



Referat für Pädagogische Entwicklung  
IKT- und Statistikreferat

Az.: 2025-08-D-23-de-1

Original: EN

**GRUNDREGELN FÜR DIE NUTZUNG VON IKT-RESSOURCEN  
DURCH PERSONALMITGLIEDER DER EUROPÄISCHEN SCHULEN  
UND DES BGS**

---

**Anlage zu MEMO 2022-01-M-2**

## Inhaltsverzeichnis

Präambel .....	4
1. ANWENDUNGSBEREICH .....	4
2. BEGRIFFSBESTIMMUNGEN .....	4
3. ZULÄSSIGE NUTZUNG UND EIGENTUM .....	5
4. ALLGEMEINE VERHALTENSREGELN .....	5
4.1 Sorgfaltspflicht .....	5
4.2 Verschwiegenheitspflicht.....	6
5. SPEZIELLE REGELN .....	6
5.1 Dateien und Dokumente .....	6
5.2 Netzwerk- und Internetnutzung.....	7
5.3 Konten und Passwörter.....	8
5.4 Elektronische Kommunikation.....	8
5.5 Unterricht.....	9
6. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN .....	10
7. ÜBERWACHUNG .....	10
8. STRAFEN .....	11
9. NATIONALES RECHT .....	11
10. ÄNDERUNGEN .....	11
<b>ANHANG I .....</b>	<b>12</b>
1. GRUNDSÄTZE DER ZWECKBESTIMMUNG UND VERHÄLTNISSMÄSSIGKEIT .....	14
2. GENEHMIGUNG DURCH DEN VERANTWORTLICHEN .....	14
3. RECHT AUF INFORMATION.....	14
4. ZUGANGSBESCHRÄNKUNGEN .....	15
4.1 Beschränkter Anwendungsbereich .....	15
4.2 Begrenzte Zeit.....	15
4.3 Beschränkung auf befugte Personen.....	15
5. AUFBEWAHRUNGSFRISTEN .....	15
<b>ANHANG II .....</b>	<b>19</b>
<b>ANHANG III .....</b>	<b>22</b>
1. VERANTWORTLICHKEIT.....	24
2. ÜBERGABE DER ARBEIT .....	24

3. ÜBERGABE VON AUSRÜSTUNG .....	24
4. BERECHTIGUNGEN UND ZUGÄNGE .....	25
<b>ANHANG IV.....</b>	<b>26</b>
VORBEMERKUNGEN.....	27
1. DEFINITION DER PÄDAGOGISCHEN ZWECKE .....	27
2. ERSTELLEN EINES KONTOS .....	27
3. SOCIAL-MEDIA-GRUNDREGELN .....	28



## Europäische Schulen

Büro des Generalsekretärs

# Grundregeln für die Nutzung von IKT-Ressourcen durch Personalmitglieder des BGS und der Europäischen Schulen

## Präambel

In diesen Grundregeln sind die Regeln für eine ordnungsgemäße Nutzung und Verhaltensregeln für die Nutzung der IKT-Ressourcen festgelegt, die dem Personal<sup>1</sup> und jedem Gast<sup>2</sup> der [Europäischen Schule (im Folgenden die „Schule“ genannt) /dem Büro des Generalsekretärs (im Folgenden "BGS" genannt)] von [IT-Technikern/dem IKT-Referat] zur Verfügung gestellt werden.

Solche Grundregeln dienen dem Schutz des BGS, der Schulen und des Personals. Die unangemessene Nutzung von IKT-Ressourcen birgt zum Beispiel die Gefahr von Cyberattacken, Datenschutzverletzungen und wirft Fragen des geistigen Eigentums auf und kann zu einer Gefährdung von Informationssystemen und Netzwerkdiensten sowie zu rechtlichen Problemen führen.

**Diese Grundregeln ersetzen alle früheren diesbezüglichen Dokumente, die damit aufgehoben werden.**

## 1. ANWENDUNGSBEREICH

Diese Grundregeln werden der Leitung der/des [Schule/BGS] und den Personalmitgliedern (im Folgenden „Personalmitglieder“ genannt) während der Einarbeitung oder sobald die neueste Fassung verfügbar ist sowie jedem Gast mit IKT-Ressourcen der/des [Schule/BGS] zur Verfügung gestellt.

Diese Grundregeln stellen eine Anlage zur Internen Schulordnung der Schule dar und entsprechen den geltenden Gesetzen und Vorschriften in Bezug auf Urheberrecht, geistiges Eigentum, Datenschutz (einschließlich insbesondere Rechte an Bildern) und die Verarbeitung personenbezogener Daten sowie Computer-Kriminalität.

## 2. BEGRIFFSBESTIMMUNGEN

„**IKT-Ressourcen**“ bezeichnet allgemein alle Hardware-Geräte (Laptops, Workstations, Mobiltelefone, Peripheriegeräte, interaktive Whiteboards usw.), Netzwerkdienste sowie alle lokal oder per Fernzugriff zugänglichen Software-Ressourcen (Anwendungen, Datenbanken), die die ES bereitstellen und verwalten.

---

<sup>1</sup> Verwaltungs- und Dienstpersonal (VDP), abgeordnetes Personal, lokal rekrutiertes Führungspersonal, Aushilfskräfte (Praktikant/inn/en, Zeitarbeitskräfte).

<sup>2</sup> Jede Person die auf Einladung des BGS/der Schule an einer Sitzung, Arbeitsgruppe oder Schulung teilnimmt und über einen Zugang zu den IKT-Ressourcen oder ein Konto der Europäischen Schulen verfügt.

„**IKT-Referat**“ bezeichnet das IKT-Referat des BGS und dessen Personalmitglieder.

„**IT-Abteilung**“ bezeichnet die örtlichen IKT-Personalmitglieder der Schulen.

„**Netzwerkdienste**“ bezeichnet die Bereitstellung von lokalen und Remote-Diensten wie zum Beispiel Anwendungen, Nachrichtenübermittlung, Internet, Konferenzen usw. über die Netzwerk-Infrastruktur der ES.

„**Anwender**“ bezeichnet die Person, die, unabhängig von ihrem Status, Zugang zu IKT-Ressourcen und Netzwerkdiensten hat oder diese benutzt.

### **3. ZULÄSSIGE NUTZUNG UND EIGENTUM**

Die IKT-Ressourcen der/des [Schule/BGS] dienen der Erledigung der beruflichen Aufgaben der Personalmitglieder entsprechend ihrer vertraglichen oder dienstrechtlichen Beziehung zur/zum [Schule/BGS].

Die Nutzung von IKT-Ressourcen für private Zwecke ist nicht verboten, aber es wird von den Personalmitgliedern erwartet, dass sie ihr gesundes Urteilsvermögen nutzen, mit Sorgfalt vorgehen und ihr Bestes tun, um Risiken bei der Nutzung von Ressourcen für private Angelegenheiten zu vermeiden und/oder zu minimieren und gleichzeitig bei der Arbeit produktiv zu bleiben, wenn sie die Ressourcen für private Angelegenheiten nutzen.

Personalmitglieder sollten bedenken, dass berufliche Dateien und Dokumente, die über die IKT-Ressourcen der/des [Schule/BGS] erstellt wurden und die zu ihrem Beschäftigungs- oder Abordnungsumfang gehören, sowie ihnen zugewiesene Aufgaben Eigentum der/des [Schule/BGS] werden.

Aus Internetsicherheits- und Wartungsgründen können die IKT-Ressourcen der/des [Schule/BGS], wie zum Beispiel Ausrüstung, Systeme und Datenverkehr, jederzeit überwacht werden.

Alle Dokumente, Lizenzen und Software, die über die IKT-Ressourcen bereitgestellt werden, sind Eigentum der/des [Schule/BGS] und dürfen ohne vorherige Genehmigung nicht kopiert, verändert oder übertragen werden.

### **4. ALLGEMEINE VERHALTENSREGELN**

#### **4.1 Sorgfaltspflicht**

Von Personalmitgliedern wird erwartet, dass sie bei der Nutzung der IKT-Ressourcen der/des [Schule/BGS] mit Sorgfalt vorgehen. Verlust, Schäden oder Diebstahl von Eigentum der/des [Schule/BGS] ist der [IT-Abteilung/dem IKT-Referat] sofort zu melden.

Personalmitglieder müssen Geräte ausschalten oder in den Ruhezustand versetzen, wenn sie nicht genutzt werden, Ladegeräte müssen aus der Steckdose entfernt und defekte Geräte gemeldet werden, die Strom verschwenden.

Mangelnde Sorgfalt bei der Nutzung von BGS-Eigentum kann als Begründung für Disziplinarmaßnahmen angesehen werden.

## 4.2 Verschwiegenheitspflicht

Alle Personalmitglieder unterliegen zum Schutz personenbezogener und nicht-öffentlicher Daten, zu denen sie im Laufe oder im Zusammenhang mit ihrer Tätigkeit Zugang haben, einer gesetzlichen Verschwiegenheitspflicht<sup>3</sup>. Sie werden aufgefordert, die Vertraulichkeitsvereinbarung (Anhang II) während der Einarbeitung zu unterzeichnen oder sobald eine aktualisierte Fassung der Vertraulichkeitsvereinbarung zur Verfügung steht.

Diese Verschwiegenheitspflicht gilt insbesondere für alle Informationen, die den Personalmitgliedern über die bereitgestellten IKT-Ressourcen zur Verfügung stehen.

Falls Personalmitglieder Zugang zu Ressourcen haben, deren Verfügbarkeit für sie unangemessen ist, sind sie verpflichtet, das IKT-Referat/die lokale IT-Abteilung zu informieren, damit das Problem behoben werden kann.

## 5. SPEZIELLE REGELN

### 5.1 Dateien und Dokumente

#### 5.1.1 Speicherung

Personalmitglieder müssen ihre beruflichen Dateien und Dokumente im Speicherbereich ihres Geräts und/oder, falls andere Kollegen ebenfalls Zugang benötigen, in einem gemeinsamen Speicherbereich speichern.

Wie bereits erwähnt, sind IKT-Ressourcen für berufliche Zwecke bestimmt. Es können aber private Dokumente auf dem Gerät des Personalmitglieds gespeichert werden, **sofern sie keine personenbezogenen Daten anderer Personen enthalten**. Solche Dokumente müssen in einem Ordner mit der Bezeichnung „PRIVAT“ aufbewahrt werden. Personalmitglieder sollten bedenken, dass im Falle einer Datenpanne ihre privaten Dokumente betroffen sein könnten.

#### 5.1.2 Clean-Desk-Prinzip

Personalmitglieder sollten bedenken, dass Dokumente, die sie auf ihrem Schreibtisch liegenlassen, unbefugtem Zugang ausgesetzt sind. Dokumente, die vertrauliche Informationen enthalten, sollten nicht auf dem Schreibtisch oder im Drucker zurückgelassen werden.

#### 5.1.3 Verbot

Dateien und/oder Dokumente, die der öffentlichen Ordnung und Moral widersprechen oder illegal sind, zum Beispiel solche mit rassistischen, fremdenfeindlichen oder pornographischen Inhalten, sind strengstens verboten.

---

<sup>3</sup>Siehe Statuten für Personalmitglieder der Europäischen Schulen:

- Artikel 18 des Statuts für abgeordnetes Personal
- Artikel 19 des Statuts für lokal rekrutiertes Führungspersonal

## 5.2 Netzwerk- und Internetnutzung

Die Anwender sind für die angemessene Nutzung von Netzwerkressourcen und Internet verantwortlich.

Die Verwendung privater digitaler Geräte entbindet die Anwender nicht von der Verpflichtung, die in den vorliegenden Grundregeln verankerten Regeln im Hinblick auf Respekt gegenüber ihren Kollegen und den Mitgliedern der Gemeinschaft der Europäischen Schulen einzuhalten.

Ferner entbindet die Nutzung von Social Media -über IKT-Ressourcen oder ein privates digitales Gerät- die Anwender nicht von ihrer Verantwortung für von ihnen weitergegebene Inhalte.

Anwender sollten:

- Sich auf ihrem beruflich genutzten Konto nur von einem sicheren Gerät aus anmelden und die Nutzung von kostenlosem öffentlichen W-LAN vermeiden
- Ihre Geräte sperren, wenn diese unbeaufsichtigt sind
- Beim Öffnen von E-Mail-Anhängen von unbekanntem Absender besonders vorsichtig sein
- Jede verdächtige elektronische Kommunikation sofort der [IT-Abteilung/dem IKT-Referat der Schule] melden
- Im Hinblick auf die Angemessenheit der persönlichen Nutzung mit gutem Urteilsvermögen zu handeln

Folgende Aktionen sind Anwendern untersagt:

- Zugreifen auf Server, personenbezogene Daten oder ein Konto zu anderen Zwecken als der Ausübung beruflicher Aufgaben, selbst wenn sie zugangsberechtigt sind
- Versenden vertraulicher Informationen an unbefugte Empfänger
- Anmeldung in den sozialen Netzwerken mit der E-Mail-Adresse ihres Dienstkontos
- Posten oder Veröffentlichen in sozialen Netzwerken von Inhalten, die gegenüber ihren Kollegen und den Mitgliedern der Gemeinschaft der Europäischen Schulen unangemessen oder verletzend sind
- Zugreifen auf bzw. Herunterladen oder Hochladen von obszönen, beleidigenden, diskriminierenden oder anderen, gesetzlich verbotenen Inhalten
- Gesetzeswidriges Herunterladen oder Hochladen von urheberrechtlich geschützten Inhalten (z. B.: Bilder, Musik, Videos und Software)
- Herunterladen, Installieren oder Ausführen von Upgrades, Updates, Patches oder Programmen, Software oder dergleichen
- Erforschung, Untersuchung und Veränderung der Sicherheit der bereitgestellten IKT-Lösungen ohne vorherige Genehmigung
- Ausnutzung von Sicherheitslücken oder Anomalien im Systembetrieb

### 5.3 Konten und Passwörter

Konten werden (händisch oder automatisch) vom Personal des IKT-Referats erstellt. Sie sind temporär, rein persönlich und nicht übertragbar. Sie werden deaktiviert, wenn der Inhaber die Organisation verlässt.

Anwender sollten:

- Ihr Passwort gemäß den Anweisungen des IKT-Referats des BGS erstellen
- Ein starkes Passwort verwenden und es geheim halten
- Die Systemadministratoren sofort informieren, wenn ein Missbrauch des persönlichen Kontos entdeckt oder vermutet wird

**Es ist Anwendern strengstens untersagt, ihr Konto, ihre Zugangsdaten oder Passwort an Dritte** (einschließlich Systemadministratoren) weiterzugeben oder offenzulegen oder anderen die Nutzung ihres Kontos zu gestatten.

### 5.4 Elektronische Kommunikation

#### 5.4.1 Allgemeine Überlegungen

Personalmitglieder und Anwender sind für die Verwaltung ihrer E-Mail-, Chat- und sonstigen Kommunikationsinhalte während der Nutzung der IKT-Ressourcen der/des [Schule/BGS] verantwortlich.

Folgendes ist ihnen untersagt:

- Nutzung von Listen mit E-Mail-Adressen oder sonstigen Kommunikationskanälen für Zwecke, die nicht durch berufliche Ziele vorgegeben sind
- Verwenden von unangemessener Sprache in ihrer Kommunikation
- Versenden ungebetener (kommerzieller oder sonstiger), unerwünschter oder belästigender Kommunikation

Da die elektronische Kommunikation zur Erledigung der beruflichen Aufgaben der Personalmitglieder bestimmt ist, sollte die Nutzung dieser Kommunikation für persönliche Angelegenheiten auf ein Mindestmaß beschränkt werden. In einem solchen Fall sollten Personalmitglieder ihre elektronische Kommunikation als „PRIVAT“ kennzeichnen.

Funktionspostfächer dürfen nicht zum Versenden elektronischer Kommunikation benutzt werden, die nicht mit den beruflichen Aufgaben des Personalmitglieds in Zusammenhang steht.

#### 5.4.2 Abwesenheit eines Personalmitglieds

Falls Personalmitgliedern der Zugang zu ihrer elektronischen Kommunikation nicht möglich ist, wird erwartet, dass sie folgende notwendige Vorkehrungen getroffen haben, um die Kontinuität des Dienstbetriebs der Schule/des BGS zu gewährleisten:

- Aktivieren einer automatischen Abwesenheitsnachricht in Kommunikationsprogrammen wie Outlook und Angabe einer Alternative/der Kontaktdaten eines Kollegen sowie eine

Statusmeldung in Teams, die Kollegen über die Abwesenheit informiert

- Verwendung gemeinsam genutzter Ordner, in denen die Informationen für die Backup-Kollegen und/oder für alle Personen zugänglich sind, die während der Abwesenheit ein funktionelles Interesse am Zugang zu den Informationen haben

Es wird davon abgeraten, E-Mails während der Abwesenheit des Personalmitglieds weiterzuleiten, da der neue Empfänger ohne Wissen des Absenders oder des abwesenden Personalmitglieds Kenntnis von potentiell sensiblen Informationen erlangen könnte.

In Ausnahmefällen und falls vor der Abwesenheit des Personalmitglieds keine Vorkehrungen getroffen werden konnten, kann die/das [Schule/BGS] gemäß den Bedingungen in **Anhang I** den Zugang zum persönlichen Postfach gestatten. Hierbei müssen folgende Grundsätze eingehalten werden:

- Der Grundsatz der Zweckbestimmung
- Der Grundsatz der Verhältnismäßigkeit
- Der Grundsatz der Transparenz

Aufgrund der Datenschutzanforderungen<sup>4</sup> ist der Zugang zu Postfächern und Dokumenten von Personalmitgliedern, die das System der Europäischen Schulen verlassen haben (z. B. Entlassung oder Abgang) nicht möglich. Das gesamte arbeitsbezogene Material und alle Dokumente sind gemäß den Anweisungen der Vorgesetzten der Personalmitglieder vor deren Abgang auszuhändigen (siehe Anhang III).

## 5.5 Unterricht

### 5.5.1 Fernunterricht und -lernen

Lehrkräfte müssen die Bestimmungen der Strategie zu Fernunterricht und -lernen für die Europäischen Schulen in der durch den Obersten Rat genehmigten Fassung vom 29. März 2021 einhalten<sup>5</sup>.

### 5.5.2 Digitale Lernmittel

Lehrkräfte, die neue digitale Ressourcen benötigen, die für Lern- und/oder pädagogische Zwecke konzipiert und bestimmt sind, müssen den DSB der Schule konsultieren.

Dieser wird solche Ressourcen gemäß dem Verfahren zur Genehmigung des Einsatzes von digitalen Lernmitteln an den Europäischen Schulen beurteilen<sup>6</sup>.

### 5.5.3 Social Media

Im Hinblick auf die Nutzung von Social Media muss wie folgt unterschieden werden:

- Social Media fallen nicht unter das vorgenannte Verfahren, da Lehrkräfte die personenbezogenen Daten von Schüler/innen auf Social-Media-Plattformen nicht verwenden dürfen.
- Lehrkräfte dürfen Schüler/innen nicht ermutigen, persönliche

Social-Media-Konten zu erstellen.

- Lehrkräfte dürfen zu Lern- und/oder pädagogischen Zwecken gemäß den in Anhang IV festgelegten Bedingungen ein Social-Media-Konto anlegen.

Wie in Absatz 5.2 ausgeführt, dürfen Lehrkräfte aus Sicherheitsgründen mit ihren beruflich genutzten Zugangsdaten und E-Mail-Adresse kein Social-Media-Konto anlegen.

## 6. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

Gemäß DSGVO<sup>7</sup> bezeichnet die Verletzung des Schutzes personenbezogener Daten eine Verletzung der Sicherheit die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Gemäß der Richtlinie der Europäischen Schulen über die Verletzung des Datenschutzes<sup>8</sup> sind Personalmitglieder gehalten, sofort zu handeln und Verletzungen des Datenschutzes an den Generalsekretär/Direktor und/oder den DSB zu melden. Sie müssen auch mit der [IT-Abteilung/dem IKT-Referat] Kontakt aufnehmen, damit sofort Maßnahmen ergriffen werden können, um negative Folgen zu vermeiden und/oder zu begrenzen.

## 7. ÜBERWACHUNG

Aus Gründen der Internetsicherheit sowie zur Sicherung des IT-Betriebs und der Wartung können IT-Ressourcen und Datenverkehr dauerhaft oder punktuell überwacht, analysiert und auf Einhaltung und im Rahmen des geltenden Rechts geprüft werden, zu folgenden Zwecken:

- Verhinderung von Internetsicherheitsvorfällen und -angriffen
- Verhinderung von rechtswidrigen oder verleumderischen Handlungen, Handlungen, die gegen die guten Sitten verstoßen oder geeignet sind, die Würde anderer Personen zu beeinträchtigen
- Schutz wirtschaftlicher oder finanzieller Interessen der Schulen, die als vertraulich gekennzeichnet sind, und Kampf gegen gesetzeswidrige Praktiken
- Sicherheit und/oder ordnungsgemäßer technischer Betrieb der Computersysteme im Netzwerk der Schulen, einschließlich Kontrolle der damit verbundenen Kosten, sowie der physische Schutz der Anlagen in den Schulen
- Einhaltung in gutem Glauben der Grundsätze und Regeln für die Nutzung von im System der Europäischen Schulen eingerichteter Netzwerktechnik

Eine solche Überwachung -speziell für das Verwaltungsnetz- wird zumeist durch das IKT-Referat des BGS durchgeführt, während die IT der Schule für das pädagogische Netz verantwortlich ist.

Eine Überwachung sollte nach Möglichkeit mithilfe automatisierter Verfahren

erfolgen. Bei jedem manuellen Eingriff ist der Grundsatz der Verhältnismäßigkeit zu beachten, und der Systemadministrator muss das Personalmitglied, dessen Informationen überwacht werden, über die Einzelheiten des Eingriffs informieren.

Besteht der Zweck des manuellen Eingriffs darin, die Einhaltung in gutem Glauben der Grundsätze und Regeln für die Nutzung von im System der Europäischen Schulen eingerichteter Netzwerktechnik zu gewährleisten, muss dem Eingriff eine Phase der Unterrichtung vorausgehen.

## 8. STRAFEN

Verstöße gegen die Bestimmungen dieser Grundregeln können mit Disziplinarmaßnahmen gemäß den einschlägigen Statuten geahndet werden:

- Titel VI des Statuts für Mitglieder des abgeordneten Personals
- Kapitel VIII des Statuts für das Verwaltungs- und Dienstpersonal
- Kapitel VIII des Statuts für die Ortslehrkräfte

## 9. NATIONALES RECHT

Die Anwendung restriktiverer Bestimmungen der nationalen Rechtsvorschriften des Gastlandes, in dem sich die/das [Schule/BGS] befindet, bleibt von den Bestimmungen dieser Grundregeln unberührt.

## 10. ÄNDERUNGEN

Diese Grundlagen werden spätestens im Schuljahr 2027-2028 wieder überarbeitet.

---

<sup>4</sup> Grundsätze der Zweckbindung, Datenminimierung und befristeten Speicherung.

<sup>5</sup> 2020-09-D-10.

<sup>6</sup> 2020-01-D-9 Anhang zu Memorandum 2019-12-M-3/GM. Ein solches Verfahren stützt sich als Rechtsgrundlage auf die „berechtigten Interessen des Verantwortlichen“.

<sup>7</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

<sup>8</sup> 2020-05-D-7 Anhang zu Memorandum 2020-05-M-3-en-1/GM.

## ANHANG I



Schola Europaea

Büro des Generalsekretärs

Az.: 2021-10-D-71-de-1

Original: EN

### **Protokoll über den Zugang zu E-Mails und Dokumenten von Personalmitgliedern im Falle der Abwesenheit**

Anhang zu den Grundregeln für die Nutzung von IKT-Ressourcen  
durch Personalmitglieder der Europäischen Schulen und des BGS  
(2025-08-D-23)

## Protokoll über den Zugang zu E-Mails und Dokumenten von Personalmitgliedern im Falle der Abwesenheit

### Inhalt

1. GRUNDSÄTZE DER ZWECKBESTIMMUNG UND VERHÄLTNISSMÄSSIGKEIT .....	14
2. GENEHMIGUNG DURCH DEN VERANTWORTLICHEN .....	14
3. RECHT AUF INFORMATION.....	14
4. ZUGANGSBESCHRÄNKUNGEN.....	15
4.1 Beschränkter Anwendungsbereich .....	15
4.2 Begrenzte Zeit.....	15
4.3 Beschränkung auf befugte Personen.....	15
5. AUFBEWAHRUNGSFRISTEN .....	16

## **Protokoll über den Zugang zu E-Mails und Dokumenten von Personalmitgliedern im Falle der Abwesenheit**

Mit vorbeugenden Maßnahmen, wie sie in Absatz 4.4.2 genannt sind, soll die Notwendigkeit des Zugangs zum Postfach und zu den Dokumenten von Personalmitgliedern im Falle der Abwesenheit verringert werden.

Sofern diese vorbeugenden Maßnahmen die Notwendigkeit des Zugangs zu E-Mails und/oder Dokumenten eines/einer abwesenden Arbeitnehmer/s/in durch den Arbeitgeber nicht umgehen oder wenn solche Maßnahmen von dem/der Arbeitnehmer/in vor der Abwesenheit nicht ergriffen wurden, legt das vorliegende Protokoll fest, wie ein solcher Zugang erfolgen muss, um rechtlichen und datenschutztechnischen Erwägungen zu entsprechen.

### **1. GRUNDSÄTZE DER ZWECKBESTIMMUNG UND VERHÄLTNISSMÄSSIGKEIT**

Die Gewährleistung der Kontinuität des Dienstbetriebs innerhalb des/der [BGS/Schule] stellt einen rechtmäßigen Zweck für den Zugang zum Postfach und zu den Dokumenten von Personalmitgliedern dar, sofern (i) eine Dringlichkeit besteht und (ii) es keine andere, weniger einschneidende Möglichkeit gibt, auf die benötigten Informationen zuzugreifen.

### **2. GENEHMIGUNG DURCH DEN VERANTWORTLICHEN**

Die Notwendigkeit des Zugangs ist mit Hilfe des nachstehenden Formulars schriftlich angemessen zu begründen.

Ein solches Formular muss an den Generalsekretär/Direktor gesendet werden, der entscheiden wird, ob ein solcher Zugang unter den gegebenen Umständen genehmigt wird und ob:

- Die benötigten Informationen mit weniger einschneidenden Maßnahmen erlangt werden können
- Ein solcher Zugang für die Kontinuität des Dienstbetriebs erforderlich ist
- Ein solcher Zugang dringend ist oder in Anbetracht der Dauer der Abwesenheit des Personalmitglieds verschoben werden kann
- Ein solcher Zugang im Rahmen zusätzlicher vorbeugender Maßnahmen, die nicht in dem vorliegenden Anhang aufgeführt sind, genehmigt werden sollte

Der Generalsekretär/Direktor wird auch den Rat des Datenschutzbeauftragten einholen.

### **3. RECHT AUF INFORMATION**

Personalmitglieder erhalten die IKT-Grundregeln während der Einarbeitung oder sobald eine aktualisierte Fassung vorliegt. Daher sind sie über die Möglichkeit des Zugangs zu ihrem Postfach und/oder ihren Dokumenten unter den in dem vorliegenden Protokoll festgelegten Bedingungen unterrichtet.

Falls das/die [BGS/Schule] tatsächlich auf das Postfach und/oder auf Dokumente von Personalmitgliedern zugreifen muss, müssen diese telefonisch kontaktiert und ihnen *„eine ausführliche Erklärung für diesen Zugang unter Angabe der Notwendigkeit, Dringlichkeit, der Art und Weise und des Umfangs der gesuchten*

Informationen“<sup>9</sup> übermittelt werden.

Neben der Informationspflicht gemäß Artikel 13 DSGVO<sup>10</sup> sind Personalmitglieder auch über ihr Widerspruchsrecht gemäß Artikel 21 DSGVO zu informieren.

Wenn das Personalmitglied nicht zu erreichen ist und die fragliche Situation den dringenden Zugang erfordert, kann der Generalsekretär/Direktor den Zugang im Einklang mit dem vorliegenden Protokoll genehmigen.

## **4. ZUGANGSBESCHRÄNKUNGEN**

### **4.1 Beschränkter Anwendungsbereich**

Wenn eine Genehmigung erteilt wurde, um die Kontinuität des Dienstbetriebs zu gewährleisten, muss der Zugang auf die E-Mails und/oder Dokumente beschränkt werden, die sich auf den Zeitraum der Abwesenheit des Personalmitglieds oder auf einen angemessenen Zeitraum vor dieser Abwesenheit beziehen.

Der Generalsekretär/Direktor kann einen weitreichenderen Zugang genehmigen, sofern die Gründe hierfür in dem ihm/ihr vorgelegten Antrag deutlich erklärt und ausreichend begründet wurden.

Überdies sind nur die E-Mails und/oder Dokumente zu konsultieren, die sich auf den ursprünglichen Antrag auf Genehmigung beziehen.

Auf E-Mails und Dokumente, die, wie in den vorliegenden Grundregeln angegeben, als „PRIVAT“ gekennzeichnet sind, darf nicht zugegriffen werden.

### **4.2 Begrenzte Zeit**

Sobald eine Genehmigung erteilt wurde, muss der Zugang zu den Informationen des abwesenden Personalmitglieds auf zwei Arbeitstage begrenzt werden.

### **4.3 Beschränkung auf befugte Personen**

Der Generalsekretär/Direktor bestimmt die Personen, die ein rechtmäßiges Interesse daran haben, auf das Postfach und/oder die Dokumente des Personalmitglieds zuzugreifen.

Die IT-Techniker der Schule müssen die Zugangsrechte beim IKT-Referat anfordern, da sie keinen solchen Zugang zum Verwaltungsnetz haben.

Der Zugang zu den benötigten Informationen muss in Anwesenheit eines anderen Personalmitglieds (z. B. Personalvertreter/in, unmittelbare/r Vorgesetzte/r, HR-Verantwortliche/r, Referatsleiter/in) und nach Möglichkeit unter Aufsicht von IKT-Personal erfolgen.

Das IKT-Personal hat dafür Sorge zu tragen, dass bei Bedarf alle notwendigen Maßnahmen ergriffen wurden, um die Sicherheit der Informationen des Personalmitglieds (z. B. Ändern von Passwörtern) zu gewährleisten.

## **5. AUFBEWAHRUNGSFRISTEN**

Im Hinblick auf die Speicherung der Informationen, die bei dem Zugang abgerufen wurden, ist der DSB zu konsultieren.

---

<sup>9</sup> Guidelines on personal data and electronic communications in the EU institutions, Europäischer Datenschutzausschuss, Februar 2020.

<sup>10</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).



Schola Europaea

Büro des Generalsekretärs

**Formular für den Antrag auf Zugang zu den E-Mails und/oder Dokumenten eines  
abwesenden Personalmitglieds in dringenden Fällen**

<b>Name des abwesenden Personalmitglieds</b> <i>(auf dessen Informationen zugegriffen werden muss)</i>	
<b>Name der Zugang beantragenden Person</b>	
<b>Gründe für den Antrag auf Zugang</b> <i>(Warum besteht Dringlichkeit, warum ist dies der einzige Weg zur Erlangung der benötigten Informationen usw.)</i>	
<b>Art der benötigten Informationen</b>	
<b>Beschluss des Generalsekretärs/Direktors</b>	<input type="checkbox"/> Zugang gewährt <input type="checkbox"/> Zugang verweigert Datum und Uhrzeit: Unterschrift:
<b>Personalmitglied wurde telefonisch informiert</b>	<input type="checkbox"/> Ja ... Datum/Uhrzeit ..... <input type="checkbox"/> Die Person war nicht zu erreichen
<b>Name des/der Personalmitglied/s/er, das/die während des Zugangs anwesend ist/sind</b>	

**Während** des Zugangs auszufüllen:

<b>Tatsächliches Zugangsdatum</b>	Datum und Uhrzeit ...
<b>Name der Personen, die während des Zugangs anwesend sind</b>	
<b>Anmerkungen</b> <i>(Art der abzurufenden Informationen und Zeitrahmen)</i>	

**Am Ende** des Zugangs auszufüllen:

<b>Zugangsende</b>	Datum und Uhrzeit ...
<b>Anmerkungen</b> <i>(Art und Zeitrahmen der abgerufenen Informationen, Ergebnisse des Abrufs (Informationen gefunden oder nicht))</i>	
<b>Name und Unterschrift der Person, die Zugang hatte</b>	

## ANHANG II



Schola Europaea

Büro des Generalsekretärs

Az.: 2021-10-D-73-de-1

Original: EN

### Vertraulichkeitsvereinbarung

---

Anhang zu den Grundregeln für die Nutzung von IKT-Ressourcen  
durch Personalmitglieder der Europäischen Schulen und des BGS  
(2025-08-D-23)



## Schola Europaea

Büro des Generalsekretärs

### Vertraulichkeitsvereinbarung

Gemäß den für sie geltenden Statuten haben alle Personalmitglieder über Fakten und Informationen, von denen sie im Laufe oder im Zusammenhang mit der Ausübung ihrer Tätigkeit Kenntnis erlangen, strengste Verschwiegenheit zu bewahren.

Der Unterzeichnete, Herr/Frau \_\_\_\_\_, beschäftigt als \_\_\_\_\_ im/in der \_\_\_\_\_ [BGS/Europäischen Schule] \_\_\_\_\_ (im Folgenden „BGS/Schule“ genannt), habe Zugang zu vertraulichen Informationen und personenbezogenen Daten, die dem/der [BGS/Schule] gehören, und erkläre, dass ich die Vertraulichkeit der genannten Daten anerkenne.

Ich verpflichte mich daher gemäß den Anforderungen des für mich geltenden Statuts und der DSGVO<sup>11</sup>, innerhalb meines Aufgabenbereichs alle notwendigen Vorkehrungen zum Schutz des vertraulichen Charakters der Informationen zu treffen, zu denen ich Zugang habe, und insbesondere deren Änderung, Beschädigung oder Weitergabe an Personen, die nicht ausdrücklich befugt sind, solche Informationen zu erhalten, zu verhindern.

Ich verpflichte mich

- Daten, zu denen ich möglicherweise Zugang habe, nur zu den Zwecken zu nutzen, die im Rahmen meiner Tätigkeiten vorgesehen sind
- Solche Daten nur an Personen weiterzugeben, die aufgrund ihrer Tätigkeit ordnungsgemäß befugt sind, solche Daten zu erhalten
- Keine Kopie dieser Daten anzufertigen, es sei denn, es ist für die Ausübung meiner Tätigkeit erforderlich
- Alle notwendigen Vorkehrungen zu ergreifen, um die physische Sicherheit dieser Daten zu erhalten

---

<sup>11</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

- Im Rahmen meiner Befugnisse dafür zu sorgen, dass nur sichere Kommunikationsmittel zur Übermittlung solcher Daten genutzt werden, und im Zweifelsfall den DSB zu konsultieren.
- Die respektvolle Nutzung sämtlicher KI-Technologien gemäß den Vorgaben und Richtlinien der Europäischen Schulen zu gewährleisten.
- Im Falle der Beendigung meiner Tätigkeit alle Daten, Dokumente und zugrundeliegenden Informationen bezüglich dieser Daten zurückzugeben

Diese Vertraulichkeitsvereinbarung, die für die Dauer meiner Beschäftigung wirksam ist, bleibt nach Beendigung meiner Beschäftigung, gleich aus welchem Grund, unbegrenzt wirksam, soweit diese Vereinbarung die Nutzung und Offenlegung von personenbezogenen Daten oder vertraulichen Informationen betrifft.

Ich wurde darüber informiert, dass mir bei Verletzung dieser Verpflichtung disziplinarische und strafrechtliche Maßnahmen und Strafen gemäß den geltenden Rechtsvorschriften drohen.

(Ort) \_\_\_\_\_ den \_\_\_\_\_ in

\_\_\_\_\_ Exemplaren.

Name:

Unterschrift:

## ANHANG III



Schola Europaea

Büro des Generalsekretärs

Az.: 2021-10-D-74-de-1

Original: EN

### Leitlinien für die Vorgehensweise bei Personalabgängen

Anhang zu den Grundregeln für die Nutzung von IKT-Ressourcen durch Personalmitglieder der Europäischen Schulen und des BGS (2025-08-D-23)

## LEITLINIEN FÜR DIE VORGEHENSWEISE BEI PERSONALABGÄNGEN

### Inhalt

1. VERANTWORTLICHKEIT.....	24
2. ÜBERGABE DER ARBEIT .....	24
3. ÜBERGABE VON AUSRÜSTUNG .....	24
4. BERECHTIGUNGEN UND ZUGÄNGE .....	25

## LEITLINIEN FÜR DIE VORGEHENSWEISE BEI PERSONALABGÄNGEN

Das BGS und die Europäischen Schulen müssen ein Verfahren vorsehen, das zu befolgen ist, wenn ein Personalmitglied an ein/e andere/s [Referat/Schule] versetzt wird oder das/die [BGS/Schule] endgültig verlässt.

Mit einem solchen Verfahren soll eine Unterbrechung der Arbeit auf ein Mindestmaß reduziert und eine effiziente Übergabe aller Informationsinhalte gemäß den datenschutzrechtlichen Bestimmungen gewährleistet werden.

Ein solches Verfahren muss mindestens folgende Punkte abdecken:

### 1. VERANTWORTLICHKEIT

Das Übergabeverfahren ist in erster Linie von dem ausscheidenden Personalmitglied durchzuführen. Der/die [unmittelbare Vorgesetzte des ausscheidenden Personalmitglieds/Personalverantwortliche in der Schule] ist für die Einleitung und Überwachung des Übergabeverfahrens und dessen Durchführung im Sinne der Kontinuität des Dienstbetriebs des/der [BGS/Schule] verantwortlich.

### 2. ÜBERGABE DER ARBEIT

- Festlegung eines Plans und Zeitrahmens für die Übergabe der Informationen des/der [BGS/Schule] (z. B. Ordner, Dateien, Dokumente usw.)
- Übertragung von Aufgaben und Kenntnissen an den/die Nachfolger/in des ausscheidenden Personalmitglieds (z. B. alltägliche Aufgaben, offene Fragen, Zugang zu relevanten Informationen usw.)
- Übermittlung von Informationen, elektronisch und in Papierform (z. B. Checkliste der Dateien, Dokumente, Archive, Kopien relevanter E-Mails usw.), an den festgelegten Ort und an den/die [unmittelbare/n Vorgesetzte/n des ausscheidenden Personalmitglieds/Personalverantwortliche/n in der Schule]

Solche Informationen sollten an einem gemeinsamen Ablageort des Referats, der Abteilung und/oder Kolleg/inn/en (z. B. Server, Aktenschränke usw.) aufbewahrt werden.

### 3. ÜBERGABE VON AUSRÜSTUNG

Der/die [unmittelbare Vorgesetzte des ausscheidenden Personalmitglieds/Personalverantwortliche in der Schule] ist verantwortlich für:

- Aufstellung einer Liste aller Geräte und Gegenstände, die zurückzugeben/zu übergeben sind, und Festlegung einer Person, die für die Rückgabe der beruflichen Ausrüstung, Ausweise, Schlüssel sowie der beruflich genutzten Mobiltelefone des/der [BGS/Schule] zuständig ist
- Planung der Modalitäten für die Übergabe an die designierte/n Person/en und des festgelegten Zeitrahmens und Information des ausscheidenden Personalmitglieds darüber

#### 4. BERECHTIGUNGEN UND ZUGÄNGE

- Vor seinem Ausscheiden ist dem Personalmitglied zu gestatten:
  - i. Seine persönlichen Sachen abzuholen
  - ii. Seine private elektronische Kommunikation abzuholen oder zu löschen
  - iii. Dokumente zu vernichten, die für die Kontinuität des Dienstbetriebs des BGS/der Schule nicht mehr gebraucht werden
- Das Personalmitglied muss über die Deaktivierung seines Kontos und den Widerruf seiner gesamten Zugangsberechtigungen zu den Ressourcen des/der [BGS/Schule] am Tag der Beendigung seines Vertrags unterrichtet werden. Der Inhalt des Kontos des ausscheidenden Personalmitglieds wird nach Ablauf einer Speicherfrist von 30 Tagen, unbeschadet der Rechte gemäß Kapitel III der DSGVO, gelöscht.
- Die lokale IT-Abteilung oder das IKT-Referat des BGS/die IT und das ServiceDesk müssen durch den/die [unmittelbare/n Vorgesetzte/n / Personalverantwortliche/n im BGS/ in der Schule] über eine Service - [Anfrage an IOSG-ICT-SERVICEDESK@eursc.eu](mailto:IOSG-ICT-SERVICEDESK@eursc.eu) (für das BGS)/oder an [ES-ICT-SERVICEDESK@eursc.eu](mailto:ES-ICT-SERVICEDESK@eursc.eu) (für die Schulen)] ordnungsgemäß informiert werden, um die Deaktivierung aller Konten des ausscheidenden Personalmitglieds und die Löschung aller Inhalte dieser Konten nach einem Kalendermonat anzufordern.

## ANHANG IV



Schola Europaea

Büro des Generalsekretärs

Az.: 2021-12-D-09-de-1

Original: EN

### Leitlinien für die Nutzung von Social Media durch das Personal der Europäischen Schulen

Anhang zu den Grundregeln für die Nutzung von IKT-Ressourcen durch Personalmitglieder der Europäischen Schulen und des BGS (2025-08-D-23)

## LEITLINIEN FÜR DIE NUTZUNG VON SOCIAL MEDIA DURCH LEHRKRÄFTE

Diese Leitlinien sollen Lehrkräften helfen, Social Media im Unterricht mit ihren Schüler/innen in verantwortungsvoller, sicherer und zuverlässiger Weise zu nutzen, ohne den Ruf oder die Gemeinschaft der Schule zu schädigen.

### VORBEMERKUNGEN

Um die Einhaltung der Anforderungen der DSGVO und der geltenden nationalen Rechtsvorschriften zu gewährleisten, gestatten die Europäischen Schulen den Schüler/innen gemäß IT-Charta nicht, individuelle Social-Media-Konten mit ihren Schulkonten/Zugangsdaten zu erstellen.

Solche Plattformen bieten in Bezug auf Datenschutz keinerlei Garantie, da ihre Nutzungsbedingungen nicht durch den Direktor der Schule ausgehandelt werden können.

Dennoch kann die Schule unter den nachfolgend aufgeführten Bedingungen die Erstellung eines Kontos im Namen der Klasse gestatten.

#### 1. DEFINITION DER PÄDAGOGISCHEN ZWECKE

Die Lehrkraft muss die Schüler/innen zu einer sicheren und verantwortungsvollen Nutzung anleiten. Die pädagogischen Zwecke, die die Lehrkraft mit der Erstellung eines Social-Media-Kontos für die Klasse verfolgt, müssen im Vorfeld definiert werden.

Solche Ziele können sein:

- Erwerb von digitalen Kompetenzen
- Sensibilisierung für das Internet (*rechtliche Aspekte, Bildrechte, Verantwortungsbewusstsein, E-Reputation, Sensibilisierung für Gefahren und Chancen*)
- Vermittlung von Lerninhalt in schriftlichen und audiovisuellen Formen
- Förderung der Fähigkeit zu kritischem Denken

#### 2. ERSTELLEN EINES KONTOS

Die Lehrkraft ist für die Erstellung des Kontos verantwortlich und das Passwort darf den Schüler/innen nicht mitgeteilt werden.

Das Konto muss mit einer „temporären/Einweg-E-Mail-Adresse“ werden, die nur kurze Zeit genutzt wird und verworfen werden kann, sobald sie nicht mehr von Nutzen ist.

Mit anderen Worten, die „temporären/Einweg-E-Mail-Adresse“ ist eine E-Mail-Adresse, die speziell für die Erstellung des Social-Media-Kontos eingerichtet wird.

Solche E-Mail-Adressen sind zur Vermeidung von Sicherheitsbedrohungen für die Informationen der Lehrkräfte sowie der Schule erforderlich.

### **3. SOCIAL-MEDIA-GRUNDREGELN**

Die Lehrkraft stellt zusammen mit den Schüler/innen Grundregeln für die Nutzung von Social Media auf, um die Ziele des Projekts zu definieren und um für die Nutzung zu sensibilisieren.