ECOLE EUROPEENNE DE BRUXELLES III
EUROPEAN SCHOOL BRUSSELS III
EUROPÄISCHE SCHULE BRÜSSEL III

EEB3 | Charter for use of IT resources and devices by Pupils

Creation : 2020
Update : 04/2026
Service : Management

Diffusion : **Whole school**

Contents

1. PREAMBLE

The European Schools endeavour to offer pupils the best possible working conditions in terms of IT digital 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 rules of the European School Brussels III, (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 technical devices and ICT services of the School's: network, servers and workstations, interactive whiteboards, peripheral devices (printers, external hard drives, etc...), laptops, computers and tablets, software applications, user credentials, and use of the Internet services in the School as well as digital learning resources 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 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 conduct 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.

The School offers access to different IT resources:

- To the School's computers via a personal account (provided user credentials),
- 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.
- School Management System (SMS)
- Wi-Fi

- All access accounts and user credentials with which the pupil is provided are personal and may be used only by the pupil concerned. Thus, access codes and user credentials must be absolutely confidential and may not be divulged to third parties (with the exception of the pupil's legal representatives). However, **the parents/legal representatives of the pupils are strictly prohibited to use the ICT resources provided to the pupils for any other purposes than aiding the pupils teaching and learning** (such as, using the MS 365 office suite for personal needs or joining meetings with the pupil's account etc.).

- 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

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. Thus, access to resources by a pupil who is using his/her own personal mobile device in the School (i.e. access to the network) or outside the School also means complying with this Charter.

For personal use outside school, each pupil will be given 5 Office 365 installation licences (for the use of Word, Excel, PowerPoint, one note, outreach and one drive) for computers and/or smart phones and tablets. These licences may be used and installed on IT devices regularly used by the pupil and password-protected in compliance with the general rules of good behaviour set out in this Charter.

3.2 Respect for confidentiality

Pupils are forbidden from:

- Seeking to appropriate other people's passwords,
- Logging in with other people's usernames and passwords,
- Using another user's open session without his/her explicit permission,
- Opening, disclosing/sharing, editing, downloading, 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. Computers, keyboards, mice, and screens must be handled with care. Thus, pupils are not allowed to eat and drink when using school workstations in the School, so as not to damage them.

Pupils are forbidden from:

- Seeking to change the equipment's (such as laptop's, tablet's 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),
- Subverting or attempting to subvert the protection systems installed (firewall, antivirus programs, etc...),
- Using VPN[1] tunnels.

3.4 Respect for intellectual property rights

Pupils are forbidden from:

- Downloading/uploading or making illegal copies of material (streaming, audio, films, software, games, etc.) protected by intellectual property rights, unless such material is made available under a licence (such as Creative Commons) that permits such use.

- 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.). They must also give appropriate credit when referring to others' hypotheses, theories, or opinions.

- 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 that connection.

During ICT lessons, pupils are provided with information concerning the respect for intellectual property rights so that they can start to learn how to discern about what is legal and illegal.

[1] In computing, a **Virtual Private Network, VPN** for short, is a system allowing a direct link to be created between remote computers, by isolating this traffic in a tunnel.

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

All pupils are expected to use digital tools in a way that respects the dignity, wellbeing, and rights of all members of the school community.

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. Pupils are encouraged to report any cyberbullying to a trusted adult or staff member, while the School will support all parties involved, taking a restorative and educational approach where possible. The school's Anti-Bullying Policy should be followed
- Using other people's lists of email addresses or personal data for purposes other than those intended by pedagogical or educational objectives and in accordance with data protection regulations.
- 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 and not a right.
Use of the pedagogical Internet-based network is for the sole purpose of teaching and learning activities corresponding to the European Schools' missions.

Pupils are strictly prohibited from:

- Connecting to live chat services or to discussion forums unless otherwise authorized by a member of the educational team, on account of their pedagogical purpose, or to social media,
- Sharing personal information allowing the pupil's identification (first name, surname(s), email, address, etc...),
- Accessing websites with pornographic content or material promoting hate, discrimination, or violence based on race, ethnicity, religion, sexual orientation, or other personal characteristics, downloading or installing any software or application whatsoever.
- Downloading or installing any program whatsoever, including access to videogame websites.

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 and/or someone else's personal data.

Pupils are strictly prohibited from using the email address linked to their O365 account (...@student.eursc.eu) to create accounts on any applications, websites or software not authorized 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 will use a supervision and assistance system to ensure that pupils are engaged in a continuous learning process and to allow the people responsible for the course in question and the library staff to help pupils directly from their workstation.

Only persons authorized by the Management may use the supervision and assistance software and they are required to comply with the IT Charter applicable to their role in the School.

This system allows:

- Pupils' screens to be accessed remotely to help them and to keep them focused on their tasks,
- Teaching to be more effective, by displaying the screen of the person in charge of the lesson to the class,
- Pupils' screens to be selected to present their work,
- All pupils' screens to be deactivated to capture their attention.

No recording of their session or of their activity is made.

4.3 Social media

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

Reuse of password used for the MS365 account in other systems, websites and applications is strictly prohibited.

Use of a private digital device (telephone, tablet, laptop) does not exempt pupils from following the rules for their proper use and good behavior 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.

4.3 Artificial Intelligence

Artificial intelligence (AI) refers to the capability of computational systems to perform tasks typically associated with human intelligence, such as learning, reasoning, problem-solving, perception, and decision-making. Generative AI can process content (analyse, transform, or create) based on user input, generally in a conversational manner.

- Pupils can access web-based AI tools using their school-linked email address (...@student.eursc.eu) only when explicitly authorized by the school.
- If AI is used outside school for homework or projects, pupils must remain honest and transparent, in line with the school's policy or the course-specific guidelines.
- Pupils must use AI tools in a responsible and legally compliant way, by protecting privacy and confidentiality, respecting intellectual property, being accountable for any AI-generated content they use, and using such tools thoughtfully given their environmental impact.

5. SPECIAL RULES CONCERNING ONLINE LEARNING/ TEACHING

Online teaching and learning may be decided upon for specific reasons by the school management. When this occurs, certain rules apply.

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

- **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 specific situations decided upon by the school management.
- **Online learning or** teaching involves voluntary use of the camera by either teacher or student. It is obligatory that the audio is switched on, but the use of camera is a personal choice. It is clear that communication is more effective if teacher and student can see each other, but the choice of camera operation remains with the individual.
- **Online teaching and learning** involve only the teacher and students in the process and there can be no third-party participation/observation/evaluation in the lesson unless it is approved by the teacher concerned.

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, bully, defame or threaten other people.

The right to control the use of one's image is recognised for all members of the school community, which is why the School will not tolerate the use of images/videos taken without the knowledge or consent of the persons concerned.

A student, upon instruction from their teacher, needs to have the consent of a person to use their data (e.g. photos, names, etc) for any publication to take place.

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.
- any activity that compromises a student/staff/s integrity (e.g. knowledge of a peer uploading defamatory photos).

7. DATA PROTECTION

The School undertakes to process personal data collected in the context of the use of IT resources in strict compliance with the General Data Protection Regulations and the School's privacy statement.

If you have any questions regarding the processing of your personal data under this Charter, please contact the School's Data Protection Officer at the following e-mail address:
✉ : IXL-DPO-CORRESPONDENT@eursc.eu

8. 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 is allowed 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.
The school's Mobile Devices Policy must be respected.

9. SANCTION 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 School's own rules, as well as 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.

10. REVIEW

This Charter will be reviewed in the light of reviews carried out by the Office of the Secretary-General.