

Richtlinie zur Internet- und E-Mail-Nutzung

Amtliche Mitteilungen

IXX / 2021 | 27. August 2021

Beschlossen im Akademischen Senat am 07. Juli 2021

Herausgeber:
Der Rektor der
Evangelischen Hochschule Berlin
Teltower Damm 118-122
14167 Berlin

Richtlinie zur Internet- und E-Mail-Nutzung

Vorbemerkung

Die Nutzung von dienstlich zur Verfügung gestellten Internet- und E-Mail-Diensten bildet eine wichtige Grundlage für die Erfüllung der Arbeitsaufgaben aller Beschäftigten.

Diese Richtlinie regelt den Umfang der zulässigen Nutzung der dienstlich zur Verfügung gestellten Internet- und E-Mail-Dienste. Zudem regelt die Richtlinie datenschutzrechtlich relevante Situationen und schafft die Grundlagen für den sicheren Betrieb der Dienste und den Schutz der technischen Systeme. Diese Richtlinie soll dabei die Persönlichkeitsrechte aller Beschäftigten sichern und den Schutz personenbezogener Daten gewährleisten.

Erster Abschnitt: Allgemeines

1. Anwendungsbereich

- (1) Diese Richtlinie gilt für alle Beschäftigten der Evangelischen Hochschule Berlin, die im Rahmen ihrer Tätigkeit dienstliche E-Mail-Adressen bzw. Internetzugänge nutzen (Nutzer*innen).
- (2) Sofern die Evangelische Hochschule Berlin Personen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, dienstliche E-Mail-Adressen bzw. Internetzugänge zur Verfügung stellt, gelten die in dieser Richtlinie getroffenen Regelungen entsprechend als verbindliche Nutzungsrichtlinie.

2. Unzulässige Nutzung

- (1) Eine Nutzung der zur Verfügung gestellten dienstlichen E-Mail-Adressen bzw. Internetzugänge ist in jedem Falle unzulässig, wenn diese Nutzung
 - gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt,
 - sonstige Rechtsvorschriften verletzt,
 - offensichtlich den Hochschulinteressen entgegensteht.
- (2) Eine unzulässige Nutzung liegt insbesondere vor, wenn
 - kostenpflichtige Seiten oder kostenpflichtige Angebote ohne ausdrückliche Erlaubnis eines Vorgesetzten aufgerufen, genutzt oder angewiesen werden,
 - Inhalte mit sexistischen, pornographischen oder gewalt- bzw. kriegsverherrlichenden Äußerungen oder Abbildungen abgerufen oder zur Verfügung gestellt werden,
 - die Nutzung geeignet ist, Kinder oder Jugendliche zu gefährden oder die Menschenwürde zu verletzen.

Zweiter Abschnitt: Dienstliche und private Nutzung

3. Grundsatz der dienstlichen Nutzung
 - (1) Die zur Verfügung gestellten dienstlichen E-Mail-Adressen bzw. Internetzugänge sind grundsätzlich nur für dienstliche Zwecke zu nutzen, es sei denn, der*die Nutzer*in hat eine schriftliche Einwilligung gemäß Ziffer 16 gegenüber der Evangelischen Hochschule Berlin abgegeben. In diesem Fall ist die Nutzung in geringfügigem Umfang nach den Vorgaben dieser Richtlinie erlaubt. Solange eine solche schriftliche Einwilligung nicht abgegeben wurde, ist jegliche private Nutzung verboten.
 - (2) Private Interessen sind grundsätzlich den Hochschulinteressen unterzuordnen. Die Verfolgung kommerzieller Zwecke im Rahmen der Privatnutzung ist untersagt.
 - (3) Die Installation von Programmen aus dem Internet oder aus E-Mail-Anhängen ist unzulässig.
 - (4) Die Erlaubnis der privaten Nutzung kann jederzeit im Ganzen zurückgenommen werden. Ein Anspruch auf die Erlaubnis der privaten Nutzung besteht nicht.

Dritter Abschnitt: Internetnutzung

4. Allgemeines
 - (1) Die Erlaubnis der privaten Nutzung des zur Verfügung gestellten Internetzugangs ist auf das Abrufen von Inhalten beschränkt.
 - (2) Inhalte, die aus dem Internet geladen werden, dürfen nur dann auf einem Server oder Arbeitsplatzrechner gespeichert werden, wenn dies für dienstliche Belange erforderlich ist. Nicht mehr benötigte Inhalte sind zu löschen.
 - (3) Sofern die private Nutzung erlaubt ist, dürfen zulässige private Inhalte nur in einem als „privat“ gekennzeichneten Ordner in sehr geringem Umfang gespeichert werden.
5. Filterung und Sperrung unzulässiger Inhalte

Zur Vermeidung von unzulässigen Inhalten kann der Zugriff auf bestimmte Internetseiten und Internetdienste ohne vorherige Ankündigung zentral gesperrt werden (z.B. über entsprechende Einstellungen der Firewall).

6. Webmailer

Die Erlaubnis der privaten Nutzung des zur Verfügung gestellten Internetzugangs schließt die Erlaubnis von Webmail-Diensten zu privaten Zwecken ein. Zu den Webmail-Diensten zählen alle bei einem externen Dienstleister geführten E-Mail-Postfächer (z.B. GMX, Google Mail). Sofern Webmail-Dienste genutzt werden, dürfen die Webmail-Postfächer jedoch nur im Internet und nicht über das dienstliche E-Mail-Programm abgerufen werden. Webmail-Dienste fallen unter die Regelungen zur Internetnutzung im Sinne dieser Richtlinie.

Vierter Abschnitt: E-Mail-Nutzung

7. Allgemeines

- (1) E-Mail-Anhänge dürfen nur auf Arbeitsplatzrechnern oder Hochschulservern gespeichert werden, wenn dies für dienstliche Belange erforderlich ist. Nicht mehr benötigte Inhalte sind zu löschen.
- (2) Das Abonnieren von E-Mails über Mailing-Listen ist nur für dienstliche Zwecke und nur in dem hierfür notwendigen Maß zulässig.
- (3) Sofern die private Nutzung nicht erlaubt ist, sind eingehende private E-Mails umgehend zu löschen. Zudem sind die Absender*innen der E-Mails vom*von der Nutzer*in darauf hinzuweisen, dass dieser*diese die dienstliche E-Mail-Adresse nur zu dienstlichen Zwecken nutzen darf. Sofern die private Nutzung erlaubt ist, sollen private E-Mails nur in einem als „privat“ gekennzeichneten Unterordner des dienstlichen Postfachs gespeichert werden.

8. Vertretungsregelung

- (1) Grundsätzlich hat der*die Nutzer*in dafür zu sorgen, dass bei geplanter längerer Abwesenheit (ohne Zugriffsmöglichkeit auf das Postfach seitens des*der Nutzers*Nutzerin) eine geregelte Vertretung eingerichtet wird. Zu diesem Zweck kann ein automatischer Antworttext eingerichtet werden, der den*die Absender*in automatisch von der Abwesenheit des*der Empfängers*Empfängerin benachrichtigt und die E-Mail-Adresse eines*einer Vertreters*Vertreterin nennt. Soweit erforderlich, kann veranlasst werden, dass eingehende E-Mails automatisch an eine*n Vertreter*in weitergeleitet werden. Vertreter*innen können davon ausgehen, dass ankommende E-Mails, soweit sich aus der Betreffzeile nichts anderes ergibt, dienstlichen Charakter haben.
- (2) Kann der*die Nutzer*in eine geregelte Vertretung nicht selbst sicherstellen, darf sein*ihr elektronisches Postfach auf Anweisung des*der Vorgesetzten für einen Antworttext oder eine Weiterleitung freigeschaltet werden, sofern dies erforderlich ist. Der*Die Nutzer*in ist hierüber zu informieren.
- (3) Sofern aus dringenden dienstlichen Gründen ein Zugriff des*der Vertreters*Vertreterin auf die sonstigen Inhalte des elektronischen Postfaches erforderlich ist und der*die Inhaber*in des Postfaches nicht rechtzeitig erreicht werden kann, darf auf Anweisung eines*einer Vorgesetzten Zugriff auf die vorhandenen Inhalte des Postfachs genommen werden. Der erfolglose Kontaktversuch, Gründe und der Umfang des Zugriffs sind zu dokumentieren. Der*Die Nutzer*in ist hierüber baldmöglichst zu informieren.
- (4) Sobald der*die Vertreter*in feststellt, dass eine E-Mail privater Natur ist, darf diese nicht gelesen werden.

9. Sicherer E-Mail-Betrieb

- (1) Zur Sicherung der technischen Systeme werden E-Mails automatisiert auf das Vorhandensein von Viren oder sonstigen für das System schädlichen bzw. das System belastenden Inhalten (Bulk-Mails, Spam-Mails etc.) gescannt. Als schädlich identifizierte E-Mails können ohne Benachrichtigung des*der Nutzers*Nutzerin oder Absenders*Absenderin gelöscht werden.

- (2) Soweit trotz dieser Filterung in den Postfächern E-Mails eingehen, deren Absender*in oder Inhalt zweifelhaft erscheinen, sind diese durch den*die Nutzer*in oder dessen*deren Vertreter*in ungeöffnet zu löschen.
- (3) Absender*innen- oder Zieladressen von E-Mails können gesperrt werden, ohne Absender*in oder Empfänger*in davon zu unterrichten, wenn besondere Gründe (z.B. Abwehr von Angriffen auf Anwender*in oder Infrastruktur) dafür vorliegen.
- (4) Anlagen in Dateiform sind grundsätzlich zulässig. Das Ausführen von anhängenden Programmdateien bzw. Dateien aus unbekanntem Quellen ist wegen der damit verbundenen Virengefahr jedoch unzulässig.
- (5) Um die Verfügbarkeit der E-Mail-Systeme zu gewährleisten, werden E-Mails regelmäßig für eine bestimmte Dauer in einem Backup gespeichert. Die vom Backup erfassten E-Mails unterliegen vollumfänglich dem Schutzbereich dieser Richtlinie.

10. Archivregelung

- (1) Im Rahmen der Archivierung werden auch private E-Mails archiviert. Ein Anspruch auf Löschung privater E-Mails aus Archiven besteht grundsätzlich nicht, da die Löschung in der Regel einen unzumutbaren Aufwand erfordert. Die archivierten E-Mails unterliegen vollumfänglich dem Schutzbereich dieser Richtlinie.
- (2) Von der Archivierung nicht umfasst sind die Inhalte des als „privat“ gekennzeichneten Unterordners des dienstlichen Postfachs. Alternativ wird zudem auf die Möglichkeit des Einsatzes von Webmailern verwiesen.

Fünfter Abschnitt: Protokollierung und Auswertung

11. Protokollierung

- (1) Das E-Mail-System führt Protokolldateien über ein- und ausgehende E-Mails.
- (2) Im Zusammenhang mit der Nutzung des Internets werden
 - die IP-Adresse des abrufenden Arbeitsplatz-PCs,
 - die aufgerufenen Internetseiten (URL),
 - das Datum und die Uhrzeit des Abrufs sowie
 - der Umfang der Datenmenge
 protokolliert.

- (3) Die Protokolldaten werden nach 90 Tagen gelöscht.

12. Auswertung

- (1) Jede Auswertung von Protokolldaten muss die Regelungen des Datenschutzes berücksichtigen, insbesondere den Grundsatz der Verhältnismäßigkeit.
- (2) Die für den Datenschutz und die Sicherheit der technischen Systeme zuständigen Administrator*innen sind berechtigt, die erhobenen Protokolldaten unter Bildung von

Pseudonymen zu statistischen Zwecken auszuwerten. Sofern bei der statistischen Auswertung der begründete Verdacht entsteht, dass eine unzulässige Nutzung stattfindet bzw. stattfand, erfolgt nach Rücksprache mit dem*der Kanzler*in eine personenbezogene Auswertung der betroffenen Protokolldaten. Der betriebliche Datenschutzbeauftragte wird vor Durchführung der Auswertung informiert. Die personenbezogene Auswertung, der Umfang und die Gründe der Auswertung sind schriftlich zu dokumentieren. Die von der Auswertung betroffenen Nutzer*innen sind über die Auswertung zu informieren.

- (3) Bei dem Vorliegen des Verdachts von Straftaten können die Strafverfolgungsbehörden eingeschaltet und Beweise gesichert werden.
- (4) Gesetzlich geregelte Datenverarbeitungen bzw. gesetzlich geregelte Eingriffe in das Fernmeldegeheimnis bleiben von den vorstehenden Regelungen unberührt. Dies gilt insbesondere für Maßnahmen der Störungsprävention und dem Schutz der technischen Systeme.

Sechster Abschnitt: Schlussbestimmungen und Einwilligung

13. Ausscheiden eines*einer Nutzers*Nutzerin

- (1) Bevor ein*e Nutzer*in die Hochschule verlässt, hat er dafür zu sorgen, dass keine privaten Inhalte auf den Datenspeichern hinterlassen werden. Alle verbleibenden Daten werden als dienstlich gewertet. Offensichtlich private Inhalte unterfallen aber weiterhin dem Schutzbereich dieser Richtlinie. Die verbleibenden Datenbestände werden durch den*die ausscheidende*n Nutzer*in an den*die Vorgesetzte*n oder ggf. eine*n Nachfolger*in geordnet übergeben – diese erhalten vollen Zugriff auf die verbliebenen Datenbestände eines*einer ausgeschiedenen Nutzers*Nutzerin.
- (2) Ist eine geordnete Übergabe unter Beteiligung des*der Nutzers*Nutzerin nicht möglich, aber zu dienstlichen Zwecken dringend erforderlich, darf auf Anweisung eines*einer Vorgesetzten Zugriff auf die vorhandenen Daten und Postfächer genommen werden. Offensichtlich private Inhalte sind von dieser Regelung ausgenommen.

14. Leistungs- und Verhaltenskontrollen

Die Nutzung der Protokolldaten zu allgemeinen Leistungs- und Verhaltenskontrollen ist nicht zulässig. Davon unberührt bleibt die Auswertung von Daten gemäß den Regelungen dieser Richtlinie oder anderen Rechtsvorschriften.

15. Information der Nutzer*innen

Die Nutzer*innen sind auf die besonderen Regelungen zur Internet- und E-Mail-Nutzung hinzuweisen. Diese Richtlinie wird daher jedem*jeder Nutzer*in bekannt gemacht.

16. Einwilligung

- (1) Die Ermöglichung der privaten Nutzung in dem in dieser Richtlinie beschriebenen Rahmen setzt voraus, dass der*die Nutzer*in ausdrücklich in die in dieser Richtlinie geregelten Datenverarbeitungen einwilligt. Dies umfasst insbesondere die zentrale Spam- und Virenfilterung, die Vertretungsregelungen, die Archivierungsregelung, die Protokollierung

und die Kontrolle der Einhaltung der Richtlinie. Eine entsprechende Einwilligungserklärung muss schriftlich unterzeichnet werden.

- (2) Erklärt der*die Nutzer*in diese Einwilligung nicht, ist ihm die Internet- und E-Mail-Nutzung zu privaten Zwecken untersagt.

17. Inkrafttreten

Die Richtlinie tritt mit der Veröffentlichung in den Amtlichen Mitteilungen der EHB in Kraft.

Evangelische Hochschule Berlin
Einwilligungserklärung private Internet- und E-Mail-Nutzung

Die Evangelische Hochschule Berlin stellt mir die Nutzung der dienstlichen Internet- und E-Mail-Dienste sowohl zur Erfüllung von Arbeitsaufgaben als auch zur eingeschränkten privaten Nutzung zur Verfügung. Näheres wird durch die Richtlinie zur Internet- und E-Mail-Nutzung vom 27.08.2021 geregelt, über deren Inhalt ich aufgeklärt worden bin.

Mit dieser Einwilligung stimme ich den Inhalten der Richtlinie zu, insbesondere, dass

- durch eine zentrale Spam- und Virenfilterung ggf. auch E-Mails privaten Inhalts gelöscht werden können,
- im Falle meiner Abwesenheit (z.B. wegen Urlaubs, Krankheit, Freistellung, sonstiger Verhinderung) an mich adressierte E-Mails an eine*n Vertreter*in weitergeleitet werden oder eine Abwesenheitsnotiz versendet wird,
- in eilbedürftigen Ausnahmefällen zu Zwecken der Vertretung auf meine dienstlichen E-Mails zugegriffen werden darf,
- ich mit der Archivregelung einverstanden bin,
- die Internet- und E-Mail-Nutzung in dem in der Richtlinie näher beschriebenen Umfang zu Zwecken der Datenschutzkontrolle und zur Gewährleistung der technischen Sicherheit der Systeme protokolliert wird,
- ich bei meinem Ausscheiden sämtliche private Daten auf Systemen der Hochschule löschen werde und verbleibende Daten grundsätzlich dienstlicher Natur sind.

Die Einwilligung kann ich jederzeit mit Wirkung für die Zukunft widerrufen. In diesem Fall kann ich die zur Verfügung gestellten Internet- und E-Mail-Dienste jedoch ausschließlich zu dienstlichen Zwecken verwenden. Eine Privatnutzung ist dann verboten. Private Daten müssen gelöscht werden und dürfen nicht auf Systemen der Hochschule verbleiben.

Vorname, Nachname

Gesellschaft/ Bereich/ Abteilung

Datum Unterschrift Mitarbeiter*in