Berner
Bildungszentrum Pflege

IT-Weisung für Studierende – Prozesse, Nutzung, Datenschutz und Sicherheit

Verfasser:	A. Herzig / D. Breiting	Version: V1.2
Datum	01.03.2012	Genehmigung: GL
Inkrafttreten	01.03.2012	

1. Anschaffungen: Sämtliche Anschaffungen resp. Bestellungen sind durch unsere Informatikabteilung (SI) zu prüfen resp. durch SI direkt zu besorgen. Ausnahme: persönliche Laptop; hier gelten lediglich die Mindestanforderungen, welche bei der Studierendenadministration angefragt werden können.

2. Installieren/Einrichten/private Geräte: Hardware und Software (einschliesslich Programme, Konfigurations- und Programmänderungen, Treiber, Modems, WLAN Access Points, etc.) dürfen nur durch SI installiert werden. Die Verwendung von privaten Geräten innerhalb des Netzwerkes der Schule ist nur auf Antrag und mit Zustimmung von SI erlaubt. (Ausnahme: persönliche Laptop).

3. Herunterladen von Daten: Daten (einschliesslich Multimedia) dürfen nur auf das Netzwerk der Schule heruntergeladen werden, wenn die Daten schulrelevant sind, die Auflagen der Schule sowie die gesetzlichen Bestimmungen für die Beschaffung und Verwendung eingehalten werden und die Sicherheitsbestimmungen der Schule nicht verletzt werden.

4. Herunterladen von Software: Das teilweise oder vollständige Kopieren von Software (Programme, Applikationen) und/oder Daten von der IT-Architektur der Schule ist, unabhängig deren Herkunft, in jeder Hinsicht untersagt.

5. Datenschutz: Ziel des Datenschutzes ist es, die Privatsphäre und Persönlichkeitsrechte jedes Einzelnen umfassend zu schützen. Dieser Schutz ist gewährt, wenn personenbezogene Daten nicht an Dritte resp. nicht ohne Wissen resp. Einwilligung der Betroffenen weitergegeben resp. durch das Email oder Internet zugänglich gemacht werden. Personendaten im Sinne der Datenschutzgesetzgebung sind Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person. Darunter fallen im Schulbereich u.a. **Eignungsabklärungen, Prüfungsunterlagen, personenbezogene Dossiers (Verfügungen, Korrespondenz, Gesuche, Vermerke, Berichte, Evaluationen, Fragebögen, Befragungsprotokolle, Foto, etc.)**. Studierende sind angewiesen, schützenswerte Daten nicht einzusehen, zu kopieren und/oder zu versenden.

6. Urheberrecht: Im Web veröffentlichte Daten (Bilder, Texte, Grafiken, etc.) müssen in jedem Fall auf ihre Urheberrechte geprüft werden. Auszüge aus urheberrechtlich geschützten Werken (Zeitungsartikel, Bilder, etc) sind mit Quellenangaben zu publizieren. Für die Veröffentlichung von Namen oder Aufnahmen von Personen ist deren Zustimmung sicherzustellen. Das Setzen von Links in veröffentlichten Daten kann bereits urheberrechtliche Auflagen mit sich ziehen, insbesondere wenn die verlinkte Seite nicht in einem neuen Fenster aufgeht. Um Klagedrohungen oder Schadenersatzforderungen zu entgehen, ist der Urheber für die Veröffentlichung um Erlaubnis zu fragen. Im Bedarfsfall müssen gesonderte Nutzungsrechte mit den jeweiligen Urhebern im Voraus abgeklärt werden.

7. Virenschutz: Trotz der technischen Vorkehrungen der Schule, welche die Einschleusung und Verbreitung von Viren laufend verhindern soll, sind Vorkehrungen und Sicherheitsmassnahmen durch die einzelnen Studierenden notwendig. Bei Virenmeldungen, Unstimmigkeiten oder im Zweifelsfalle muss umgehend SI kontaktiert werden. Die persönlichen Laptops sind mit einem laufend aktuell gehaltenen Virenschutzprogramm zu versehen.

8. Zugriffsrechte: Der Zugriff auf Anwendungen und Daten wird grundsätzlich über Berechtigungsgruppen und/oder –rollen geregelt.

9. Individuelle Zugriffsberechtigungen: Jedem/r Studierenden ist ein eigener Benutzername (User-ID) mit dazugehörendem Passwort zu vergeben. Die Verwendung derselben User-ID für mehrere Personen ist grundsätzlich nicht gestattet. Das Zugangskonto ist persönlich und nicht übertragbar. Die auf das Zugangskonto eingetragene Person ist für dessen Geheimhaltung unter Beachtung aller notwendigen Vorsichtsmassnahmen verantwortlich.

10. Fernzugriff: Der Zugriff auf Sharepoint von extern ist passwortgeschützt. Die Studierenden sind verantwortlich für den entsprechenden Zugriffsschutz zur Verhinderung unberechtigter Einsichtnahme und Verwendung.

11. Passwort: Das persönliche Passwort muss zum persönlichen Schutz streng vertraulich behandelt werden, und darf Dritten und anderen Studierenden nicht weitergegeben werden. Für die Passwortbildung kann man sich einen Satz merken und dessen Anfangsbuchstaben verwenden: Mein neues Auto kostet mich jetzt 40k$ = MnAkmj40k$. Beim kurzzeitigen Verlassen des Arbeitsplatzes ist die Sessionssperre obligatorisch zu aktivieren.

12. Beim **Beenden der IT-Arbeit** und Verlassen des IT-Arbeitsplatzes ist die Arbeitsstation runterzufahren.

13. e-mail/Internet: Der Email-Verkehr gilt als Schul-korrespondenz – die dafür gesetzlichen Auflagen sind zu beachten. Die zur Verfügung gestellten IT-Mittel dienen ausschliesslich dem dafür vorgesehenen betrieblichen Zweck.

Ausnahmen:

- Die Nutzung für private Zwecke ist auf ein Minimum zu beschränken.
- Die private Nutzung ist in der Regel ausserhalb der Schulzeiten (während den Pausen, über Mittag oder nach Feierabend) vorzunehmen.
- Der Schulbetrieb und die Erfüllung der zugewiesenen Aufgaben dürfen nicht beeinträchtigt werden.
- Die Systemsicherheit und die technische Infrastruktur des Auftraggebers dürfen nicht gefährdet, unverhältnismässig belastet oder gar gestört werden.
- **Die gesetzlichen Bestimmungen sind ausnahmslos zu beachten. Es ist insbesondere untersagt, auf Material mit widerrechtlichem, urheberrechtverletzendem, rassistischem, beleidigendem, erotischem, pornografischem, gewalttätigem oder herabwürdigendem Inhalt zuzugreifen oder solches zu verbreiten.**

- Online-Dienste wie interaktive Medien, Chatrooms, Newsgroups und dergleichen werden regelmässig von der SI überprüft. Bei hoher Frequenz wird der Antrag gestellt (Geschäftsleitung) diese abzustellen (kein Zugriff mehr).
- Es dürfen keine kostenpflichtigen Webseiten abgerufen, keine privaten Geschäfte getätigt, keine Spiele sowie keine Finanztransaktionen (z.B. Telebanking) durchgeführt werden.

14. Individuelle Sicherheitsprüfungen bei eingehenden Emails: Folgende Emails dürfen aus Sicherheitsgründen keinesfalls geöffnet werden:

- Emails ohne Absender oder von dubiosen Absendern mit unklaren oder zweideutigen, vielfach englischen Betreffzeilen.
- Emailanhänge resp. Beilagen mit den Endungen: bat, cmd, com, exe, ink, cmd, js, jese, msi, msp, pif, reg, scf, scr, sct, vb, vbe, vbs, wsc, wsf, wsh.

Solche Mails sind im Zweifelsfalle ungeöffnet zu löschen und aus dem elektronischen Papierkorb zu entfernen.

15. Vertragsabschluss im Internet: Für Einkäufe, die aus eigener Initiative durch persönliche Bankkarten bezahlt werden, haftet der/die jeweilige Studierende selber.

16. Auswertungen, Protokollierung: Um die technischen Schutzmassnahmen und Sicherheitsanforderungen zu gewährleisten, prüft SI auf Basis von periodischen, anonymen Auswertungen die Beanspruchung und Benutzung der Systeme, Anwendungen, Netzwerke, den Email- und Internet-Verkehr sowie die auf den Servern abgelegten Datenbestände. Der Zugang zu den ICT-Mitteln kann vorsorglich gesperrt werden und verdächtige Informationen können gesichert werden. Bei konkretem begründetem Verdacht auf eine strafbare Handlung kann Strafanzeige erstattet werden; der Entscheid liegt bei der Schulleitung.