



Richtlinien zum Datenschutz an der HPS Region Thun

- Nutzung elektronischer Kommunikationsmittel durch Mitarbeitende der HPS Region Thun
- Richtlinien für Bild – und Tonaufnahmen
- Bekanntgabe, Aufbewahrung und Vernichtung von Personendaten

Steffisburg, Januar 2017



Integrierender Bestandteil zum Arbeitsvertrag

Nutzung elektronischer Kommunikationsmittel durch Mitarbeitende der HPS Region Thun

Einleitung

Die HPS Region Thun will den Mitarbeitenden durch die Nutzung elektronischer Kommunikationsmittel (ICT) ermöglichen, ihre Aufgaben zeitgemäss und möglichst effizient zu erfüllen und die dafür nötigen Kontakte aufrecht zu halten.

Die von der Institution hierfür zur Verfügung gestellte Infrastruktur ist von den Mitarbeitenden sorgfältig und gemäss diesem Reglement zu nutzen. Jede missbräuchliche Nutzung ist untersagt. Die Institution bietet eine Einführung im Umgang mit der Infrastruktur und ihren Risiken an.

I. Allgemeine Bestimmungen

Art. 1 Geltungsbereich

1 Dieses Reglement gilt für jegliche Nutzung der durch die Institution zur Verfügung gestellten ICT-Infrastruktur und -dienste. Diese umfassen Hardware (Geräte), Software (Programme), Netzwerke, Daten, Support etc.

2 Das Reglement gilt auch für jegliche Nutzung privater Geräte, welche über die ICT-Infrastruktur der Institution erfolgt. Die Nutzung aller elektronischen Kommunikationsmittel während der Arbeitszeit für private Zwecke ist auf ein Minimum zu beschränken.

Art. 2 Begriffe

Elektronische Kommunikationsmittel umfassen Telefon, Fax, Internet, E-Mail, SMS, Instant Messaging und ähnliches.

II. Grundsätze und Einschränkung der Nutzung der ICT-Infrastruktur

Art. 3 Verwendung des Benutzungszugangs

1 Wer die von der Institution bereit gestellte Infrastruktur nutzen will, erhält nach schriftlicher Anerkennung dieses Reglements eine persönliche Zugangsberechtigung (Login) bzw. ein individuelles Konto.

2 Mit der Erteilung dieser Zugangsberechtigung ist die Verpflichtung verbunden, alle persönlichen und allgemeinen Benutzernamen, Kennwörter, Netzwerkschlüssel, Zertifikate etc. gemäss den Bestimmungen dieses Reglements einzusetzen, zu schützen, sowie an einem sicheren Ort aufzubewahren und vertraulich zu behandeln. Persönliche Login-Daten dürfen keinesfalls weitergegeben werden. Geschäftlich genutzte Passwörter dürfen nicht privat genutzt werden. Drittpersonen darf kein Zugang zur ICT-Infrastruktur ermöglicht werden.



3 Um unbefugte Zugriffe zu verhindern, haben die Berechtigten angemessene Schutzmassnahmen zu treffen. Dazu gehören sichere Passwörter, die regelmässig geändert werden, sowie die Verschlüsselung sensibler Daten.

4 Untersagt ist insbesondere

- a) das Umgehen der Anmeldung am Netz,
- b) die Anmeldung unter falschem Namen,
- c) der Angriff auf fremde Passwörter,
- d) das unbefugte Eindringen in Netzbereiche, für die eine besondere Zutrittsberechtigung gilt.

5 Der Mitarbeiter verhindert den unberechtigten Zugriff auf Daten der HPS durch einen angemessenen Zugriffsschutz. Ein Teil dieses Schutzes ist das automatische Sperren des Computers nach einer systemdefinierten Zeit.

6 Die Benutzenden haben zu verhindern, dass Unbefugte Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugang zu Informationen erhalten.

7 Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen des Büros, Sperren oder Herunterfahren des PCs). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

Art. 4 Unerlaubte Nutzung

Untersagt ist die Benutzung der ICT-Infrastruktur insbesondere

- a) zwecks Erwerb, Konsum und Verbreitung pornografischer Inhalte,
- b) in jeglicher Weise, welche unter Strafe gestellt ist; darunter fallen u.a. ehrverletzende, sexistische oder rassistische Äusserungen, betrügerische Handlungen, unbefugtes Abhören oder Aufnehmen von Gesprächen, urheberrechtsverletzende Nutzung etc.,
- c) zur Verwendung oder Installation von Programmen sowie durch das Einführen von Daten, welche die Sicherheit der ICT-Infrastruktur in irgendeiner Weise negativ beeinflussen oder ihre Kapazitäten übermässig belasten,
- d) durch die übermässige Beanspruchung der ICT-Infrastruktur, welche für die Institution hohe Kosten verursacht oder andere Berechtigte in der Nutzung erheblich einschränkt,
- e) zu privaten Zwecken durch Mitarbeitende, soweit die Institutionsleitung nichts anderes bestimmt.

Art. 5 Umgang mit Mails

1 Dienstliche Mails erfolgen ausschliesslich via Mail – Account der HPS (...@hpsregionthun.ch). Eine Weiterleitung dienstlicher Mails an private Mail – Accounts ist nicht erlaubt. Die Beantwortung dieser Mails erfolgt in der Regel innerhalb von zwei Arbeitstagen.



2 Verwenden Sie immer einen kurzen, aussagekräftigen Betreff. Ein Bezug auf Personen wird ausschliesslich mit Initialen markiert (z.B. Einladung Standortgespräch X.Y.)

3 Im Mailtext sind Personen ebenfalls nur mit Initialen erwähnt. Weisen Sie im Text immer auf eventuell beigefügte Anhänge hin.

4 Lernberichte, Diagnosen, Standortbestimmungen etc. sind besonders schützenswerte Daten und werden nicht als Anhang mit einer Mail versendet.

5 Die Speicherung von Lernberichten, Diagnosen, Standortbestimmungen, etc. auf einem privaten Datenträger (Festplatte, USB – Stick, etc.) ist untersagt. Dazu stellt die HPS Region Thun allen Mitarbeitenden die persönlichen Datenablagen auf der internen Matrix zur Verfügung (Speicherung im Personenordner nur so lange als notwendig). Der Versand an externe Stellen geschieht ausschliesslich per Briefpost.

6 E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten, vorsichtig zu behandeln. Es wird nahegelegt, beim Empfang einer zweifelhaften E-Mail keinen angegebenen Link anzuklicken, keine Anhänge (Attachments) zu öffnen und keinesfalls Zugangsdaten oder sonstige wichtige dienstliche oder private Daten einzugeben.

7 Die Nutzung der geschäftlichen E-Mail-Adressen als Login oder Kontaktmail für private Internet-Accounts wie zum Beispiel eBay, Amazon usw. ist verboten.

8 Ebenfalls untersagt ist das Abonnieren von privaten Newslettern auf die geschäftliche E-Mail-Adresse.

Art. 6 Überwachung und Einschränkung der Nutzung durch die Institution

1 Die Institution trifft die geeigneten technischen Massnahmen zum Schutz ihrer ICT-Infrastruktur und zur Verhinderung missbräuchlicher Benutzung.

2 Um unerlaubte Nutzung zu verhindern, ist die Institution insbesondere berechtigt, ohne besondere Vorankündigung sämtlichen Datenverkehr auf der bereitgestellten Infrastruktur zu protokollieren (ohne Kenntnisnahme der Inhalte).

3 Die Institution stellt sicher, dass die gesetzlichen Vorgaben bezüglich zulässigem Zweck und Inhalt sowie der Aufbewahrung der protokollierten Informationen eingehalten werden.

4 Personenbezogene Daten werden bei Verdacht auf Missbrauch erst aufgrund einer ausdrücklichen Anordnung der Institutionsleitung oder der Strafverfolgungsbehörden ausgewertet.

5 Bei Verstössen gegen dieses Reglement kann die Institutionsleitung die Nutzung der ICT-Infrastruktur einschränken. Wird das Reglement trotz Verwarnung erneut missachtet, kann die betreffende Person vollständig von der Nutzung ausgeschlossen werden.

6 Die Institution hat auch das Recht, Strafanzeige zu erstatten.

7 Die Institution behält sich zudem vor, in schwerwiegenden Fällen den Arbeitsvertrag mit der fehlbaren Person (fristlos) aufzulösen



III. Datenschutz

Art. 7 Datenschutz

Die Mitarbeitenden beachten bei der Nutzung der ICT-Infrastruktur, insbesondere bei der Bearbeitung von Personendaten, die Bestimmungen des eidgenössischen und kantonalen Datenschutzrechts. Die Institution stellt die hierfür nötige Orientierung und Schulung sicher.

Art. 8 Datensicherung

1 Auf allgemein zugänglichen Computern sollen keine Daten gespeichert werden. Lokal gespeicherte Daten können vom ICT-Support jederzeit und ohne Vorwarnung gelöscht werden.

2 Die Mitarbeitenden tragen persönlich die Verantwortung für den sorgfältigen und sicheren Umgang mit den benutzten Daten und Dokumente sowie deren regelmässige Sicherung bzw. Verschlüsselung gemäss den Vorgaben der Institution.

Art. 9 Massnahmen bei Austritt oder Tod

1 Beim Austritt bzw. Tod einer nutzungsberechtigten Person werden ihr Zugang sowie ihr allfälliges E-Mail-Konto und anderweitige, von der Institution zur Verfügung gestellte Nutzungsmöglichkeiten sofort gesperrt. Es wird eine entsprechende automatische Abwesenheitsmeldung installiert.

2 Das Verfügungsrecht über geschäftliche Informationen auf dem E-Mail-Konto von ausscheidenden Mitarbeitenden steht der Institution zu.

3 Allfällige private E-Mails und Daten müssen bis zur Beendigung des Arbeitsverhältnisses von der ICT-Infrastruktur der Institution entfernt werden. Andernfalls werden sie anschliessend ohne weitere Mitteilung durch den ICT-Support vollständig gelöscht.

IV. Haftung

Art. 10 Grundsatz

Alle Berechtigten sind persönlich dafür verantwortlich, dass sie bei der Nutzung der ICT-Infrastruktur nicht gegen dieses Reglement oder gegen die Rechtsordnung im Allgemeinen (Datenschutz, Strafrecht etc.) verstossen und keine Rechte Dritter verletzen.

Art. 11 Meldepflicht

Wer bei der Nutzung der ICT-Infrastruktur Unregelmässigkeiten (wie z. B. Defekte, Virenbefall, Missbräuche etc.) feststellt, ist verpflichtet, diese so schnell wie möglich dem ICT-Support bzw. der vorgesetzten Person zu melden.



Art. 12 Kostenersatz

Führen Verstösse gegen dieses Reglement zu Schäden an der ICT-Infrastruktur bzw. zu erhöhtem Supportaufwand, können diese Kosten den verursachenden Personen in Rechnung gestellt werden.

Art. 13 Haftungsausschluss

Die Institution übernimmt keine Haftung für Schäden, die Berechtigten aus der Benutzung der ICT-Infrastruktur entstehen. Dies gilt insbesondere für Schäden, welchen an privaten Geräten entstehen.

Richtlinien für Bild – und Tonaufnahmen

Einleitung

Mit Bild- und Tonaufnahmen am Arbeitsplatz und in der Freizeit werden heute oft alltägliche Ereignisse und auch besondere Momente festgehalten. Damit werden Erinnerungsstücke geschaffen, welche den Beteiligten und auch Dritten später Freude bereiten können.

Die HPS Region Thun will sicherstellen, dass die Herstellung von Bild- und Tonaufnahmen in ihrem Bereich respektvoll und rechtmässig erfolgt und dass bei der späteren Verwendung dieser Aufnahmen die Persönlichkeitsrechte und weitere berechnigte Interessen der Beteiligten und Dritter („Recht am eigenen Bild“ bzw. „Recht an der eigenen Stimme“) beachtet werden.

I. Allgemeine Bestimmungen

Art. 1 Geltungsbereich

1 Diese Richtlinie gilt für jede Art von Bild- und Tonaufnahmen, welche im Rahmen eines Betreuungs- bzw. Arbeitsverhältnisses mit der Institution hergestellt werden.

2 Sie regelt zudem die Verwendung und Verbreitung dieser Aufnahmen innerhalb und ausserhalb der Institution.

3 Diese Richtlinie gilt grundsätzlich für alle im Rahmen eines Betreuungs- bzw. Arbeitsverhältnisses mit der Institution beteiligten Personen. Für Mitarbeitende werden zusätzliche Regelungen erlassen.

Art. 2 Begriffe

Als Bild- und Tonaufnahmen gilt das Festhalten visuell bzw. akustisch wahrnehmbarer Erscheinungen mit hierfür geeigneten Einrichtungen und Geräten jeder Art.



II. Zulässigkeit, Einschränkung und Verbot von Aufnahmen

Art. 3 Zulässige Aufnahmen

1 Bild- und Tonaufnahmen sind ohne weiteres gestattet, soweit sich diese auf die allgemeine Umgebung beziehen und keine Identifizierung von einzelnen Personen ermöglichen.

2 Aufnahmen sollen generell rücksichtsvoll und grundsätzlich nur für persönliche bzw. private Zwecke erfolgen.

3 Aufnahmen dürfen die Institution oder die aufgenommenen Personen weder materiell noch ideell schädigen.

4 Aufnahmen auf privaten Geräten sind nach der deklarierten Verwendung unverzüglich zu löschen.

Art. 4 Erfordernis der Zustimmung

1 Wer Aufnahmen machen will, auf welchen eine bestimmte Person individuell oder in einer Gruppe erkennbar ist, muss vorgängig deren Einwilligung einholen.

2 Diese Einwilligung muss bei urteilsfähigen Personen freiwillig und nach angemessener Orientierung über den Zweck und die spätere Verwendung der Aufnahme eindeutig klar erfolgen. Für urteilsunfähige Personen entscheidet die gesetzliche Vertretung über die Einwilligung.

3 Für jede nicht ausschliesslich private Nutzung, insbesondere für jede kommerzielle Verwendung jeglicher Aufnahmen, ist auch eine ausdrückliche Bewilligung der Institutionsleitung erforderlich.

Art. 5 Unerlaubte Aufnahmen

Untersagt ist die Herstellung oder Verwendung von Aufnahmen insbesondere

a) im Privat- und Intimbereich; dazu zählen insbesondere Aufnahmen von Personen in den Toilettenbereichen und bei der Körperpflege,

b) wenn eine auf einer Aufnahme erkennbare Person ihre Einwilligung nicht erteilt,

c) wenn anderweitig und anhand ihres Verhaltens oder der Umstände erkennbar ist, dass die aufgenommene Person (insbesondere eine urteilsunfähige Person) mit der Aufnahme nicht einverstanden ist,

d) die Institutionsleitung keine Bewilligung gemäss Art. 4 Abs. 3 erteilt hat.

III. Aufnahmen durch die Institution

Art. 6 Verwendung für bestimmte Zwecke

1 Die Institution ist befugt, im Rahmen dieser Richtlinien (insbesondere Art. 4 und 5) Aufnahmen herzustellen und diese für allgemeine Informationszwecke (u.a. zum internen Gebrauch, zur Illustration von Internet-Seite, Jahresbericht etc.) sowie für Werbe-, Sponsoring- und weitere Zwecke zu Gunsten ihrer generellen Zielsetzungen zu verwenden.



IV. Besondere Bestimmungen für Mitarbeitende

Art. 7 Besondere Bestimmungen für Mitarbeitende

1 Mitarbeitende, welche eine Missachtung dieser Richtlinien feststellt, intervenieren unmittelbar und unmissverständlich. Soweit ihre Beobachtung von Missachtungen dies gebietet, orientieren sie darüber unverzüglich die Institutionsleitung.

Bekanntgabe, Aufbewahrung und Vernichtung von Personendaten

Der Leitfaden Datenschutz der ERZ Bern ist für die Bekanntgabe von Personendaten sowie für deren Aufbewahrung und Vernichtung verbindlich (http://www.erz.be.ch/dam/documents/ERZ/AKVB/de/09_Schulleitungen_Lehrpersonen/Sl_Ip_Unterlagen_datenschutz_leitfaden_d.pdf). Einige Exemplare des Datenschutz - Leitfadens sind in der Fachbibliothek im Teamzimmer deponiert.

V. Hinweise auf Rechtsfolgen bei Missachtung dieser Richtlinien

Art. 8 Pflicht zur Leistung von Schadenersatz bzw. Genugtuung

Mitarbeitende und Besucher/innen der Institution nehmen zur Kenntnis, dass die Missachtung dieser Richtlinien Persönlichkeitsrechtverletzungen darstellen und die Pflicht zur Leistung von Schadenersatz- bzw. Genugtuungszahlungen an betroffene Personen zur Folge haben können.

Art. 9 Haftungsausschluss

Die Institution übernimmt keine Haftung für Forderungen, welche Betroffene aufgrund von Verletzungen dieser Richtlinien geltend machen, wenn die schädigende Person über diese Richtlinien durch die Institutionsleitung hinreichend informiert wurde, insbesondere im Rahmen vertraglicher Vereinbarung oder durch allgemein zugängliche Orientierung (namentlich auf ihrer Internet-Seite).

Steffisburg, 17.01.2018

Schulleitung HPS Region Thun

V. Schlussbestimmungen

Art. 14 Inkrafttreten

Dieses Reglement tritt am 17.01.2018 in Kraft und ersetzt alle früheren Regelungen gleicher Art.