Pedagogical Development Unit
ICT and Statistics Unit

Ref.: 2025-08-D-25-en-1

Orig.: EN

CHARTER FOR USE OF IT RESOURCES AND DEVICES BY PUPILS OF THE EUROPEAN SCHOOL

Annex to MEMO 2025-08-M-1

Table of Contents

Schola Europaea

Office of the Secretary-General

Charter for the use of ICT resources and devices by pupils of the European Schools

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 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.

1. IT RESOURCES AND DEVICES

1.1 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*[1] *provided by the latter.*

1.2 Golden rule

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

1.3 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 ICT 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 ICT 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 Microsoft 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.
- to the school's Wi-Fi on personal device for the students eligible to BYOD.

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 (except for the pupil's legal representatives). However, **the legal representatives of the pupils are strictly prohibited to use the ICT resources provided to the pupils for any other purposes then 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 their workstation, the pupils must always ensure that they have logged out properly.

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

2. GENERAL RULES OF GOOD BEHAVIOUR

2.1 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 provided 5 Microsoft 365 installation licenses for computers and/or smart phones and tablets. These licenses 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.

2.2 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**.

2.3 Respect for the network and for workstations

Scrupulous respect for the premises and the hardware must be shown. Computer keyboards, mice and screens 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. Students must not deliberately block lockers with free electronic padlocks reserved for charging BYOD devices.

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[2] tunnels.

2.4 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, unless such material is made available under a licence (such as Creative Commons) that permits such use,
- Plagiarising, i.e. reproducing, (re)disseminating, or communicating to the public, in any form whatsoever and via any medium (e.g. tables, graphs, equations, legal texts, images, written texts), any content protected by intellectual property rights (such as copyright). 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.

[2] 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 sort of tunnel.

2.5 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, pornographic, or discriminatory nature, whether based on racial or ethnic origin, political opinions, religion or philosophical beliefs, state of health, or sexual orientation.
- bullying others (cyberbullying[3]), whether 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.
- using others's email address lists or personal data for purposes other than those intended by pedagogical or educational objectives, and in accordance with data protection regulations.
- using inappropriate language in emails, posts, chats or any other means of communication (the message's author has sole responsibility for the content sent).
- damaging the reputation of a member of the school community or the School 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.

3. SPECIAL RULES FOR USE OF THE INTERNET

3.1 Use of the School's network

Access to the Internet within the European School is a privilege, 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 authorised by a member of the educational team, on account of their pedagogical purpose, or to social media,
- sharing personal information that could lead to the identification of a person (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.

[3] Cyberbullying includes repeated or intentional harassment, threats, exclusion, or humiliation of others through digital means, such as messages, social media, images, or videos.

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 MS365 account (…@student.eursc.eu) to create accounts on any applications, websites or software not authorised by a member of the educational team or by the School's Management.

3.2 Supervision and assistance during sessions for pupils in the School

The School will use a supervision and assistance system to support pupil engagement 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 authorised by the School 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.

3.3 Social media

Pupils are prohibited from connecting to social media with their email address linked to their MS365 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 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.

3.4 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 authorised 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.

4. SPECIAL RULES CONCERNING ONLINE LEARNING / TEACHING

Online learning or teaching requires compliance with the rules for appropriate use and good behaviour set out in this Charter, whether in the context of:

- Blended learning: online learning or teaching at school, using digital resources approved by the School's Management or doing asynchronous activities (e.g. homework);
- Distance learning: when online lessons take place while the School is closed;
- Hybrid learning: when some pupils attend lessons in person and others take part online.

The following actions are prohibited:

- Photographing and/or filming teachers or pupils participating in online learning using personal devices, and especially the publication of such images or videos,
- Participating in online learning or teaching sessions without having been expressly invited to attend,
- inviting hers 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 others.

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

5. REPORTING TO THE EDUCATIONAL/ICT TEAM

The pupil 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.

6. 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 (2014-03-D-14).

Any pupil who chooses to bring a mobile phone or other digital 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 a 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.

7. 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 (2014-03-D-14) 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.

8. REVIEW

This Charter will be reviewed again at the latest in the school year 2027/28.