbestimmungen der SAMD

Die Schweizerische Alpine Mittelschule Davos (SAMD) hat Informatikmittel, welche den Mitarbeitenden sowie Schülerinnen und Schülern im Rahmen ihrer Schulausbildung und zur Festigung der Medienkompetenz zur Verfügung stellt.

Als Informatikmittel gelten Hardware wie Computer-Arbeitsstationen, Server, Netzwerke, Beamer, Telekommunikationseinrichtungen, Drucker, Multimediageräte und sonstige Peripherie sowie Software wie Betriebssysteme, Programme und Dateien. Die Informatikmittel stehen im Alleineigentum der SAMD.

Diese Informatik-Nutzungsbestimmungen der SAMD sind Teil der Schulordnung und beinhalten verbindliche Benutzungsregeln für den rücksichtsvollen und verantwortungsbewussten Umgang mit der Informatikinfrastruktur.

Mit jeder Nutzung der Informatikinfrastruktur der SAMD erfolgt die automatische Zustimmung zu den im Zeitpunkt der Nutzung in Kraft stehenden Benutzungsrichtlinien:

Allgemein

1. Die Zugangsberechtigung und Identifikationsmethoden wie Benutzername, Passwörter, etc. sind persönlich und daher vertraulich; sie dürfen weder weitergegeben noch Dritten zugänglich gemacht werden.
2. Die Nutzung von Informatikmitteln, insbesondere Computer, deren Peripheriegeräte, die zur Verfügung gestellten Anwendungen sowie das Netzwerk, dient der Ausbildung und Schulungszwecken („bestimmungsgemässe Nutzung“). Eine private Nutzung ist nur zugelassen, wenn sie unbedeutend und nicht kommerziell ist. Die Verwendung der Computer als Spielkonsolen ist untersagt, ausser ein Spiel wird im Rahmen des Unterrichts verwendet.
3. Alle Benutzenden sind persönlich dafür verantwortlich, dass die Benutzung der Informatikmittel nicht gegen Bestimmungen dieser Benutzungsordnung oder gegen die Rechtsordnung (z.B. Strafrecht, Datenschutz) verstösst bzw. die Rechte Dritter (z.B. Urheberrechte, Lizenzbestimmungen, Persönlichkeitsrechte) verletzt.

Missbrauch

4. Missbräuchlich ist jede Nutzung von Informatikmitteln der SAMD, welche die Vorschriften dieser Benutzungsordnung missachtet, gegen übergeordnetes Recht verstösst oder Rechte Dritter verletzt. Als missbräuchlich gelten namentlich die folgenden Verhaltensweisen:
   a) Die Verarbeitung, Speicherung oder Übermittlung von Material mit widerrechtlichem oder unsittlichem Inhalt, wie z.B. Gewaltdarstellungen, Pornographie (Art. 197 des Schweizerischen Strafgesetzbuches StGB)
   b) Aufforderung zu Verbrechen oder Gewalttätigkeit (Art. 259 StGB)
   c) Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB) oder Rassendiskriminierungen (Art. 261bis StGB)
   d) Die Herstellung, die Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen oder Programmteilen im Sinne von Art. 144bis Ziff. 2 StGB (Viren, Würmer, Trojaner, etc.)
   e) Das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB „Hacking“)
   f) Das Ausspionieren von Passwörtern, unautorisiertes Absuchen von internen und externen Netzwerken auf Schwachstellen (z.B. Port-Scanning), Vorkehrung und Durchführung von Massnahmen zur Störung von Netzwerken und Computern (z.B. Denial of Service Attacks). Im Einzelfall kann das „Hacking“ in einer sicheren Testumgebung zu Zwecken der Lehre erlaubt sein, sofern vorgängig die schriftliche Zustimmung der Schulleitung oder der von dieser autorisierten Stelle eingeholt worden ist. Für die Beseitigung von Verwundbarkeiten und Sicherheitslücken dürfen die

Netzwerkbereich- und Systemverantwortlichen die aufgeführten Methoden (z.B. Port-Scanning) anordnen und durchführen.

g) Datendiebstahl (Art. 143 StGB) und Datenbeschädigung (Art. 144bis Ziff. 1 StGB);
h) Die Nutzung von Informatikmitteln der SAMD in absichtlicher Verletzung von Lizenzbestimmungen oder Urheberrechten;
i) Das Versenden von Mitteilungen mittels elektronischer Kommunikationsmittel mit vorgetäuschten oder irreführenden Absenderangaben (inkl. technischer Adresse) oder von unverlangten Werbe-E-Mails (SPAM);
j) Die Belästigung oder Irreführung von Angehörigen der SAMD oder Dritter durch Mitteilungen mit elektronischen Kommunikationsmitteln (z.B. mit persönlichkeitsverletzenden, sexistischen, rassistischen, rufschädigenden oder diskriminierenden Inhalten);
k) Das Einrichten von Direktanschlüssen an die SAMD-Kommunikationsnetze (z.B. durch Modems, Routers oder WLAN Access Points) ohne vorgängige Zustimmung des Informatikverantwortlichen der SAMD.
l) Das vollständige oder teilweise Kopieren von SAMD-lizenzierter Software (Programme und Dokumentation), gleich welcher Herkunft, soweit nicht Lizenzbestimmungen oder das Urheberrechtsgesetz dies ausdrücklich erlauben.

5. Als schwerer Missbrauch gelten:
   a) Missbräuche welche vorsätzlich bzw. absichtlich erfolgen
   b) Missbräuche im Wiederholungsfall

   Wird ein Missbrauch festgestellt, so kann die bzw. der Informatikverantwortliche der SAMD entsprechende Massnahmen und Sanktionen anordnen, wie etwa die Sperrung des Zugangs zu Informatikmitteln. Bei schwerem Missbrauch wird in jedem Fall ein Disziplinarverfahren und gegebenenfalls auch ein Zivil- und Strafverfahren eingeleitet. Besonders schwere Fälle können zur Entlassung bzw. zum Schulausschluss führen. Die bzw. der Informatikverantwortliche der SAMD leitet Fälle von schwerem Missbrauch an die Schulleitung zur weiteren Behandlung und Entscheidung weiter.

Privatnutzung

6. Die Nutzung von Informatikmitteln ist für private Zwecke erlaubt, soweit sie nicht übermässig ist und die Erfüllung der Arbeits- oder Studienpflichten nicht beeinträchtigt. Die Nutzung von Informatikmitteln der SAMD darf nicht zu einer technischen Störung oder Beeinträchtigung des Betriebs der SAMD oder zu einer unverhältnismässigen Beanspruchung oder Belastung von allgemein genutzten Ressourcen (Netzwerke, Internetzugang, etc.) führen. Insbesondere sind Onlinespiele verboten, sofern diese nicht im Rahmen des erteilten Unterrichts verwendet werden.
7. Die private Nutzung von SAMD-lizenzierter Software ist für an der SAMD immatrikulierte Schüler bzw. Mitarbeitende erlaubt, soweit dies der jeweilige Lizenzvertrag zulässt. Der Informatikverantwortliche der SAMD gibt über die entsprechenden Nutzungsmöglichkeiten Auskunft.
8. Die Verwendung von privaten Geräten im Netzwerk der SAMD ist nur mit Einhaltung von Sicherheitsmassnahmen erlaubt. Dazu gehören insbesondere:
   a) Installation und Aktivierung der neuesten Antivirus-Software;
   b) Installation der Sicherheitsupdates der Betriebssysteme;
   c) regelmässige Datensicherung; sofortiges Melden von Sicherheitsproblemen an den Informatikverantwortlichen der SAMD.
9. Die Verantwortung für die Erfüllung der Sicherheitsmassnahmen obliegt der Eigentümerin oder dem Eigentümer des privaten Gerätes.

Sorgfaltspflicht / Haftung

10. Die Benutzenden haben die ihnen von der SAMD zur Verfügung gestellten Informatikmittel mit der gebotenen Sorgfalt zu nutzen.
11. Für vorsätzlich oder fahrlässig verursachte Schäden und technische Störungen an Informatikmitteln der SAMD haftet in jedem Fall der bzw. die Verursachende. Dies gilt auch

für vorsätzlich oder fahrlässig verursachte Schäden und Verletzungen von Rechten Dritter (insbesondere Urheberrechte und Lizenzbestimmungen), welche innerhalb oder ausserhalb der Schule mit Informatikmitteln der SAMD verursacht wurden. Die SAMD behält sich vor, Regress auf den Verursacher, die Verursacherin zu nehmen, sollte sie von Dritten belangt werden.

12. Bei Lizenzverletzungen durch Anbieten bzw. durch zur Verfügung stellen von Musik-, Film oder anderen Dateien auf Websites oder anderen Datenhaltungssystemen müssen die Mitarbeitenden bzw. Schüler mit möglichen Schadenersatzforderungen rechnen.
13. Bei der Beteiligung an Diskussionen in Newsgroups sind die Regeln -"Netiquette" -der jeweiligen Newsgroup zu beachten. Bei Unklarheiten wenden sich die Nutzer an den Netzwerk-Administrator.

Überwachung / Datenspeicherung

14. Die Netzaktivitäten (inkl. Information über besuchte Internetseiten, E-Mailaktivitäten etc.) können von der SAMD bis zu 18 Monate gespeichert werden. Nach spätestens 18 Monaten werden die Daten gelöscht.
15. Der Informatikverantwortliche der SAMD kann gestützt auf die Datenschutzgesetzgebung Protokollierungen (z.B. Logfiles) summarisch auswerten, ohne dabei bestimmte Personen zu identifizieren. Ergibt sich aus dieser nicht personenbezogenen Auswertung ein Verdacht auf Verstoss gegen die Weisung betreffend Nutzung von Informatikmitteln, kann nach Ankündigung die Aufzeichnungen personenbezogen während einer begrenzten Zeitdauer ausgewertet werden, um fehlbare Personen zu ermitteln.
16. Grundsätzlich werden die Schülerinnen und Schüler sowie die Mitarbeitenden im Voraus darüber informiert, wenn eine personenbezogene Prüfung vorgenommen wird. Auf die Vorankündigung kann auf Anordnung des Informatikverantwortlichen verzichtet werden, wenn die Datensicherheit, insbesondere die Verfügbarkeit der Systeme nicht mehr garantiert werden kann oder Anhaltspunkte für ein rechtswidriges, insbesondere strafbares Handeln vorliegen.
17. Der Computerraum wird videoüberwacht. Die Videodaten werden in aller Regel höchstens während eines Monats gespeichert und danach gelöscht. Das Videomaterial wird nur in begründeten Fällen gesichtet.
18. Wird aufgrund der personenbezogenen Prüfung ein Missbrauch festgestellt, werden die Schulleitung bzw. gegebenenfalls die Strafverfolgungsbehörde informiert.

Weitergehende Bestimmungen

Computerraumbenutzung

19. Schülerinnen und Schüler der SAMD erhalten nach einer Einführung Zugang zum Computerraum. Zum Vorbereitungszimmer A15 haben Schüler keinen Zutritt.
20. Die Öffnungszeiten werden per Anschlag bekannt gegeben. Der Klassenunterricht im Computerraum hat Priorität. Die Reservationsliste ist verbindlich.
21. Essen und Trinken ist im Computerraum nicht gestattet.
22. Der von der Schule erhaltene Mail-Account ist täglich zu lesen.
23. Beim Verlassen des Computerraumes wird der Arbeitsplatz sauber aufgeräumt. Stühle werden wieder an den vorgesehenen Platz gestellt. Papiere und Abfälle sind zu entsorgen!
24. Vorschläge, Änderungswünsche und weitere Hinweise sind zu richten an: ivan.bergamin@samd.ch

Speicherplatz

25. Alle Schüler der SAMD erhalten die Möglichkeit, auf den Speichermedien der SAMD ihre für den Unterricht erforderlichen Daten abzuspeichern. Dazu stehen ihnen jeweils maximal 50 GB Speicherplatz zur Verfügung. Dem Lehrkörper steht jeweils maximal 100 GB Speicherkapazität zur Verfügung. Die Speicherplatzmenge kann vom Informatikverantwortlichen der SAMD nach Bedarf und auf Ankündigung hin angepasst werden.
26. Die von den Schülern gespeicherten Daten werden nicht durch ein Backup gesichert. Es ist daher anzuraten, kritische Daten auf privater Basis ebenfalls zu sichern.

Datenzugriff

27. Der Zugriff auf die persönlichen Daten erfolgt entweder vor Ort durch das Anmelden auf einem Client mit den persönlichen Zugangsdaten, oder mittels VPN-Verbindung. Die Informationen zur Einrichtung des VPN-Zugangs sind auf der Website der SAMD bzw. auf moodle.samd.ch publiziert.

Bandbreite

28. Die jedem Nutzer zur Verfügung stehende Netzwerkbandbreite des WLANS ist limitiert auf 5 MBits/s.

Störungen

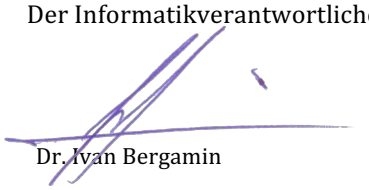
29. Störungen sind unverzüglich dem Systemverantwortlichen mündlich, schriftlich oder per E-Mail mitzuteilen: ivan.bergamin@samd.ch zu melden. **Eigene Reparaturversuche jeglicher Art sind zu unterlassen**. Reparaturkosten, die durch unsachgemässen Umgang entstehen, werden den Schülern belastet.

Schlussbestimmungen

30. Änderungen dieses Benutzerreglements bleiben vorbehalten.

Davos, August 2017

Der Informatikverantwortliche



Dr. Ivan Bergamin