ICT-Charta

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

Version vom 07.12.2020

Inhalt

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 bereitgestellte digitale Lernmittel[1] umfasst.

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 und Geräten 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.

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.

[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).

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 Internet.

Alle Zugangsaccounts, 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.

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 (Nur für Höhere Schule), oder außerhalb der Schule auf Ressourcen (also auf das Netzwerk) zugreift, muss diese Charta eingehalten werden.

Für die persönliche Nutzung außerhalb der Schule erhält jede/r Schüler/in 5 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 beschriebenen (2.3) allgemeinen Regeln für richtiges Verhalten, die Zugangs-

kennungen 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 Google Chrome, Internet Explorer, Firefox usw. zu speichern, wenn sie Geräte verwenden, die nicht persönlich sind.

3.3 Respekt vor dem Netzwerk und vor Arbeitsplätzen

Vor den Anlagen und der Hardware muss höchster Respekt gezeigt werden. Computertastaturen und -Mäuse müssen mit Sorgfalt gehandhabt werden. Deshalb dürfen die Schüler/innen nicht essen und trinken, wenn sie die Arbeitsplätze an der Schule benutzen, damit diese nicht beschädigt werden.

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.

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;
- 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.

[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.

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.

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 Maß-

nahmen 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

Diese von der Schulleitung der ESM am 07.12.2020 genehmigte Charta wird ihrer Federführung zu einem gegebenen Zeitpunkt aktualisiert.

ICT Charter

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

Version dated 07/12/2020

Table of Contents

1. PREAMBLE

The European Schools endeavour to offer pupils the best possible working conditions in terms of IT and multimedia services. This Charter sets out the rules for proper use of and good behaviour vis-à-vis the IT resources with a pedagogical purpose made available to them.

This Charter forms an annex to the House Rules of the European School, […] (hereinafter referred to as 'the School') and falls within the framework of the laws and regulations in force relating in particular to copyright, to intellectual property rights, to privacy protection (including in particular image rights) and to the processing of personal data, as well as computer crime.

2. IT RESOURCES AND DEVICES

2.1 Definition

'IT resources and devices' means the package composed of the School's network, servers and workstations, interactive whiteboards, peripheral devices (printers, external hard drives), software, laptop computers and tablets, use of the Internet in the School and digital learning resources[1] provided by the latter.

2.2 Golden rule

The European School's IT resources are intended to be used *solely* for pedagogical activities.

2.3 Access to IT resources and devices

Access to the resources and devices provided by the School is a privilege and not a right.

Each and every pupil is required to comply scrupulously with the operating conditions and the rules for proper use and good behaviour contained in this Charter.

The School can carry out regular or occasional checks to verify that IT resources and devices are being used in compliance with the provisions of this Charter and reserves the right to revoke this privilege if need be.

In the School, access to IT resources and devices is provided under the responsibility of the School's Management and under the control of a member of the educational team.

[1] In accordance with the definition mentioned in the Procedure for approval of use of a Digital Learning Resource within the European Schools (Annex to MEMO 2019-12-M-3/GM).

The School offers access to different IT resources:

- To the School's computers via a personal account,
- To the School's network, comprising:
  - storage spaces on the School's servers: shared spaces or restricted to one's personal account,
  - network printers,
- To Office 365 online services (including in particular an email/messaging service) managed by the European School,
- To proprietary software, licensed or open source,
- To the Internet.

All access accounts with which the pupil is provided are personal and may be used only by the pupil concerned. Thus, access codes must be absolutely confidential and may not be divulged to third parties (with the exception of the pupil's legal representatives). Before leaving his/her workstation, the pupil must always ensure that he/she has logged out properly.

The pupil will inform his/her educational adviser in the event of a problem with his/her account and of loss, theft or compromising of his/her access codes.

3. GENERAL RULES OF GOOD BEHAVIOUR

3.1 General comments

Pupils are required to follow the rules of good behaviour when using the resources and devices made available to the School for pedagogical purposes. If a pupil accesses resources (i.e. the network) with his / her own mobile device at school, e.g. as part of the BYOD project (only for the high school), or outside the school, this charter must also be adhered to.

Every student receives 5 Office 365 installation licenses for personal use outside of school. These licenses can be installed and used on IT devices that are regularly used by the student. In order to ensure that, in accordance with the general rules for correct behaviour described in this charter (2.3), access IDs and account information are not accessible to third parties, end devices must be password-protected.

Particular attention should be paid to the following rule: It is strictly forbidden to enter an ICT room and to use the IT equipment provided without the supervision of a responsible adult.

3.2 Respect for confidentiality

Pupils are forbidden from:

- seeking to appropriate other people's passwords,
- logging in with other people's user names and passwords,
- using another user's open session without his/her explicit permission,
- opening, editing or deleting other people's files and, more generally, trying to access information belonging to them without their permission,
- saving a password in Internet software such as Google Chrome, Internet Explorer, Firefox, etc., when using non-personal devices.

3.3 Respect for the network and for workstations

Scrupulous respect for the premises and the hardware must be shown. Computer keyboards and mice must be handled with care. Thus, pupils are not allowed to eat and drink when using workstations in the School, so as not to damage them.

Headphones should be tidied up properly after use. Monitors should not be switched off manually. These are system-controlled and switch off after fifteen minutes of inactivity in order to reduce power consumption and thus protect the environment.

Pupils are forbidden from:

- seeking to change the workstation's configuration,
- seeking to change or to destroy network or workstation data,
- installing software or copying software present on the network,
- accessing or attempting to access resources other than those allowed by the School,
- opening messages, files, documents, links, images sent by unknown senders,
- inserting, into any device whatsoever, a removable drive, without the permission of a responsible adult,
- connecting a storage device or medium (USB, mobile phone, other) without the permission of a responsible adult,
- deliberately interfering with the network's operation, and in particular by using programs designed to input malicious programs or to circumvent security (viruses, spyware or other),
- Using a VPN tunnel or attempting to divert network traffic by using a proxy server.

3.4 Respect for intellectual property rights

Pupils are forbidden from:

- downloading or making illegal copies of material (streaming, audio, films, software, games, etc.) protected by intellectual property rights,
- plagiarising, i.e. reproducing, (re)disseminating, communicating to the public, in any form whatsoever, any information, irrespective of the medium (table, graph, equation, article of a legal act, image, text, hypothesis, theory, opinion, etc), which might be protected by intellectual property rights (copyright, etc.).

The use of information found on the Internet for classwork implies that the sources must be included and correctly quoted by the pupil. He/she may seek the assistance of one of the members of the educational team in this regard.

3.5 Respect for the members of the school community and of the School

Pupils are forbidden from:

- displaying on screen, publishing documents or taking part in exchanges of a defamatory, abusive, extremist or, pornographic, or discriminatory nature, whether based upon racial or ethnic origin, political opinions, religion or philosophical beliefs, state of health, or sexual orientation;
- bullying other people (cyberbullying), in their own name or using a false identity or a pseudonym;
- using other people's lists of email addresses or personal data for purposes other than those intended by pedagogical or educational objectives;
- using improper languages in emails, posts, chats or any other means of communication whatsoever (the message's author has sole responsibility for the content sent);
- damaging the reputation of a member of the school community or of the School, in particular by disseminating texts, images and/or videos;
- entering into contracts, selling or advertising in any way whatsoever on the School's behalf, unless the project has been approved beforehand by the School's Management.

4. SPECIAL RULES FOR USE OF THE INTERNET

4.1 The School's network

Access to the Internet within the European School is a privilege, not a right. The use of the pedagogical internet-based network is only intended for the purpose of teaching and learning activities that are in line with the mandate of the European Schools.

It is forbidden for students to:

- share personal information that can be used to identify the student (first name, last name (s), email address, address, etc.),
- try to access pornographic, inhuman, xenophobic, anti-Semitic, racist or other websites that are harmful to minors
- downloading or installing any program or software, unless otherwise agreed with the teacher for a specific purpose.

Under no circumstances should pupils mention their name, display a photo, mention their address, telephone number or any other information facilitating their identification on the Internet.

Pupils are prohibited from using the email address linked to their O365 account (…@student.eursc.eu) to create accounts on applications, websites or software not authorised by a member of the educational team or by the School's Management.

4.2 Supervision and assistance with the session for pupils in the School

The school may employ a system of supervision and support to ensure that students are in a continuous learning process and to enable course staff and library staff to contact students directly to help from their workplace.

Only persons authorized by the school management can use the supervision and support software and they must adhere to the IT charter applicable to their role at the school.

This system offers the possibility:

- remote access to student screens to help them and to keep them focused on their tasks,
- select student screens to present their work,
- Deactivate all students' screens to ensure their attention.

4.3 Social media

Pupils are prohibited from connecting to social media with the email address linked to their O365 account (…@student.eursc.eu).

Use of a private digital device (telephone, tablet, laptop) does not exempt pupils from following the rules for their proper use and good behaviour as laid down in this Charter, as regards respect for members of the school community and of the School. Pupils remain responsible for the content displayed.

5. SPECIAL RULES CONCERNING ONLINE LEARNING / TEACHING

Online learning or teaching implies following the rules for proper use and good behaviour laid down by this Charter, whether within the framework of:

- Online learning or teaching at school ('blended learning'), implying use of digital learning resources approved by the School's Management or engaging in asynchronous online activities (homework),
- Remote online learning or teaching ('distance learning'), when lessons in the School are suspended,
- Distance and *in situ* online learning or teaching ('hybrid learning'), when lessons are attended by some pupils *in situ* and by others remotely.

In addition, the following are prohibited:

- photographing and/or filming, by means of personal devices, the teacher(s) and the pupils participating in online learning and, *a fortiori*, from publishing such images/videos,
- participating in online learning or teaching sessions which the pupil might not have been expressly invited to attend,
- inviting participants to online learning or teaching sessions without the agreement of the person organising the session,
- using digital learning resources to intimidate, insult, bully, defame or threaten other people.

Image rights are recognised rights for each of the members 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. REPORTING TO THE EDUCATIONAL/ICT TEAM

The student undertakes to report to a member of the educational and/or IT team (an educational adviser, an IT coordinator, a teacher, etc.), as quickly as possible:

- any suspicious software or device,
- any loss, theft or compromising of his/her authentication information,
- any message, file, document, link, image sent by an unknown sender.

7. RESPONSIBILITY

Intentional damage to the School's devices and IT resources may result in repair costs for the legal representatives of the pupils concerned, in accordance with Article 32 of the General Rules of the European Schools.

Any pupil who chooses to bring a mobile phone or other electronic device to the School does so at his/her own risk and is personally responsible for the safety of his/her mobile phone or device.

Without prejudice to the exceptions provided for where pupils are required to bring a device to School for the purposes of the BYOD programme, the School will not accept any liability whatsoever for the loss or, theft of, or damage to or vandalism of a telephone or any other device, or for unauthorised use of such a device.

8. SANCTIONS PROVIDED FOR

Any pupil who contravenes the rules set out above will be liable to suffer the disciplinary measures provided for by the General Rules of the European Schools and the House Rules of the School and the sanctions and criminal proceedings provided for by law.

All members of the educational team must undertake to ensure that those provisions are respected by pupils who are under their responsibility and are required to exercise rigorous control in that respect.

The IT administrator must constantly ensure to his/her satisfaction that IT resources are operating properly and being properly used. To that end, monitoring IT resources and devices allows anomalies (abnormal use of the network, excessive amount of storage space, attempted cyberattack, etc.) to be detected. Should anomalies be detected, the IT administrator will approach the School's Management to agree on the measures to be taken. However, in cases of absolute emergency and to protect the School's IT system, the IT administrator may take an immediate decision to block IT access to one or more pupils, then will immediately refer the matter to the Management.

This type of intervention can be made only subject to compliance with clearly defined purposes, namely:

- prevention of illegal or defamatory actions, actions contrary to accepted standards of good behaviour or likely to affront other people's dignity;
- protection of the Schools' economic or financial interests, to which confidentiality is attached,

- security and/or smooth technical operation of IT systems, including control of the related costs, and physical protection of the School's facilities;
- Compliance in good faith with the principles and rules for use of the technologies available, and with this Charter.

9. REVISION

This charter, approved by the ESM management team on 07.12.2020, will be updated to their lead at an appropriate time

Charte d'utilisation des ressources et dispositifs informatiques des élèves de l'École européenne de Munich

Version du 07.12.2020

Table des matières

1. PRÉAMBULE

Les Écoles européennes s'efforcent d'offrir aux élèves les meilleures conditions de travail en informatique et services multimédia. La présente Charte précise les règles de bon usage et bonne conduite des ressources informatiques à vocation pédagogique mises à leur disposition.

Cette Charte vient en annexe du Règlement intérieur de l'Ecole européenne de Munich et s'inscrit dans le cadre des lois et règlements en vigueur, relatifs notamment au droit d'auteur, au droit de la propriété intellectuelle, à la protection de la vie privée (notamment du droit à l'image) et au traitement des données à caractère personnel ainsi qu'à la criminalité informatique

2. RESSOURCES ET DISPOSITIFS INFORMATIQUES

2.1 Définition

On entend par 'ressources et dispositifs informatiques' l'ensemble constitué par le réseau, les serveurs, les postes de travail de l'Ecole, les tableaux interactifs, les périphériques (imprimantes, disques durs externes), les logiciels, les ordinateurs portables et tablettes, l'usage d'Internet à l'Ecole et les ressources d'apprentissage numériques[1] fournis par cette dernière.

2.2 Règle d'or

L'utilisation des ressources informatiques de l'Ecole européenne est uniquement réservé aux activités pédagogiques.

2.3 Accès aux ressources et dispositifs informatiques

L'accès aux ressources et dispositifs fournis par l'Ecole est un privilège et non un droit. Chaque élève est tenu de respecter scrupuleusement les conditions de fonctionnement, les règles de bon usage et bonne conduite contenues dans cette Charte. L'École peut procéder à des contrôles réguliers ou occasionnels pour vérifier que les ressources et dispositifs informatiques sont utilisés dans le respect des prescriptions de la présente Charte, et se réserve le droit de révoquer ce privilège le cas échéant.

[1] Conformément à la définition mentionnée dans la Procédure d'approbation de l'utilisation d'une ressource d'apprentissage numérique au sein des Écoles européennes (Annexe au MEMO 2019-12-M-3/GM).

Dans l'École, l'accès aux ressources et dispositifs informatiques se fait sous la responsabilité de la Direction de l'Ecole et sous le contrôle d'un membre de l'équipe éducative.

L'École propose l'accès à différentes ressources informatiques :

- aux ordinateurs de l'École via un compte personnel,
- aux appareils de l'École comprenant par exemple, des micros, des casques, des caméras ou autres matériels ou logiciels nécessaires pour l'apprentissage,
- au réseau de l'École comprenant des espaces de stockage des serveurs de l'École (espaces partagés ou limités à son compte personnel) et des imprimantes réseaux (dont des imprimantes en 3D),
- aux services en ligne Office 365 (comprenant notamment un service de messagerie) gérés par l'École européenne,
- à des logiciels propriétaires sous licences ou libres,
- à Internet.

Tous les comptes d'accès fournis à l'élève sont personnels et ne peuvent être utilisés que par l'élève concerné. Ainsi, les codes d'accès doivent être absolument confidentiels et non divulgués à de tierces personnes (exception faite des représentants légaux de l'élève). Avant de quitter sa station de travail, l'élève doit toujours s'assurer qu'il s'est bien déconnecté.

L'élève préviendra son conseiller d'éducation en cas de problème avec son compte, en cas de perte, vol ou compromission de ses codes d'accès.

3. RÈGLES GÉNÉRALES DE BONNE CONDUITE

3.1 Remarques générales

Le respect des règles générales de bonne conduite s'impose aux élèves lorsqu'ils utilisent les ressources et dispositifs mis à leur disposition par l'Ecole à des fins pédagogiques. Ainsi, l'accès à ces ressources par l'élève qui utilise son appareil mobile personnel dans l'Ecole, par exemple dans le cadre du projet BYOD (seulement en secondaire) ou à l'extérieur, implique également le respect de la présente Charte.

Pour un usage personnel à l'extérieur de l'École, chaque élève se voit offrir 5 licences d'installation d'Office 365 pour des ordinateurs et/ou des téléphones portables et tablettes. Ces licences ne peuvent être utilisées et installées que sur des dispositifs informatiques régulièrement utilisés par l'élève et protégés par un mot de passe dans le respect des règles générales de bonne conduites énoncées dans la présente Charte cf. 2.3).

Attention : il est formellement interdit d'entrer dans un local informatique et d'utiliser le dispositif informatique en l'absence d'une personne chargée de la surveillance.

3.2 Respect de la confidentialité

Il est interdit à l'élève :

- de chercher à s'approprier le mot de passe d'autrui,
- de se connecter avec le nom d'utilisateur et mot de passe d'autrui,
- d'utiliser une session ouverte d'un autre utilisateur sans son autorisation explicite,
- d'ouvrir, de modifier ou d'effacer les fichiers d'autrui et de façon plus générale d'essayer d'accéder à des informations lui appartenant sans son autorisation,
- de faire une sauvegarde de mot de passe dans les logiciels d'internet comme Google chrome, Internet explorer, Firefox … lors de l'utilisation de dispositifs non personnels.

3.3 Respect du réseau et des postes de travail

Les locaux et le matériel doivent être scrupuleusement respectés.
Les claviers et les souris doivent être manipulés avec soin. Ainsi, les élèves ne sont pas autorisés à manger et boire lorsqu'ils utilisent les postes de travail au sein de l'Ecole, afin de ne pas les endommager. Les casques doivent être bien rangés après utilisation. Les écrans ne doivent pas être éteints manuellement, car ceux-ci sont fermés automatiquement après 15 minutes d'inactivité, afin de réduire la consommation d'électricité et donc, de protéger l'environnement.

Il est interdit à l'élève :

- de chercher à modifier la configuration du poste de travail,
- de chercher à modifier ou de détruire des données du réseau ou du poste de travail,
- d'installer un logiciel ou de faire une copie d'un logiciel présent sur le réseau,
- d'accéder ou de tenter d'accéder à d'autres ressources que celles autorisées par l'École,
- d'ouvrir des messages, fichiers, documents, liens, images envoyés par des expéditeurs inconnus,
- de connecter un dispositif ou support de stockage (USB, GSM, autres) sans l'autorisation d'un adulte responsable,
- de perturber volontairement le fonctionnement du réseau, et notamment d'utiliser des programmes destinés à introduire des programmes nuisibles ou à contourner la sécurité (virus, logiciels espions ou autres).
- d'utiliser des tunnels VPN[2] ou de détourner des systèmes de protection mis en place.

[2] En informatique, un réseau privé virtuel, abrégé VPN – *Virtual Private Network*, est un système permettant de créer un lien direct entre des ordinateurs distants, en isolant ce trafic dans une sorte de tunnel.

3.4 Respect des droits de propriété intellectuelle

Il est interdit à l'élève de :

- télécharger ou effectuer des copies illégales de matériel (streaming, audio, films, logiciels, jeux…) protégé par des droits de propriété intellectuelle,
- plagier, c'est-à-dire reproduire, (re)diffuser, communiquer au public, sous quelque forme que ce soit, toute information, quel qu'en soit le support (tableau, graphique, équation, article de loi, image, texte, hypothèse, théorie, opinion, etc.), qui serait protégé par un droit de propriété intellectuelle (droit d'auteur, etc.).

L'utilisation d'informations trouvées sur internet pour les travaux de classe implique que les sources soient comprises et correctement citées par l'élève. Ce dernier peut solliciter l'aide d'un des membres de l'équipe éducative à cet égard.

3.5 Respect des membres de la communauté scolaire et de l'École

Il est interdit à l'élève :

- d'afficher à l'écran, de publier des documents ou de prendre part à des échanges ayant un caractère diffamatoire, injurieux, extrémiste, pornographique, discriminatoire, que ce soit sur la base de l'origine raciale ou ethnique, des opinions politiques, de la religion ou des convictions philosophiques, ou de l'état de santé, ou de l'orientation sexuelle,
- d'harceler autrui (cyber-harcèlement), en son nom ou à l'aide d'une fausse identité ou d'un pseudonyme,
- d'utiliser les listes d'adresses électroniques ou données personnelles d'autrui à d'autres fins que celles visées par des objectifs pédagogiques ou éducatifs,
- d'utiliser un langage incorrect dans les emails, post, chats ou quelconque autre moyen de communication (l'auteur du message engage sa seule responsabilité sur le contenu expédié),
- de porter atteinte à la réputation d'un membre de la communauté scolaire ou de l'École, notamment par l'intermédiaire de diffusion de textes, d'images et/ou vidéos,
- de contracter, vendre ou faire de la publicité, de quelque manière que ce soit, au nom de l'École, à moins d'avoir préalablement fait approuver son projet par la Direction de l'École.

4. RÈGLES PARTICULIÈRES POUR L'USAGE D'INTERNET

4.1 Réseau de l'École

L'accès à Internet au sein de l'École européenne est un privilège et non un droit. L'usage du réseau Internet pédagogique est réservé à des activités d'enseignement répondant aux missions des Écoles européennes.

Il est strictement interdit à l'élève :

- de partager des informations personnelles permettant l'identification de l'élève (prénom, noms, courrier électronique, adresse, …),
- d'accéder à des sites pornographiques, xénophobes, antisémites ou racistes,
- de télécharger et d'installer quelque programme que ce soit, excepté en cas d'accord avec l'enseignant-e, à des fins précises.

L'élève ne devra en aucun cas mentionner son nom, sa photo, son adresse, son numéro de téléphone ou d'autres informations facilitant son identification sur Internet.

Il est interdit à l'élève d'utiliser l'adresse électronique liée à son compte O365 (…@student.eursc.eu) pour créer des comptes sur des applications, sites web ou software non autorisés par un membre de l'équipe éducative ou par la Direction de l'École.

4.2 Supervision et assistance de la session des élèves dans l'École

L'École utilise un système de supervision et d'assistance pour garder les élèves dans une dynamique d'apprentissage et pour permettre aux responsables du cours en question et aux responsables de la bibliothèque d'aider les élèves directement depuis leur poste de travail.

Seules les personnes autorisées par la Direction peuvent utiliser le logiciel de supervision et d'assistance, et sont tenues de respecter la Charte informatique applicable à leur rôle au sein de l'École.

Ce système permet :

- d'accéder aux écrans des élèves à distance, pour les aider et les garder concentrés sur leurs tâches,
- de sélectionner les écrans des élèves pour présenter leur travail,
- de désactiver tous les écrans des élèves afin de capter leur attention.

4.3 Réseaux sociaux

Il est interdit à l'élève de se connecter aux réseaux sociaux (comme Facebook, Instagram) avec l'adresse électronique liée à son compte O365 (…@student.eursc.eu).

L'utilisation d'un dispositif numérique privé (téléphone, tablette, laptop) n'exonère pas l'élève du respect des règles de bon usage et de bonne conduite de la présente Charte, pour ce qui relève du respect des membres de la communauté scolaire et de l'Ecole. L'élève demeure responsable du contenu diffusé.

5. RÈGLES PARTICULIÈRES CONCERNANT L'APPRENTISSAGE / L'ENSEIGNEMENT EN LIGNE

L'apprentissage ou l'enseignement en ligne implique le respect des règles de bon usage et de bonne conduite énoncées par la présente Charte, que ce soit dans le cadre d'un :

- apprentissage ou enseignement en ligne à l'École (« blended learning »), impliquant l'utilisation de ressources d'apprentissage numérique approuvées par la Direction de l'École, ou la réalisation d'activités en ligne asynchrones (devoirs),
- apprentissage ou enseignement en ligne à distance (« distance learning »), lors d'une suspension des cours dans l'École,
- apprentissage ou enseignement en ligne à distance et in situ (« hybrid learning »), lorsque les cours sont suivis par une partie des élèves, in situ, et par une autre partie, à distance.

En outre, il est interdit :

- de photographier et/ou filmer le(s) professeur(s) ainsi que les élèves participant à l'apprentissage en ligne à l'aide de dispositifs personnels, et a fortiori, de publier ces images/vidéos,
- de participer à des sessions d'apprentissage ou enseignement en ligne, à laquelle l'élève n'aurait pas été invité de manière expresse,
- d'inviter des participants aux sessions d'apprentissage ou enseignement en ligne, sans l'accord de la personne organisant la session,
- d'utiliser les ressources d'apprentissage numériques, pour intimider, harceler, diffamer ou menacer autrui.

Le droit à l'image est un droit reconnu pour chacun des membres de la communauté scolaire, c'est pourquoi l'École ne pourra tolérer l'utilisation d'images/vidéos prises à l'insu des personnes concernées.

6. SIGNALEMENT À L'ÉQUIPE ÉDUCATIVE

L'élève s'engage à signaler à un membre de l'équipe éducative ou informatique (un conseiller, un coordinateur IT, un professeur, etc.), le plus rapidement possible :

- tout logiciel ou dispositif suspect,
- toute perte, vol ou compromission de ses informations d'authentification,
- tout message, fichier, document, lien, image envoyée par un expéditeur inconnu,
- toute activité inhabituelle sur le compte : des courriels envoyés sans connaissance de cause du propriétaire du compte, données copiées du serveur de l'École ou en ligne.

7. RESPONSABILITÉ

Les dommages intentionnels portés aux ressources informatiques de l'École peuvent entraîner des frais de réparation dans le chef des représentants légaux des élèves concernés, conformément à l'article 32 du Règlement général des Ecoles européennes.

Tout élève qui choisit d'apporter un téléphone portable ou tout autre appareil électronique à l'École le fait à ses propres risques et est personnellement responsable de la sécurité de son téléphone portable ou de son appareil.

Sans préjudice des exceptions prévues dans le cas où les élèves sont tenus d'apporter un appareil à l'Ecole pour les besoins du programme BYOD, cette dernière n'assumera aucune responsabilité pour la perte, le vol, les dommages ou le vandalisme d'un téléphone ou tout autre appareil, ou encore pour l'utilisation non autorisée d'un tel appareil.

8. SANCTIONS PRÉVUES

L'élève qui contreviendrait aux règles énoncées ci-dessus s'expose aux sanctions disciplinaires prévues par le Règlement général des Écoles européennes et le Règlement interne de l'École, ainsi qu'aux sanctions et poursuites pénales prévues par la loi.

Tout membre de l'équipe éducative s'engage à faire respecter ces dispositions par les élèves qui sont sous sa responsabilité et se doit d'exercer un contrôle rigoureux.

L'administrateur informatique doit s'assurer constamment du bon fonctionnement et du bon usage des ressources informatiques. A cette fin, la surveillance des ressources et dispositifs informatiques permet de détecter les anomalies (utilisation anormale du réseau, espace de stockage excessif, tentative de cyber-attaque, …).

En cas d'anomalies détectées, l'administrateur informatique sollicite la Direction de l'École pour convenir des mesures à prendre. Cependant, en cas d'urgence absolue et pour protéger le système informatique de l'École, l'administrateur informatique peut prendre la décision immédiate de bloquer les accès informatiques à un ou plusieurs élèves, puis en référer immédiatement à la Direction.

Si les comptes utilisateurs sont reconnus comme compromis, tous les appareils qui ont obtenu l'accès au réseau WLAN en utilisant ces données seront bloqués en permanence pour l'utilisation de ce réseau.

Ce type d'intervention ne peut être effectué que moyennant le respect de finalités clairement définies, à savoir :

- la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui,
- la protection des intérêts économiques ou financiers de l'École auxquels est attaché un caractère de confidentialité,
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'Ecole,
- le respect en toute bonne foi des principes et règles d'utilisation des technologies disponibles, et de la présente Charte.

9. RÉVISION

Cette charte, approuvée par la direction de l'EEMle 07/12/2020, sera mise à jour sous leur direction en temps voulu.