ICT-Charta

für den Gebrauch von IT-Ressourcen und -Geräten durch Schüler/innen der Europäischen Schule München

Version vom 23.09.2025

Inhalt

1. PRÄAMBEL 2
2. IT-RESSOURCEN UND -GERÄTE 2
   2.1 Definition 2
   2.2 Goldene Regel 2
   2.3 Zugang zu IT-Ressourcen und -Geräten 2
3. ALLGEMEINE VERHALTENSREGELN 4
   3.1 Allgemeine Bemerkungen 4
   3.2 Respekt vor Vertraulichkeit 4
   3.3 Respekt vor dem Netzwerk und vor Arbeitsplätzen 4
   3.4 Respekt vor Rechten an geistigem Eigentum 5
   3.5 Respekt vor den Mitgliedern der Schulgemeinschaft und der Schule 5
4. BESONDERE REGELN FÜR DIE NUTZUNG DES INTERNETS 6
   4.1 Das Netzwerk der Schule 6
   4.2 Beaufsichtigung und Hilfe bei der Sitzung für Schüler/innen in der Schule 7
   4.3 Social Media 7
   4.4 Nutzung von künstlicher Intelligenz (KI) 7
5. BESONDERE REGELN FÜR ONLINE-LERNEN/-UNTERRICHT 8
6. MELDUNGEN AN DAS PÄDAGOGISCHE/IT-TEAM 8
7. VERANTWORTUNG 9
8. VORGESEHENE SANKTIONEN 9
9. ÜBERARBEITUNG 10

1. PRÄAMBEL

Die Europäischen Schulen streben danach, ihren Schüler/innen in Bezug auf IT- und Multimedia-Dienste adäquate Arbeitsbedingungen zu bieten. Diese Charta legt die Regeln für die ordnungsgemäße Nutzung und richtiges Verhalten gegenüber den IT-Ressourcen mit pädagogischem Zweck fest, die ihnen zur Verfügung gestellt werden.

Diese Charta ist ein Anhang zur Hausordnung der Europäischen Schule München (nachstehend als „die Schule“ bezeichnet) und fügt sich in den Rahmen der Gesetze und Vorschriften ein, die sich insbesondere auf Urheberrecht, Rechte an geistigem Eigentum, Datenschutz (einschließlich insbesondere von Bildrechten) und die Verarbeitung von personenbezogenen Daten sowie Computerkriminalität beziehen.

2. IT-RESSOURCEN UND -GERÄTE

2.1 Definition

„IT-Ressourcen und -Geräte“ bezeichnet das Paket, welches Netzwerk, Server und Arbeitsplätze, interaktive Whiteboards, Peripheriegeräte (Drucker, externe Festplatten, Kameras), Software, Laptops und Tablets der Schule, den Internetgebrauch an der Schule und durch diese bereitgestellten digitalen Lernmittel[1] umfasst. Ferner sind damit auch das Schulnetzwerk und jene Geräte gemeint, bei denen man den Interzugang über dieses durch die Eingabe von Benutzeranmeldedaten herstellt, insbesondere die schülereigenen Geräte im Rahmen des Programms „Bring Your Own Device“. Diese Geräte selbst sind zwar im privaten Besitz der Familien, allerdings geht die Nutzung derer mit Pflichten einher, sobald sie sich mit der Infrastruktur der Schule verbinden.

2.2 Goldene Regel

Die IT-Ressourcen der Europäischen Schule sind *ausschließlich* für pädagogische Aktivitäten bestimmt.

2.3 Zugang zu IT-Ressourcen und -Geräten

Der Zugang zu den durch die Schule bereitgestellten Ressourcen, den Geräten und der Infrastruktur ist ein Privileg, kein Recht.

Jede/r einzelne Schüler/in muss die Betriebsbedingungen und die Regeln für die ordnungsgemäße Nutzung und das richtige Verhalten, die in dieser Charta beschrieben sind, gewissenhaft einhalten.

[1] Gemäß der Definition aus dem Verfahren zur Genehmigung des Einsatzes eines digitalen Lernmittels an den Europäischen Schulen (Anhang zu MEMO 2019-12-M-3/GM).

Die Schule kann regelmäßig oder fallweise überprüfen, ob die IT-Ressourcen und -Geräte übereinstimmend mit den Bestimmungen dieser Charta genutzt werden, und behält sich das Recht vor, dieses Privileg gegebenenfalls zu widerrufen.

An der Schule wird der Zugang zu IT-Ressourcen und -Geräten unter der Verantwortung der Schulleitung und unter der Kontrolle eines Mitglieds des pädagogischen Teams bereitgestellt.

Die Schule bietet Zugang zu verschiedenen IT-Ressourcen:

- zu den Computern der Schule über einen persönlichen Account,
- zu den Geräten der Schule, z.B. Lautsprechern, Kopfhörern, Kameras und anderen für den Lehrplan notwendigen Hardware-Geräten,
- zum Netzwerk der Schule, welches den Speicherplatz auf den Servern der Schule (geteilter Platz oder auf den persönlichen Account beschränkter Platz) und die Netzwerkdrucker (inklusive 3D-Drucker) umfasst,
- zu den Office-365-Onlinediensten (einschließlich insbesondere von E-Mail-/Messaging-Dienst), die durch die Europäische Schule verwaltet werden,
- zu eigener Software, unter Lizenz oder Open-Source,
- zum Schulnetzwerk insbesondere für die BYOD-Geräte und damit auch zum Internet.

Alle Zugangsdaten, die dem/der Schüler/in zur Verfügung gestellt werden, sind personengebunden und dürfen nur durch den/die betroffene/n Schüler/in genutzt werden. Die Zugangscodes müssen daher absolut vertraulich sein und dürfen Dritten nicht mitgeteilt werden (ausgenommen den gesetzlichen Vertreter/innen des Schülers bzw. der Schülerin). Bevor der/die Schüler/in seinen/ihren Arbeitsplatz verlässt, muss er/sie sich stets vergewissern, dass er/sie sich ordnungsgemäß abgemeldet hat.

Bei einem Problem mit seinem/ihrem Account oder bei Verlust, Diebstahl oder Gefährdung seiner/ihrer Zugangscodes wird der/die Schüler/in seine/n bzw. ihre/n Erziehungsberater/in informieren.

Ferner ist die Nutzung der gesamten digitalen Infrastruktur der Schule, und das betrifft ausdrücklich auch die BYOD-Geräte, nur unter der Bedingung möglich, dass der/die Schüler/in die IT-Ressourcen und -Geräte ausschließlich für Schul- und Unterrichtsrelevantes verwendet. Jeglicher Gebrauch für andere Zwecke ist in der gesamten Infrastruktur der Schule nicht gestattet.

3. ALLGEMEINE VERHALTENSREGELN

3.1 Allgemeine Bemerkungen

Die Schüler/innen müssen die Regeln für richtiges Verhalten einhalten, wenn sie die Ressourcen und Geräte nutzen, die die Schule für pädagogische Zwecke zur Verfügung stellt. Wenn somit ein/e Schüler/in mit seinem/ihrem eigenen mobilen Gerät an der Schule, z.B. im Zuge des BYOD Projektes, oder außerhalb der Schule auf auf das Netzwerk der Schule zugreift, muss diese Charta eingehalten werden.

Für die persönliche Nutzung außerhalb der Schule erhält jede/r Schüler/in fünf Office-365-Installationslizenzen. Diese Lizenzen können auf IT-Geräten installiert und genutzt werden, die regelmäßig durch den/die Schüler/in benutzt werden. Um sicherzustellen, dass gemäß den in dieser Charta unter Punkt 3.2. beschriebenen allgemeinen Regeln für richtiges Verhalten die Zugangskennungen und Account-informationen Dritten nicht zugänglich werden, muss das Endgerät passwortgeschützt sein.

Besonders zu beachten ist: Es ist grundsätzlich untersagt, einen ICT-Raum zu betreten und bereitgestellte IT-Geräte zu benutzen, wenn keine Aufsicht durch eine verantwortliche Person angeboten wird.

3.2 Respekt vor Vertraulichkeit

Es ist den Schüler/innen verboten:

- zu versuchen, sich die Passwörter anderer Personen anzueignen,
- sich mit Benutzernamen und Passwörtern anderer Personen anzumelden,
- die offene Sitzung eines anderen Nutzers ohne dessen ausdrückliche Erlaubnis zu nutzen,
- Dateien anderer Personen zu öffnen, zu bearbeiten oder zu löschen und allgemein zu versuchen, ohne deren Erlaubnis auf deren Informationen zuzugreifen,
- ein Passwort in Internet-Software wie etwa einem Browser zu speichern, wenn sie Geräte verwenden, die nicht im persönlichen Besitz sind.

3.3 Respekt vor dem Netzwerk und vor Arbeitsplätzen

Im Sinne des gegenseitigen Respekts und der Achtung des Schuleigentums müssen die Räume, die Geräte und die Infrastruktur mit Sorgfalt behandelt werden. Deshalb dürfen die Schüler/innen nicht essen und trinken, wenn sie das Bereitgestellte benutzen.

Kopfhörer sollen nach Gebrauch ordentlich aufgeräumt werden. Die Bildschirme sollen nicht manuell ausgeschaltet werden. Diese werden systemgesteuert nach fünfzehn Minuten Inaktivität abgeschaltet, um den Stromverbrauch zu reduzieren und somit die Umwelt zu schonen.

Es ist den Schüler/innen verboten:

- zu versuchen, die Konfiguration des Arbeitsplatzes zu ändern,
- zu versuchen, Daten von Netzwerk oder Arbeitsplatz zu ändern oder zu zerstören,
- Software zu installieren oder im Netzwerk vorhandene Software zu kopieren,
- auf andere als die durch die Schule zugelassenen Ressourcen zuzugreifen oder zuzugreifen zu versuchen,
- Nachrichten, Dateien, Dokumente, Links, Bilder von unbekannten Absendern zu öffnen,
- ohne die Erlaubnis eines/einer verantwortlichen Erwachsenen ein Speichergerät oder -medium (USB, Mobiltelefon oder Ähnliches) anzuschließen,
- absichtlich in den Betrieb des Netzwerks einzugreifen, insbesondere durch die Verwendung von Programmen, die entworfen wurden, um schädliche Programme einzuspielen oder Sicherheitsmaßnahmen zu umgehen (Viren, Spyware oder Ähnliches),
- VPN[2]-Tunnel zu verwenden oder den Netzwerkverkehr über ein Proxy-Server weiterzuleiten,
- anderen Schüler/innen die eigenen Nutzerdaten für das Netzwerk weiterzugeben, damit diese ihre Geräte unter falschem Namen anmelden können. Das führt zur Sperre des Accounts.

3.4 Respekt vor Rechten an geistigem Eigentum

Es ist den Schüler/innen verboten:

- Materialien, die durch Rechte an geistigem Eigentum geschützt sind, herunterzuladen oder illegale Kopien davon zu machen (Streaming, Audio, Filme, Software, Spiele usw.),
- Informationen, ungeachtet des Mediums (Tabelle, Grafik, Artikel eines Rechtsakts, Bild, Text, Hypothese, Theorie, Stellungnahme usw.), die durch Rechte an geistigem Eigentum (etwa Urheberrecht) geschützt sein könnten, zu plagiieren, d. h. in gleich welcher Form zu reproduzieren, zu verbreiten oder der Öffentlichkeit mitzuteilen.

Die Verwendung von im Internet gefundenen Informationen für Klassenaufgaben impliziert, dass die Quellen aufgenommen und durch den/die Schüler/in korrekt zitiert werden müssen. Er/Sie kann in dieser Hinsicht die Hilfe eines der Mitglieder des pädagogischen Teams suchen.

3.5 Respekt vor den Mitgliedern der Schulgemeinschaft und der Schule

Es ist den Schüler/innen verboten:

- Dokumente oder Webseiten diffamierender, missbräuchlicher, extremistischer, pornografischer, menschenverachtender oder diskriminierender Art – basierend auf ethnischer Herkunft, politischen Meinungen, Religion oder weltanschaulichen Überzeugungen, Gesundheitszustand oder sexueller Ausrichtung – am Schirm anzuzeigen, zu veröffentlichen oder an deren Austausch teilzunehmen;

[2] In der EDV ist ein **Virtual Private Network**, kurz **VPN**, ein System, das es ermöglicht, eine direkte Verbindung zwischen voneinander entfernten Computern herzustellen, indem dieser Verkehr in einer Art von Tunnel isoliert wird.

- andere Personen in ihrem eigenen Namen oder unter Verwendung einer falschen Identität oder eines Pseudonyms zu mobben (Cybermobbing);
- Listen von E-Mail-Adressen oder personenbezogenen Daten anderer Personen für andere Zwecke als jene zu verwenden, die durch pädagogische oder didaktische Ziele beabsichtigt sind;
- in E-Mails, Posts, Chats oder gleich welchen anderen Kommunikationsmitteln unangepasste Sprache zu verwenden (der/die Verfasser/in ist allein für den gesendeten Inhalt verantwortlich);
- den Ruf eines Mitglieds der Schulgemeinschaft oder der Schule zu schädigen, insbesondere durch die Verbreitung von Texten, Bildern und/oder Videos;
- Verträge abzuschließen, die im Namen der Schule etwas verkaufen oder bewerben, es sei denn, das Projekt wurde vorab durch die Schulleitung genehmigt.

4. BESONDERE REGELN FÜR DIE NUTZUNG DES INTERNETS

4.1 Das Netzwerk der Schule

Zugang zum Internet innerhalb der Europäischen Schule ist ein Privileg, kein Recht. Die Nutzung des pädagogischen internetgestützten Netzwerks ist nur zum Zweck von Unterrichts- und Lernaktivitäten bestimmt, die dem Auftrag der Europäischen Schulen entsprechen.

Es ist den Schüler/innen verboten:

- persönliche Angaben zu teilen, mit denen der/die Schüler/in identifiziert werden kann (Vorname, Nachname(n), E-Mail, Adresse usw.),
- zu versuchen, auf pornografische, menschenverachtende, fremdenfeindliche, antisemitische, rassistische oder sonstige jugendgefährdende Webseiten zuzugreifen.
- gleich welches Programm bzw. welche Software herunterzuladen oder zu installieren, sofern nicht anders mit dem Lehrer oder der Lehrerin zu einem bestimmten Zweck vereinbart.

Unter keinen Umständen sollten die Schüler/innen ihren Namen angeben, ein Foto zeigen, ihre Adresse, Telefonnummer oder irgendeine andere Information angeben, über die sie im Internet identifiziert werden könnten.

Es ist den Schüler/innen verboten, die mit ihrem O365-Account (…@student.eursc.eu) verbundene E-Mail-Adresse zu verwenden, um Accounts auf Applikationen, Websites oder Software anzulegen, die nicht durch ein Mitglied des pädagogischen Teams oder durch die Schulleitung zugelassen sind.

4.2 Beaufsichtigung und Hilfe bei der Sitzung für Schüler/innen in der Schule

Die Schule kann ein Beaufsichtigungs- und Unterstützungssystem einsetzen, um dafür zu sorgen, dass sich die Schüler/innen in einem kontinuierlichen Lernprozess befinden, und um den für den jeweiligen Kurs zuständigen Personen und dem Personal der Bibliothek die Möglichkeit zu bieten, Schüler/innen direkt von ihrem Arbeitsplatz aus zu helfen.

Nur durch die Schulleitung autorisierte Personen können die Beaufsichtigungs- und Unterstützungssoftware nutzen und sie müssen dabei die für ihre Rolle an der Schule geltende IT-Charta einhalten.

Dieses System bietet die Möglichkeit:

- auf Abstand auf die Bildschirme der Schüler/innen zuzugreifen, um ihnen zu helfen und um die Konzentration auf ihre Aufgaben sicherzustellen,
- Bildschirme von Schüler/innen auszuwählen, um ihre Arbeit zu präsentieren,
- die Bildschirme aller Schüler/innen zu deaktivieren, um ihre Aufmerksamkeit zu gewährleisten.

4.3 Social Media

Es ist den Schüler/innen verboten, sich mit der mit ihrem O365-Account verbundenen E-Mail-Adresse (…@student.eursc.eu) auf Social Media (etwa Facebook, Instagram) anzumelden.

Die Nutzung eines privaten digitalen Geräts (Telefon, Tablet, Laptop) befreit die Schüler/innen nicht davon, die Regeln für deren ordnungsgemäße Nutzung und richtiges Verhalten in Bezug auf Respekt vor Mitgliedern der Schulgemeinschaft und der Schule, wie beschrieben in dieser Charta, einzuhalten. Die Schüler/innen bleiben für den gezeigten Inhalt verantwortlich.

4.4 Nutzung von künstlicher Intelligenz (KI)

Den Schüler/innen ist es erlaubt, von der Schule datenschutzrechtlich geprüfte und freigegebene KI-Werkzeuge nach Autorisierung durch die Lehrkraft für die aktuelle Aufgabe oder Unterrichtssequenz zu verwenden. Es sollte dabei dennoch beachtet werden, dass keine persönlichen Daten oder die Daten Dritter an die KI übermittelt werden. Die erlaubten Werkzeuge gibt die Schule vor.

Wenn Schüler/innen KI, nach Erlaubnis der Lehrkraft, für Hausaufgaben, Arbeitsaufträge oder Projekte nutzen, dann müssen sie ehrlich und transparent sein und dies angeben. Außerdem muss die Nutzung von KI mit dem Respekt gegenüber Privatsphäre, geistigem Eigentum und dem ökologischen Fußabdruck einhergehen.

Eine detaillierte Nutzungsregelung ist durch die „Regelung zur Nutzung von Künstlicher Intelligenz“ festgelegt, die ebenfalls auf der Homepage der Schule zu finden ist.

5. BESONDERE REGELN FÜR ONLINE-LERNEN/-UNTERRICHT

Online-Lernen oder -Unterricht impliziert die Einhaltung der Regeln für ordnungsgemäße Nutzung und richtiges Verhalten, wie vorgeschrieben durch diese Charta, ob im Rahmen von:

- Online-Lernen oder -Unterricht an der Schule („Blended Learning“), was den Einsatz von durch die Schulleitung genehmigten digitalen Lernmitteln impliziert, oder die Ausführung von asynchronen Online-Aktivitäten (Hausaufgaben),
- Online-Lernen oder -Unterricht auf Abstand („Fernunterricht“), wenn der Unterricht an der Schule ausgesetzt ist,
- Online-Lernen oder -Unterricht auf Abstand und *in situ* („Hybrid Learning“), wenn die Stunden durch einige Schüler/innen vor Ort und durch andere auf Abstand absolviert werden.

Darüber hinaus ist Folgendes verboten:

- die Lehrkraft bzw. Lehrkräfte und die Schüler/innen, die am Online-Lernen teilnehmen, zu fotografieren und/oder zu filmen und, *a fortiori*, solche Bilder/Videos zu veröffentlichen,
- an Online-Lern- oder -Unterrichtssitzungen teilzunehmen, zu denen der/die Schüler/in nicht ausdrücklich eingeladen wurde,
- Teilnehmer/innen zu Online-Lern- oder -Unterrichtssitzungen ohne Zustimmung der Person einzuladen, die die Sitzung organisiert,
- digitale Lernmittel zu verwenden, um andere Personen einzuschüchtern, zu beleidigen, zu diffamieren, zu mobben oder zu bedrohen.

Bildrechte sind anerkannte Rechte für jedes Mitglied der Schulgemeinschaft, weshalb die Schule die Nutzung von Bildern/Videos, die ohne Mitwissen der betroffenen Personen aufgenommen wurden, nicht tolerieren wird.

6. MELDUNGEN AN DAS PÄDAGOGISCHE/IT-TEAM

Der/Die Schüler/in verpflichtet sich, einem Mitglied des pädagogischen oder IT-Teams (ein/e Erziehungsberater/in, ein/e IT-Koordinator/in, eine Lehrkraft usw.) Folgendes so schnell wie möglich zu melden:

- jede/s verdächtige Software oder Gerät,
- jede/n Verlust, Diebstahl oder Gefährdung seiner/ihrer Authentifizierungsinformationen,
- jede/s/r Nachricht, Datei, Dokument, Link, Bild von einem unbekannten Absender,
- jede ungewöhnliche Aktivität bezüglich des Accounts: E-Mails, die ohne Kenntnis des Account-Inhabers verschickt wurden, duplizierte Dateien auf dem Schulserver oder online.

7. VERANTWORTUNG

Die absichtliche Beschädigung der Geräte und IT-Ressourcen der Schule wird gemäß Artikel 32 der Allgemeinen Schulordnung der Europäischen Schulen Reparaturkosten für die gesetzlichen Vertreter/innen der betroffenen Schüler/innen nach sich ziehen.

Jede/r Schüler/in, der/die beschließt, ein Mobiltelefon oder ein anderes elektronisches Gerät in die Schule mitzubringen, tut dies auf eigene Gefahr und ist persönlich für die Sicherheit seines/ihres Mobiltelefons oder Geräts verantwortlich.

Unbeschadet der vorgesehenen Ausnahmen, wenn Schüler/innen ein Gerät für das BYOD-Programm mitbringen müssen, weist die Schule jegliche Haftung für Verlust, Diebstahl, Beschädigung oder Vandalismus eines Telefons oder irgendeines anderen Geräts oder für die unerlaubte Nutzung eines solchen Geräts zurück. Zum Schutz des Gerätes wird die Verwendung einer Schutzhülle empfohlen.

8. VORGESEHENE SANKTIONEN

Jede/r Schüler/in, der/die gegen die oben beschriebenen Regeln verstößt, wird sich den in der Allgemeinen Schulordnung der Europäischen Schulen und in der Hausordnung der Schule vorgesehenen Disziplinarmaßnahmen sowie den gesetzlich vorgesehenen Sanktionen und strafrechtlichen Verfahren stellen müssen.

Alle Mitglieder des pädagogischen Teams müssen sich verpflichten dafür zu sorgen, dass diese Bestimmungen durch die Schüler/innen unter ihrer Verantwortung eingehalten werden, und müssen diesbezüglich strenge Kontrolle ausüben.

Der/Die IT-Administrator/in muss dafür sorgen, dass die IT-Ressourcen ordnungsgemäß funktionieren und ordnungsgemäß genutzt werden. Dazu bietet die Überwachung der IT-Ressourcen und -Geräte die Möglichkeit, Abweichungen (anormale Nutzung des Netzwerks, überhöhte Menge an Speicherplatz, versuchter Cyberangriff usw.) zu erkennen. Sollten Abweichungen erkannt werden, wendet sich der/die IT-Administrator/in an die Schulleitung, um die erforderlichen Maßnahmen zu vereinbaren. Um das IT-System der Schule zu schützen, darf der/die IT-Administrator/in jedoch eine sofortige Entscheidung treffen, um den IT-Zugang eines/einer oder mehrerer Schüler/innen zu blockieren, und wird die Angelegenheit danach sofort der Schulleitung vorlegen. Sollten Benutzeraccounts als kompromittiert erkannt werden, so werden alle Endgeräte, die sich unter Verwendung dieser Daten den Zugang zum WLAN-Netzwerk verschaffen oder verschafft haben, permanent für die Nutzung dieses Netzwerks gesperrt.

Diese Art von Eingriff ist nur zur Erfüllung deutlich umschriebener Ziele möglich, und zwar:

- Vorbeugung illegaler oder diffamierender Handlungen, Handlungen, die gegen die akzeptierten Standards richtigen Verhaltens verstoßen oder die Würde anderer Personen verletzen können;

- Schutz der wirtschaftlichen oder finanziellen Interessen der Schule, die mit Geheimhaltung verbunden sind;
- Sicherheit und/oder reibungsloser technischer Betrieb der IT-Systeme, einschließlich Kontrolle der verbundenen Kosten, und physischer Schutz der Einrichtungen der Schule;
- Einhaltung in gutem Glauben der Grundsätze und Regeln für die Nutzung der verfügbaren Technologien und dieser Charta.

9. ÜBERARBEITUNG

Die erste Version dieser Charta wurde von der Schulleitung der ESM am 07.12.2020 genehmigt. Die aktualisierte Version, in der Passagen zum BYOD-Programm und zur Nutzung Künstlicher Intelligenz ergänzt wurden, wurden am 23.09.2025 von der Schulleitung der ESM genehmigt. Die Charta wird zu einem gegebenen Zeitpunkt erneut aktualisiert, um aktuellen Entwicklungen Rechnung zu tragen.

ICT Charter

for the use of IT resources and devices by pupils at the European School Munich

Version dated 23.09.2025

Contents

1. PREAMBLE 2
2. IT RESOURCES AND EQUIPMENT 2
   2.1 Definition 2
   2.2 Golden rule 2
   2.3 Access to IT resources and equipment 2
3. GENERAL RULES OF CONDUCT 3
   3.1 General remarks 3
   3.2 Respect for confidentiality 4
   3.3 Respect for the network and workstations 4
   3.4 Respect for intellectual property rights 5
   3.5 Respect for members of the school community and the school 5
4. SPECIAL RULES FOR THE USE OF THE INTERNET 5
   4.1 The school network 5
   4 .2 Supervision and assistance during school sessions 6
   4.3 Social media 6
   4.4 Use of artificial intelligence (AI) 7
5. SPECIAL RULES FOR ONLINE LEARNING/TEACHING 7
6. REPORTS TO THE EDUCATIONAL/IT TEAM 7
7. RESPONSIBILITY 8
8. PENALTIES 8
9. REVISION 9

1. PREAMBLE

The European Schools strive to provide their pupils with suitable working conditions in terms of IT and multimedia services. This charter sets out the rules for the proper use of and correct behaviour towards the IT resources made available to them for educational purposes.

This Charter is an appendix to the House Rules of the European School Munich (hereinafter referred to as "the School") and fits within the framework of laws and regulations relating in particular to copyright, intellectual property rights, data protection (including, in particular, image rights) and the processing of personal data, as well as computer crime.

2. IT RESOURCES AND EQUIPMENT

2.1 Definition

"IT resources and equipment" refers to the package comprising the school's network, servers and workplaces, interactive whiteboards, peripheral devices (printers, external hard drives, cameras), software, laptops and tablets, internet use at the school and the digital learning resources provided by the school[1] . It also refers to the school network and those devices that can be accessed via the network by entering user login details, in particular the pupils' own devices as part of the "Bring Your Own Device" programme. Although these devices are privately owned by families, their use is subject to certain obligations as soon as they connect to the school's infrastructure.

2.2 Golden rule

The European School's IT resources are intended *exclusively* for educational activities.

2.3 Access to IT resources and equipment

Access to the resources, equipment and infrastructure provided by the school is a privilege, not a right.

Each individual pupil must conscientiously comply with the operating conditions and rules for proper use and conduct described in this Charter.

The School may regularly check all pupils, or on a case-by-case basis, whether IT resources and equipment are being used in accordance with the provisions of this Charter and reserves the right to revoke this privilege if necessary.

[1] According to the definition in the procedure for authorising the use of a digital learning tool in European Schools (Annex to MEMO 2019-12-M-3/GM).

At the school, access to IT resources and equipment is provided under the responsibility of the school management and under the supervision of a member of the pedagogical staff.

The school provides access to various IT resources:

- to the school's computers via a personal account,
- to school equipment, e.g. speakers, headphones, cameras and other hardware devices necessary for the curriculum,
- to the school network, which includes storage space on the school's servers (shared space or space limited to the personal account) and network printers (including 3D printers),
- to Office 365 online services (including, in particular, email/messaging services) managed by the European School,
- to proprietary, licensed or open-source software,
- to the school network, in particular for BYOD devices, and thus also to the internet.

All access data provided to the pupil is personal and may only be used by the pupil concerned. The access codes must therefore be kept strictly confidential and may not be disclosed to third parties (with the exception of the pupil's legal representatives). Before leaving their workstation, pupils must always ensure that they have logged out.

In the event of a problem with their account or in the event of loss, theft or compromise of their access codes, the pupil shall inform their educational advisor.

Furthermore, the use of the school's entire digital infrastructure, including BYOD devices, is only permitted on condition that the pupil uses the IT resources and devices exclusively for school and teaching-related purposes. Any use for other purposes is not permitted within the school's entire infrastructure.

3. GENERAL RULES OF CONDUCT

3.1 General remarks

Pupils must comply with the rules of proper conduct when using the resources and equipment provided by the school for educational purposes. Therefore, if a pupil accesses the school network with his or her own mobile device at school, e.g. as part of the BYOD project, or outside of school, this charter must be complied with.

For personal use outside school, each pupil receives five Office 365 installation licences. These licences can be installed and used on IT devices that are regularly used by the pupil. To ensure that access codes and account information are not accessible to third parties in accordance with

the general rules of conduct described in section 3.2 of this charter, the end device must be password-protected.

Please note: It is strictly forbidden to enter an ICT room and use the IT devices provided if there is no supervision by a responsible person.

3.2 Respect for confidentiality

Pupils are prohibited from:

- attempting to obtain other people's passwords,
- logging in with other people's usernames and passwords,
- using another user's open session without their express permission,
- open, edit or delete other people's files and, in general, attempt to access their information without their permission,
- saving a password in Internet software such as a browser when using devices that are not their personal property.

3.3 Respect for the network and workstations

In the spirit of mutual respect and respect for school property, rooms, equipment and infrastructure must be treated with care. Therefore, pupils are not allowed to eat or drink while using the equipment provided.

Headphones should be tidied away properly after use. Screens should not be switched off manually. These are switched off by the system after fifteen minutes of inactivity in order to reduce power consumption and thus protect the environment.

Pupils are prohibited from:

- attempting to change the configuration of the workstation,
- attempt to change or destroy data from the network or workstation,
- installing software or copying software available on the network,
- accessing or attempting to access resources other than those authorised by the school,
- open messages, files, documents, links or images from unknown senders,
- connecting a storage device or medium (USB, mobile phone or similar) without the permission of a responsible adult,
- intentionally interfering with the operation of the network, in particular by using programmes designed to install malicious programmes or circumvent security measures (viruses, spyware or similar),
- using VPN[2] tunnels or forwarding network traffic via a proxy server,
- Sharing their personal user data for the network with other pupils so that they can log in to their devices under a false name. This will result in the account being blocked.

[2] In IT, a **virtual private network, or VPN** for short, is a system that enables a direct connection to be established between computers that are far apart by isolating this traffic in a kind of tunnel.

3.4 Respect for intellectual property rights

Pupils are prohibited from:

- downloading materials protected by intellectual property rights or making illegal copies of them (streaming, audio, films, software, games, etc.),
- Plagiarising information, regardless of the medium (table, graphic, article of a legal act, image, text, hypothesis, theory, opinion, etc.), which may be protected by intellectual property rights (such as copyright), i.e. reproducing, distributing or communicating it to the public in any form.

The use of information found on the internet for class assignments implies that the sources must be recorded and correctly cited by the pupil. He/she may seek the help of a pedagogical staff member in this regard.

3.5 Respect for members of the school community and the school

Pupils are prohibited from:

- Displaying, publishing or participating in the exchange of documents or websites of a defamatory, abusive, extremist, pornographic, inhuman or discriminatory nature – based on ethnic origin, political opinions, religion or ideological beliefs, health status or sexual orientation – on screen;
- bullying other persons in your own name or using a false identity or pseudonym (cyberbullying);
- using lists of email addresses or personal data of other persons for purposes other than those intended for educational or didactic purposes;
- using inappropriate language in emails, posts, chats or any other means of communication (the author is solely responsible for the content sent);
- damaging the reputation of a member of the school community or the school, in particular by disseminating texts, images and/or videos;
- enter into contracts to sell or advertise anything on behalf of the school, unless the project has been approved in advance by the school management.

4. SPECIAL RULES FOR THE USE OF THE INTERNET

4.1 The school network

Access to the internet within the European School is a privilege, not a right. Use of the educational internet-based network is intended solely for teaching and learning activities that are in line with the mission of the European Schools.

Pupils are prohibited from:

- share personal information that could identify them (first name, surname(s), email address, address, etc.),
- attempt to access pornographic, inhuman, xenophobic, anti-Semitic, racist or other websites that are harmful to minors.
- download or install any programme or software unless otherwise agreed with the teacher for a specific purpose.

Under no circumstances should pupils give their name, show a photo, give their address, telephone number or any other information that could be used to identify them on the internet.

Pupils are prohibited from using the email address associated with their O365 account (...@student.eursc.eu) to create accounts on applications, websites or software that are not approved by a member of the teaching team or the school management.

4 .2 Supervision and assistance during school sessions

The school may use a supervision and support system to ensure that pupils are engaged in a continuous learning process and to enable those responsible for the respective course and library staff to assist pupils directly from their workstations.

Only persons authorised by the school management may use the supervision and support software, and they must comply with the IT charter applicable to their role at the school.

This system offers the following options:

- remotely access pupils' screens to help them and ensure they remain focused on their tasks,
- select pupils' screens to present their work,
- deactivate all pupils' screens to ensure their attention.

4.3 Social media

Pupils are prohibited from logging into social media (such as Facebook or Instagram) using the email address associated with their O365 account (...@student.eursc.eu).

The use of a private digital device (phone, tablet, laptop) does not exempt pupils from complying with the rules for its proper use and correct behaviour with regard to respect for members of the school community and the school, as described in this charter. Pupils remain responsible for the content they display.

4.4 Use of artificial intelligence (AI)

Pupils are permitted to use AI tools that have been checked and approved by the school in accordance with data protection regulations after authorisation by the teacher for the current task or lesson sequence. However, it should be noted that no personal data or third-party data may be transmitted to the AI. The permitted tools are specified by the school.

If pupils use AI for homework, work assignments or projects, with the teacher's permission, they must be honest and transparent and disclose this. Furthermore, the use of AI must be accompanied by respect for privacy, intellectual property and the ecological footprint.

Detailed rules of use are set out in the "Regulations on the Use of Artificial Intelligence", which can also be found on the school's website.

5. SPECIAL RULES FOR ONLINE LEARNING/TEACHING

Online learning or teaching implies compliance with the rules for proper use and correct behaviour as prescribed by this charter, whether in the context of:

- Online learning or teaching at school ("blended learning"), which implies the use of digital learning tools approved by the school management, or the execution of asynchronous online activities (homework),
- online learning or teaching at a distance ("distance learning") when teaching at school is suspended,
- online learning or teaching at a distance and *in situ* ("hybrid learning"), when lessons are attended by some pupils on site and others at a distance.

In addition, the following is prohibited:

- photographing and/or filming the teacher(s) and pupil(s) participating in online learning and, *a fortiori*, publishing such images/videos;
- participating in online learning or teaching sessions to which the pupil has not been expressly invited,
- inviting participants to online learning or teaching sessions without the consent of the person organising the session,
- using digital learning tools to intimidate, insult, defame, bully or threaten other people.

Image rights are recognised rights for every member of the school community, which is why the school will not tolerate the use of images/videos taken without the knowledge of the persons concerned.

6. REPORTS TO THE EDUCATIONAL/IT TEAM

The pupil undertakes to report the following to a member of the educational or IT team (an educational advisor, IT coordinator, teacher, etc.) as soon as possible:

- any suspicious software or device,
- any loss, theft or compromise of their authentication information,
- any message, file, document, link or image from an unknown sender,
- any unusual activity relating to the account: emails sent without the account holder's knowledge, duplicate files on the school server or online.

7. RESPONSIBILITY

Deliberate damage to the school's equipment and IT resources will result in repair costs being charged to the legal representatives of the pupils concerned, in accordance with Article 32 of the General School Regulations of the European Schools.

Any pupil who decides to bring a mobile phone or other electronic device to school does so at their own risk and is personally responsible for the safety of their mobile phone or device.

Notwithstanding the exceptions provided, if pupils are required to bring a device for the BYOD programme, the school accepts no liability for loss, theft, damage or vandalism of a telephone or any other device, or for the unauthorised use of such a device. The use of a protective cover is recommended to protect the device.

8. PENALTIES

Any pupil who violates the rules described above will be subject to the disciplinary measures provided for in the General School Regulations of the European Schools and in the school's internal rules, as well as to the sanctions and criminal proceedings provided for by law.

All members of the teaching team must undertake to ensure that these rules are observed by the pupils under their responsibility and must exercise strict control in this regard.

The IT administrator must ensure that IT resources function properly and are used correctly. To this end, monitoring IT resources and equipment makes it possible to detect anomalies (abnormal use of the network, excessive use of storage space, attempted cyber-attacks, etc.). If deviations are detected, the IT administrator contacts the school management to agree on the necessary measures. However, in order to protect the school's IT system, the IT administrator may take an immediate decision to block the IT access of one or more pupils and will then immediately refer the matter to the school management. If user accounts are identified as compromised, all end devices that use this data to access or have accessed the Wi-Fi network will be permanently blocked from using this network.

This type of intervention is only possible for the fulfilment of clearly defined objectives, namely:

- Prevention of illegal or defamatory actions, actions that violate accepted standards of proper behaviour or that may violate the dignity of other persons;
- Protection of the economic or financial interests of the school that are associated with confidentiality;
- ensuring the security and/or smooth technical operation of IT systems, including control of associated costs, and the physical protection of the school's facilities;
- Compliance in good faith with the principles and rules for the use of available technologies and this charter.

9. REVISION

The first version of this Charter was approved by the ESM management on 7 December 2020. The updated version, in which passages on the BYOD programme and the use of artificial intelligence were added, was approved by the ESM management on 23 September 2025. The charter will be updated again at a given point in time to reflect current developments.