Referat für Pädagogische Entwicklung
IKT- und Statistikreferat

Az.: 2025-08-D-25-de-1

Original: EN

GRUNDREGELN FÜR DIE NUTZUNG VON IT-RESSOURCEN UND GERÄTEN DURCH DIE SCHÜLER/INNEN DER EUROPÄISCHEN SCHULEN

Anlage zu MEMO 2025-08-M-1

Inhaltsverzeichnis

Schola Europaea

Büro des Generalsekretärs

Grundregeln für die Nutzung von IKT-Ressourcen und -Geräten durch Schüler/innen der Europäischen Schulen

PRÄAMBEL

Im Hinblick auf digitale, Multimedia- und IT-Dienste bemühen sich die Europäischen Schulen, den Schüler/innen die bestmöglichen Arbeitsbedingungen zu bieten. In diesen Grundregeln sind die Regeln für eine ordnungsgemäße Nutzung und Verhaltensregeln für IT-Ressourcen mit pädagogischer Bestimmung, die ihnen zur Verfügung gestellt werden, aufgeführt.

Diese Grundregeln stellen eine Anlage zur Hausordnung der Europäischen Schule (im Folgenden „die Schule“) dar und entsprechen den geltenden Gesetzen und Vorschriften vor allem in Bezug auf Urheberrecht, Rechte des geistigen Eigentums, Schutz der Privatsphäre (insbesondere Rechte an Bildern), die Verarbeitung personenbezogener Daten sowie Computerkriminalität.

1. IT-RESSOURCEN UND -GERÄTE

1.1 Definition

„IT-Ressourcen und -Geräte“ bezeichnet das Paket aus technischen Geräten und IKT-Diensten für die Schulen: *Netzwerk*, *Server und Arbeitsplätze, interaktive Whiteboards, periphere Geräte (Drucker, externe Festplatten usw.)*, *Laptops, Computer und Tablets*, *Software-Anwendungen, Zugangsdaten der Anwender/innen und die Nutzung von Internetdiensten an der Schule sowie digitale Lernressourcen*[1]*, die von der Schule zur Verfügung gestellt werden.*

1.2 Goldene Regel

Die IT-Ressourcen der Europäischen Schulen sind *ausschließlich* für pädagogische Aktivitäten vorgesehen.

1.3 Zugang zu IT-Ressourcen und -Geräten

Der Zugang zu den Ressourcen und Geräten, die durch die Schule zur Verfügung gestellt werden, ist ein Privileg und kein Recht.

Jeder Schüler und jede Schülerin muss die Betriebsbedingungen und die Regeln für eine ordnungsgemäße Nutzung und Verhaltensregeln in diesen Grundregeln strengstens einhalten.

Die Schule kann regelmäßige oder gelegentliche Kontrollen durchführen, um festzustellen, ob die IT-Ressourcen und -Geräte gemäß den Vorgaben dieser Grundregeln genutzt werden und behält sich das Recht vor, das Privileg zu widerrufen, wenn es notwendig erscheint.

An den Schulen wird der Zugang zu IKT-Ressourcen und -Geräten unter der Verantwortung der Schulleitung und unter der Kontrolle eines Mitglieds des pädagogischen Teams ermöglicht.

[1] Gemäß der Definition, die in dem Verfahren zur Genehmigung der Nutzung einer digitalen Lernressource an den Europäischen Schulen aufgeführt ist (Anlage zu MEMO 2019-12-M-3/GM).

Die Schule bietet Zugang zu verschiedenen IKT-Ressourcen:

- zu den Computern der Schule über ein persönliches Konto (Zugangsdaten werden zur Verfügung gestellt),
- zum Netzwerk der Schule, das Folgendes umfasst:
  - ☐ Speicherplatz auf den Servern der Schule: gemeinsam genutzte Bereiche oder auf das eigene persönliche Konto beschränkte Bereiche,
  - ☐ Netzwerk-Drucker,
- zu Microsoft-365 Online-Diensten (insbesondere ein E-Mail-/Messenger-Dienst), die von der Europäischen Schule verwaltet werden,
- zu schuleigener Software, lizenziert oder Open-Source,
- zum Internet,
- zum W-LAN der Schule auf privaten Geräten für Schüler/innen, die zu BYOD berechtigt sind.

Sämtliche Zugangs- und Anmeldedaten, die ein Schüler oder eine Schülerin erhält, sind persönlich und dürfen nur durch den betreffenden Schüler bzw. die betreffende Schülerin verwendet werden. Daher müssen Zugangscodes und Anmeldedaten streng vertraulich behandelt werden und dürfen dritten Parteien nicht offengelegt werden (mit Ausnahme der rechtlichen Vertreter/innen der Schüler/innen). Jedoch **ist es den rechtlichen Vertreter/innen der Schüler/innen strengstens untersagt, die den Schüler/innen zur Verfügung gestellten IKT-Ressourcen zu anderen Zwecken zu nutzen als der Unterstützung des Unterrichts und des Lernens der Schüler/innen** (wie zum Beispiel die Nutzung der MS-365-Office-Suite für private Zwecke und die Teilnahme an Sitzungen mit dem Konto des Schülers/der Schülerin).

Bevor sie ihren Arbeitsplatz verlassen, müssen die Schüler/innen sich immer vergewissern, dass sie sich ordnungsgemäß ausgeloggt haben.

Der Schüler oder die Schülerin informiert den/die pädagogische/n Berater/in, falls es ein Problem mit dem Konto gibt, oder ein Verlust, Diebstahl oder eine Kompromittierung der Zugangscodes erfolgt ist.

2. ALLGEMEINE VERHALTENSREGELN

2.1 Allgemeine Bemerkungen

Die Schüler/innen müssen die Verhaltensregeln einhalten, wenn sie die den Schulen für pädagogische Zwecke zur Verfügung gestellten Ressourcen und Geräte nutzen. Daher müssen diese Grundregeln auch eingehalten werden, wenn Schüler/innen, die ihr eigenes Mobilgerät an der Schule (d. h. Zugang zum Netzwerk) oder außerhalb der Schule verwenden, auf Ressourcen zugreifen.

Für die private Nutzung außerhalb der Schule erhalten alle Schüler/innen fünf Microsoft-365-Installationslizenzen für Computer und/oder Smartphones und Tablets. Diese Lizenzen können auf IT-Geräten genutzt und installiert werden, die die Schüler/innen regelmäßig nutzen und die passwortgeschützt sind, gemäß den allgemeinen Verhaltensregeln in diesen Grundregeln.

2.2 Wahrung der Vertraulichkeit

Den Schüler/innen ist Folgendes untersagt:

- zu versuchen, sich die Passwörter von anderen Personen anzueignen,
- sich mit den Benutzernamen und Passwörtern anderer Personen einzuloggen,
- die offene Sitzung eines anderen Anwenders ohne die ausdrückliche Erlaubnis zu nutzen,
- die Dateien von anderen Personen zu öffnen, offenzulegen/weiterzugeben, zu editieren, herunterzuladen oder zu löschen und allgemeiner zu versuchen, auf Informationen von anderen Personen ohne deren Erlaubnis zuzugreifen,
- Passwörter in Internet-Software wie Google Chrome, Internet Explorer, Firefox, etc. speichern, **wenn nicht-private Geräte verwendet werden**.

2.3 Sorgfältiger Umgang mit dem Netzwerk und den Arbeitsplätzen

Ein sorgfältiger Umgang mit den Räumlichkeiten und der Hardware ist an den Tag zu legen. Computertastaturen, Mäuse und Bildschirme müssen sorgfältig behandelt werden. Daher ist es den Schüler/innen nicht erlaubt zu essen und zu trinken, wenn sie die Arbeitsplätze an der Schule nutzen, damit diese nicht beschädigt werden. Die Schüler/innen dürfen nicht mit Absicht die Schließfächer die für das Laden von BYOD-Geräten gedacht sind, mit kostenlosen elektronischen Vorhängeschlössern blockieren.

Den Schüler/innen ist Folgendes untersagt:

- zu versuchen, die Konfiguration der Geräte (wie Laptops, Tabletts und Arbeitsplätze) zu verändern,
- zu versuchen, Netzwerk- oder Arbeitsplatz-Daten zu verändern oder zu zerstören,
- Software zu installieren oder Software im Netzwerk zu kopieren,
- auf andere Ressourcen als die von der Schule zugelassenen zuzugreifen oder versuchen zuzugreifen,
- Nachrichten, Dateien, Dokumente, Links, Bilder von unbekannten Absendern zu öffnen,
- einen Wechseldatenträger in ein beliebiges Gerät ohne die Erlaubnis eines verantwortlichen Erwachsenen einzulegen,
- ein Speichergerät oder -medium zu verbinden (USB-Stick, Mobiltelefon usw.) ohne die Erlaubnis eines verantwortlichen Erwachsenen,
- den Netzbetrieb absichtlich zu stören, insbesondere durch die Verwendung von Programmen, die dazu bestimmt sind, schädliche Programme einzuschleusen oder Sicherheitsvorkehrungen zu umgehen (Viren, Spyware oder andere),
- die installierten Schutzsysteme zu umgehen oder versuchen zu umgehen (Firewall, Antivirenprogramme usw.),
- VPN-Tunnel[2]zunutzen.

2.4 Einhaltung der Rechte des geistigen Eigentums

Den Schüler/innen ist Folgendes untersagt:

- Material herunterzuladen oder illegal zu kopieren (Streaming, Audiomaterial, Filme, Software, Spiele usw.), die durch Rechte des geistigen Eigentums geschützt sind, es sei denn, solches Material wird im Rahmen einer Lizenz zur Verfügung gestellt (wie zum Beispiel Creative Commons), die eine solche Nutzung zulässt,

- Inhalte, die durch Rechte des geistigen Eigentums geschützt sind (wie zum Beispiel das Urheberrecht), zu kopieren, d. h. zu reproduzieren, (weiter)zuverbreiten oder an die Öffentlichkeit weiterzugeben in jeglicher Form und unabhängig vom Medium (zum Beispiel Tabellen, Grafiken, Gleichungen, Rechtstexte, Bilder, schriftliche Texte). Sie müssen ebenfalls angemessene Quellenangaben einfügen, wenn sie sich auf Hypothesen, Theorien oder Meinungen von anderen Personen beziehen.
- Die Nutzung von im Internet gefundener Informationen für Klassenarbeiten bedeutet auch, dass die Quellen genannt und von den Schüler/innen korrekt angegeben werden müssen. Die Schüler/innen können sich von den Mitgliedern des pädagogischen Teams in dieser Hinsicht helfen lassen.

[2] Im Bereich IT ist ein **Virtual Private Network, abgekürzt VPN** , ein System, durch das eine direkte Verbindung zwischen Computern im Fernzugriff erstellt werden kann, indem dieser Datenverkehr in einer Art Tunnel isoliert wird.

2.5 Respektvoller Umgang mit den Mitgliedern der Schulgemeinschaft und der Schule

Von allen Schüler/innen wird erwartet, dass sie digitale Werkzeuge so nutzen, dass die Würde, das Wohlbefinden und die Rechte von allen Mitgliedern der Schulgemeinschaft gewahrt bleiben.

Den Schüler/innen ist Folgendes untersagt:

- Anzeige auf dem Bildschirm, Veröffentlichung von Dokumenten oder Teilnahme an diffamierendem, beleidigendem, extremistischem, pornografischem oder diskriminierendem Austausch, sei es aufgrund der Rasse oder ethnischen Herkunft, der politischen Meinungen, der Religion oder Weltanschauung, des Gesundheitszustands oder der sexuellen Orientierung.
- Mobbing anderer Personen (Cybermobbing[3]), sowohl in eigenem Namen als auch bei der Nutzung einer falschen Identität oder eines Pseudonyms. Die Schüler/innen werden dazu aufgefordert, jeglichen Vorfall von Cybermobbing einem vertrauenswürdigen Erwachsenen oder einem Personalmitglied zu melden, die Schule wird alle beteiligten Parteien unterstützten und dabei, soweit möglich, einen versöhnlichen und pädagogischen Ansatz wählen.
- Verwendung der Adresslisten aus den E-Mail-Konten oder personenbezogener Daten anderer Personen für andere Zwecke als die der pädagogischen oder didaktischen Ziele und nicht gemäß den Vorgaben des Datenschutzes.
- Unangemessene Sprache in E-Mails, Posts, Chats oder anderen Kommunikationsmitteln (der Autor der Nachricht hat die alleinige Verantwortung für den versendeten Inhalt).
- Schädigung des Rufs eines Mitglieds der Schulgemeinschaft oder der Schule durch die Verbreitung von Texten, Bildern und/oder Videos.
- Vertragsabschlüsse, Verkäufe und Werbung im Namen der Schule, egal auf welche Art und Weise, es sei denn, das Projekt wurde vorab durch die Schulleitung genehmigt.

3. BESONDERE REGELN FÜR DIE INTERNETNUTZUNG

3.1 Nutzung des Netzwerks der Schule

Der Zugang zum Internet an den Europäischen Schulen ist ein Privileg, kein Recht.
Die Nutzung des pädagogischen internetbasierten Netzwerks ist für den alleinigen Zweck der Unterrichts- und Lernaktivitäten gemäß der Mission der Europäischen Schulen gedacht.

Den Schüler/innen ist Folgendes strengstens untersagt:

- sich mit Live-Chat-Diensten oder Diskussionsforen zu verbinden, es sei denn, es liegt eine anderweitige Genehmigung durch das pädagogische Team aufgrund des pädagogischen Zwecks vor, oder sich mit Social Media zu verbinden,
- personenbezogene Informationen weiterzugeben, die zur Identifizierung einer Person führen könnten (Vorname, Nachname, E-Mail, Adresse usw.),
- auf Websites mit pornographischen Inhalten oder Materialien zugreifen, die Hass, Diskriminierung oder Gewalt aufgrund von Rasse, ethnischer Herkunft, Religion, sexueller Orientierung oder anderer persönlicher Eigenschaften fördern, jedwede Softwareprogramme oder Anwendungen herunterzuladen und zu installieren.

[3] Cybermobbing umfasst die wiederholte oder beabsichtigte Belästigung, Bedrohung, Ausschließung oder Demütigung von anderen durch digitale Mittel, wie zum Beispiel Nachrichten, soziale Medien, Bilder oder Videos.

Unter keinen Umständen sollten Schüler/innen ihren Namen angeben, Fotos anzeigen, ihre Adresse, Telefonnummer oder irgendeine andere Information angeben, die ihre Identifikation im Internet erleichtert, und/oder die personenbezogene Daten einer anderen Person.

Es ist den Schüler/innen strengstens untersagt, die mit ihrem MS-365-Konto (…@student.eursc.eu) verbundene E-Mail-Adresse zu nutzen, um bei Anwendungen, Websites oder Softwareprogrammen Konten zu erstellen, die nicht durch ein Mitglied des pädagogischen Teams oder die Schulleitung genehmigt sind.

3.2 Supervision und Hilfe während der Sitzungen für Schüler/innen an der Schule

Die Schule wird ein Supervisions- und Hilfesystem nutzen, um das Schülerengagement in einem kontinuierlichen Lernprozess zu unterstützen und es den fraglichen kursverantwortlichen Personen und dem Bibliothekspersonal zu ermöglichen, den Schüler/innen direkt von ihren Arbeitsplätzen zu helfen.

Nur von der Schulleitung autorisierte Personen dürfen die Supervisions- und Hilfssoftware nutzen, und sie müssen die IT-Grundregeln einhalten, die für ihre Rolle an der Schule gelten.

Dieses System ermöglicht Folgendes:

- auf die Bildschirme der Schüler/innen aus der Ferne zuzugreifen, um ihnen zu helfen, und damit sie sich auf ihre Aufgaben konzentrieren können,
- den Unterricht effektiver zu gestalten, indem der Bildschirm der für die Stunde verantwortlichen Person für die Klasse angezeigt wird,
- die Bildschirme von Schüler/innen auszuwählen, um ihre Arbeit vorzustellen,
- alle Bildschirme von Schüler/innen zu deaktivieren, um ihre Aufmerksamkeit zu erhalten.

Es werden keine Aufnahmen ihrer Sitzungen oder Aktivitäten gemacht.

3.3 Social Media

Es ist den Schüler/innen untersagt, sich mit der E-Mail-Adresse ihres MS-365-Kontos (…@student.eursc.eu) mit Social Media zu verbinden. **Es ist strengstens verboten, das Passwort für das MS-365-Konto bei anderen Systemen, Websites und Anwendungen zu verwenden**.

Die Verwendung privater digitaler Geräte (Telefon, Tablet, Laptop) entbindet die Schüler/innen nicht von der Verpflichtung, die in den vorliegenden Grundregeln verankerten Regeln für eine ordnungsgemäße Nutzung und Verhaltensregeln im Hinblick auf Respekt gegenüber den Mitgliedern der Schulgemeinschaft einzuhalten. Die Schüler/innen bleiben verantwortlich für den angezeigten Inhalt.

3.4 Künstliche Intelligenz

Künstliche Intelligenz (KI) bezieht sich auf die Fähigkeit von Rechnersystemen, Aufgaben durchzuführen, die typischerweise mit menschlicher Intelligenz assoziiert werden, wie zum Beispiel lernen, abwägen, Probleme lösen, wahrnehmen und Entscheidungen treffen. Generative KI kann Inhalte auf Grundlage von Eingaben der Anwender/innen verarbeiten (Analyse, Transformation oder Erhebung), im Allgemeinen durch eine Konversation.

- Die Schüler/innen können auf webbasierte KI-Tools mit ihrer schulverbundenen E-Mail-Adresse (…@student.eursc.eu) nur dann zugreifen, wenn dies ausdrücklich von der Schule genehmigt wurde.
- Wenn KI außerhalb der Schule für Hausaufgaben oder Projekte genutzt wird, müssen die Schüler/innen ehrlich und transparent bleiben, gemäß der Richtlinie der Schule oder den kursspezifischen Leitlinien.
- Die Schüler/innen müssen KI-Tools verantwortlich und gesetzeskonform nutzen, indem sie Privatsphäre und Vertraulichkeit schützen, geistiges Eigentum respektieren und für jegliche KI generierten Inhalte, die sie nutzen, Verantwortung übernehmen und solche Tools durchdacht einsetzen aufgrund ihrer Auswirkungen auf das Umfeld.

4. SONDERREGELN ZUM ONLINE-LERNEN/-UNTERRICHT

Online-Lernen oder -Unterricht erfordert die Einhaltung der Regeln für eine ordnungsgemäße Nutzung und Verhaltensregeln, die in diesen Grundregeln erläutert sind, in den folgenden Kontexten:

- Blended Learning (Integriertes Lernen): Online-Lernen oder -Unterricht an der Schule, wobei digitale, von der Schulleitung genehmigte Ressourcen verwendet werden, oder die Durchführung von asynchronen Aktivitäten (beispielsweise Hausaufgaben);
- Fernunterricht: wenn Online-Unterricht bei Schulschließungen stattfindet;
- Hybrides Lernen: wenn einige Schüler/innen vor Ort am Unterricht und andere online teilnehmen.

Folgendes ist untersagt:

- Foto- oder Filmaufnahmen von Lehrkräften oder Schüler/innen, die an Onlinekursen teilnehmen, mit privaten Geräten und insbesondere die Veröffentlichung solcher Bilder oder Videos,
- Teilnahme an Online-Lernen oder -Unterrichtsstunden ohne ausdrücklich zur Teilnahme eingeladen worden zu sein,
- Einladungen zu Online-Lernen oder -Unterrichtsstunden ohne die Zustimmung des Organisators/der Organisatorin der Sitzung,
- Einsatz von digitalen Lernressourcen, um andere einzuschüchtern, zu mobben, zu diffamieren oder zu bedrohen.

Das Recht, die Verwendung des eigenen Bildes zu kontrollieren, wird allen Mitgliedern der Schulgemeinschaft zuerkannt. Aus diesem Grund toleriert die Schule die Nutzung von Bildern oder Videos nicht, die ohne das Wissen oder die Zustimmung der betroffenen Personen erstellt wurden.

5. MELDUNG AN DAS PÄDAGOGISCHE/IKT-TEAM

Die Schüler/innen verpflichten sich, einem Mitglied des pädagogischen Teams oder des IT-Teams (pädagogische/r Berater/in, IT-Koordinator/in, Lehrkraft usw.) so schnell wie möglich Folgendes zu melden:

- verdächtige Software oder verdächtige Geräte,
- Verlust, Diebstahl oder Kompromittierung der Authentifizierungsinformation,
- Nachrichten, Dateien, Dokumente, Links und Bilder, die von einem unbekannten Absender verschickt wurden.

6. VERANTWORTLICHKEIT

Vorsätzliche Beschädigung der Geräte und IT-Ressourcen der Schule kann zu Reparaturkosten für die gesetzlichen Vertreter/innen der betroffenen Schüler/innen führen, gemäß Art. 32 der Allgemeinen Schulordnung der Europäischen Schulen (2014-03-D-14).

Alle Schüler/innen, die ein Mobiltelefon oder ein anderes digitales Gerät zur Schule mitbringen, tun dies auf ihr eigenes Risiko und sind persönlich verantwortlich für die Sicherheit ihres Mobiltelefons oder Geräts.

Unbeschadet der Ausnahmen, wenn Schüler/innen ein Gerät für die Zwecke eines BYOD-Programmes mit in die Schule bringen müssen, übernimmt die Schule keinerlei Haftung irgendeiner Art für Verlust, Diebstahl, Beschädigung eines Telefons oder irgendeines anderen Geräts oder Vandalismus noch für die unautorisierte Nutzung eines solchen Geräts.

7. VORGESEHENE SANKTIONEN

Alle Schüler/innen, die gegen die oben aufgeführten Regeln verstoßen, unterliegen Disziplinarmaßnahmen gemäß der Allgemeinen Schulordnung der Europäischen Schulen und der Hausordnung der Schule sowie den gesetzlich vorgesehenen Strafen und Strafverfahren.

Alle Mitglieder des pädagogischen Teams müssen sich verpflichten zu gewährleisten, dass diese Vorgaben von den Schüler/innen eingehalten werden, die ihrer Verantwortung unterliegen, und sie müssen rigorose Kontrollen in dieser Hinsicht durchführen.

Der/die IT-Administrator/in muss durchgängig zu seiner/ihrer Zufriedenheit gewährleisten, dass die IT-Ressourcen ordnungsgemäß funktionieren und ordnungsgemäß genutzt werden. Zu diesem Zweck können Anomalien (anomale Nutzung des Netzwerks, übermäßiger Speicherplatz, versuchte Cyberattacken usw.) durch die Überwachung von IT-Ressourcen festgestellt werden. Sollten Anomalien festgestellt werden, muss sich der/die IT-Administrator/in mit der Schulleitung in Verbindung setzen, um sich auf die durchzuführenden Maßnahmen zu einigen. In Fällen eines absoluten Notfalls und zum Schutz der IT-Systeme der Schule darf der/die IT-Administrator/in sofortige Entscheidungen treffen, um den IT-Zugang für einen oder mehrere Schüler/innen zu blockieren. Er/sie wird im Anschluss die Angelegenheit unmittelbar an die Schulleitung weiterleiten.

Diese Art von Interventionen können nur zur klar definierten Zwecken erfolgen, nämlich:

- Vermeidung von illegalen oder diffamierenden Aktionen und von Aktionen, die den akzeptierten Standard des allgemeinen Verhaltens zuwiderlaufen oder die Würde anderer Menschen verletzen könnten.
- Schutz der wirtschaftlichen und finanziellen Interessen des Schule, die vertraulich sind,
- Sicherheit und/oder reibungsloser technischer Betrieb der IT-Systeme, einschließlich Kontrolle der damit verbundenen Kosten, und physischer Schutz der Einrichtungen der Schule.
- Gutgläubige Einhaltung der Prinzipien und Regeln für die Nutzung der verfügbaren Technologien und dieser Grundregeln.

8. ÜBERPRÜFUNG

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