Informatik-Reglement

Inhalt

1. Grundlagen

Die Primarschule Weinfelden stellt vernetzte Computer inklusive Lern- und Standardsoftware, Peripheriegeräte, verschiedene Serverdienste (E-Mail, usw.) sowie den Zugang zum Internet zur Verfügung. Die Vernetzung erfolgt sowohl per LAN (kabelgebunden) als auch per gemanagtem WLAN.
Das Netzwerk ist gegen Bedrohungen durch Viren und Spam geschützt, Serverdaten werden automatisch gesichert (Backup).
Jegliche Anschaffung von Geräten, die ins Netzwerk eingebunden werden (z.B. WLAN-Accesspoints), muss mit dem Informatikverantwortlichen abgesprochen werden.

Ergänzende Informationen

Umfassende und ergänzende Informationen zur gesamten Informatik sowie die in diesem Reglement erwähnten Anleitungen findet man auf der Webseite www.informatik-psw.ch.

Einführungskurs für neue Mitarbeitende

Einmal pro Jahr findet ein obligatorischer Einführungskurs für neue Mitarbeitende statt.

2. Allgemeines

Erwachsene Nutzerinnen und Nutzer sind selbst für die Einhaltung dieses Reglementes verantwortlich. Bei Verstössen werden in Absprache mit der vorgesetzten Stelle disziplinarische Massnahmen in Betracht gezogen (zum Beispiel bei grobem Verstoss, der Ausschluss von der Nutzung der gesamten Informatik-Infrastruktur).
Die Server- und E-Mail-Dienste stehen von Zeit zu Zeit während kurzen Wartungsfenstern nicht zur Verfügung.

Persönliche Informatikmittel

An der Primarschule gibt es in der Regel keine privaten Informatikmittel. Hingegen erhalten alle Mitarbeitenden einen eigenen Account (mit E-Mail-Adresse), persönlichen Speicherplatz auf dem Server und ein servergespeichertes persönliches Profil. Auf jedem Gerät, mit dem man sich im Netzwerk anmeldet, erhält man seinen individuellen Desktop und seine individuellen Einstellungen.

Einsatz von privaten Geräten

Die Mitarbeitenden dürfen private Geräte im Schulnetz verwenden, halten sich aber auch an die Bestimmungen, sofern anwendbar (z.B. einzelne Punkte aus den Kapiteln Sicherheit, Datenablage, Datenschutz).
Die Mitarbeitenden beachten die ausgeführten Verhaltensweisen auch für private Geräte oder Datenträger, die sie in der Schule benutzen, und für die Geräte, mit welchen sie auf den Schulserver per Remote zugreifen (Fernzugriff).
Private Netzwerkgeräte (z.B. WLAN-Accesspoints, Netzwerk-Drucker) dürfen nur mit entsprechender Bewilligung durch den Informatikverantwortlichen eingesetzt werden.

Nutzung durch Schülerinnen und Schüler

Den Lehrpersonen obliegt die Aufsichtspflicht (Einführung und Aufsicht gemäss der Schüler-Nutzungsvereinbarung siehe www.informatik-psw.ch/seiten/nutzungsvereinbarung.php) über die Nutzung der Informatikmittel durch die Schülerinnen und Schüler inklusive Internet und E-Mail.
Bei einem erkannten Missbrauch der Nutzung reagiert die Klassenlehrpersonen verhältnismässig.

3. Sorgfalt

Umgang mit Informatikmitteln

Die Mitarbeitenden gehen sorgfältig mit den Informatikmitteln um. Spätestens am Ende des Arbeitstages schalten sie die Geräte / Steckdosenleisten aus. Störungen oder Schäden melden sie dem Informatikverantwortlichen.

Einsatz von Informatikmitteln ausserhalb der Schule

Bei der Verwendung der Informatikmittel (Notebook, Beamer u.a.) ausserhalb des Schulhauses (z.B. Klassenlager) treffen die Mitarbeitenden der Situation angepasste Massnahmen gegen Verlust, Diebstahl oder Beschädigung.

4. Installationen

Zusätzliche Software

Die Mitarbeitenden dürfen zusätzliche Software installieren und erhalten hierfür den lokalen Administratorenzugang vom Informatikverantwortlichen.
Es darf nur Software aus sicheren Quellen installiert werden, die vor der Installation auf Malware untersucht wurde.
Die Mitarbeitenden sind sich bewusst, dass individuell installierte Software nach einer Computer-Neuinstallation wieder gelöscht und die Grundkonfiguration wiederhergestellt wird.

Kopieren von Software

Die Mitarbeitenden kopieren keine auf Server oder Client installierte Software auf einen privaten Datenträger, ausgenommen die Softwarelizenz erlaubt dies explizit. Auch geben sie den Schülerinnen und Schülern nur Software mit nach Hause, die für einen solchen Gebrauch lizenziert ist.

5. Sicherheit

Kennwort für Anmeldung

Die Mitarbeitenden verpflichten sich, ein sicheres Kennwort für die Anmeldung am Computer/Server zu verwenden. Dies gilt auch für weitere Zugänge wie z.B. LehrerOffice.
(mindestens 10 Zeichen, Gross- und Kleinbuchstaben, Zahlen, Sonderzeichen, keine existierenden Wörter oder Daten, nicht identisch mit Benutzernamen auch nicht teilweise, am besten die Abkürzung eines Satzes wie “Ich gehe oft mit meinen 3 Kindern und unserem Hund auf den Spielplatz.“ = “I-gomm3K+uHadS.“)
Das vom Administrator erstellte Initialkennwort wird sofort geändert.
Das Kennwort muss sicher verwaltet werden und darf an niemanden weitergegeben werden.
Von Zeit zu Zeit wird das Kennwort geändert, insbesondere bei Missbrauchsverdacht und unverzüglich nach entsprechender Aufforderung.
Wenn Mitarbeitende ein Kennwort von einem anderen Nutzer erfahren, melden diese das dem Nutzer und / oder dem Informatikverantwortlichen sofort.
Wenn Mitarbeitende den Computerarbeitsplatz – auch nur für kurze Zeit – verlassen, melden sie sich ab oder sperren den Account (⊞ + L).

Administratorenzugang

Die Mitarbeitenden gehen vertraulich mit dem lokalen Administratorenzugang um und verwenden diesen nur, wenn er unbedingt benötigt wird (Installationen, Softwaretests, Softwareaktualisierungen u.ä.).

Viren und Malware

Die Mitarbeitenden versuchen nach bestem Wissen und Gewissen zu verhindern, dass sie Viren oder andere Malware einschleppen.
Im weiteren sollen die allgemein gültigen E-Mail-Sicherheitsrichtlinien eingehalten werden, wie sie zum Beispiel auf der Webseite www.informatik-psw.ch beschrieben sind.

Verbindung mit Server

Eine Remoteverbindung soll nur für die Dauer des Austausches und nicht für die Bearbeitung von Daten auf dem Sever aufrechterhalten werden.

Internet

Die Mitarbeitenden rufen bei der Arbeit mit dem Internet (Down- und Upload) keine anstössigen oder widerrechtlichen Seiten auf (z.B. Pornografie), machen keine illegalen Downloads und halten sich an Copyright und Datenschutz (z.B. bezüglich Film-, Foto- und Musikdateien).
Die Wahrung von Persönlichkeitsrechten muss gewährleistet sein.
Quellen werden grundsätzlich angegeben, nach Möglichkeit wird für die Weiterverarbeitung die Bewilligung der Autorinnen und Autoren eingeholt.

E-Mail

E-Mail Anhänge dürfen nur geöffnet werden, wenn diese von einer vertrauenswürdigen Quelle stammen oder diese angefordert wurden.
Es dürfen keine Materialien (Texte, Bilder, Filme, usw.) verbreitet werden, welche gegen Gesetze verstossen oder den Ruf der Primarschule beeinträchtigen könnten.
Rechtswidrige und persönlichkeitsverletzende Aussagen per E-Mail sind verboten, ebenso wie das Versenden von Massenmails und Kettenbriefen.

6. Datenablage

Server

Die Mitarbeitenden speichern ihre Daten auf dem Server in ihrer persönlichen Datenablage / im Home (U:\) oder in einer allgemeinen Ablage (z.B. Teachers EH/MH/PR/ALL). Diese werden durch ein tägliches Backup gesichert. Auf dem Desktop werden in der Regel nur Verknüpfungen abgelegt.
Speicherintensive Daten (z.B. Foto-, Film- oder Audiosammlungen) werden – wenn überhaupt – nur temporär auf dem Server gespeichert, ausgenommen diese werden regelmässig für den Unterricht benötigt. Der Speicherplatz auf dem Server und für das E-Mail-Konto ist kontingentiert. Daten, die sich im Papierkorb des E-Mail-Konto befinden, werden nach 30 Tagen definitiv gelöscht.
Von Zeit zu Zeit räumen die Mitarbeitenden ihre persönliche Datenablage und die von ihnen abgelegten Daten in allgemeinen Ablagen auf und löschen nicht mehr Benötigtes (z.B. alte Fotosammlungen).

Lokale Festplatte

Die Mitarbeitenden sind sich bewusst, dass Daten, die sie auf der lokalen Festplatte speichern (z.B. im Laufwerk D:\), nicht gesichert werden und nach Updates möglicherweise gelöscht sind.

Cloud

Datenablagen in der Cloud (auch jene, die mit dem Schullogin verknüpft ist) unterliegen der eigenen Verantwortung.

Transfer der Daten bei Austritt

Wenn die Primarschule Weinfelden verlassen wird, kümmern sich die Mitarbeitenden selber um den Transfer ihrer Daten. Der Informatikverantwortliche informiert sie über das genaue Datum, an welchem ihr Account und ihre Daten auf dem Server gelöscht werden. Dazu gehören auch die Mailadresse und alle Maildaten (Mails, Kontakte, Kalender usw.). Falls Mitarbeitende aus einem speziellen Grund (z.B. Freistellung, Tod u.a.) nicht mehr auf ihre Daten zugreifen können, erhält der Informatikverantwortliche, in Absprache mit der Schulleitung, vollumfängliche Zugriffsrechte auf Daten und E-Mails, egal ob diese geschäftlicher oder privater Natur sind. Geschäftliche Daten werden anschliessend der Schulleitung übergeben.

7. Datenschutz

Datensicherung (Backup)

Grundsätzlich sind alle Mitarbeitenden verantwortlich für den Inhalt und die Sicherung der von ihm abgelegten Daten (Eigensicherung von besonders wichtigen Daten).
Die Daten auf dem Server werden täglich gesichert. Der Informatikverantwortliche übernimmt aber keine Haftung für verlorengegangene Daten.
Wenn Daten oder Mails versehentlich gelöscht oder überschrieben wurden, meldet sich der Mitarbeitende so schnell wie möglich beim Informatikverantwortlichen, der diese in den meisten Fällen über einen beschränkten Zeitraum aus alten Sicherungen wiederherstellen kann.

Allgemeine Ablagen

Daten auf allgemeinen Ablagen werden von den Mitarbeitenden besonders sorgfältig behandelt und nur gemäss Absprache (benutzen, ändern, löschen) verwendet.
Von Daten, die der Mitarbeitende selber auf solchen Ablagen speichert, hat er bei Bedarf eine Sicherheitskopie in seiner persönlichen Ablage erstellt, da diese von anderen jederzeit gelöscht werden können (insbesonders Ablage “Alle“).

8. Umgang mit besonders sensiblen und vertraulichen Daten

Wird in einem separaten Merkblatt geregelt.