Electronic Device Policy

European School of Bergen | Secondary Cycle

September 2024

Contents

IT Charter

The Office Secretary-General (OSG) provides a revised, harmonized IT charter for the pupils across all European schools.

The Charter is the outcome of a consultation process including the external and internal legal services of the OSG, the OSG Data Protection Officer, the Pedagogical Development Unit, the ICT Unit and the representatives of the Directors and school Data Protection Officers.[1]

The IT Charter is the backbone of our Electronic Device policy.

What you will find below are school-specific addendums for the European School of Bergen.

Highlights | Code of Conduct

The golden rule is that the European School's IT resources (i.e. laptops, tablets, servers, printers, etc.) are intended to be used solely for pedagogical activities.

Some measures we would like to highlight from this IT Charter:

- Access to the internet within the European school is a privilege and not a right.
- It is forbidden to make an account on websites with your email address from the school.
- Students can only access apps and software which have been approved by the school.
- School accounts are personal and may be used only by the pupil concerned.
- The school account has a normal and decent picture of the student's face and his/her legal name.
- Students can't damage the hardware (i.e. no food/drinks when using laptops or computers).
- Students can't damage or interfere with software (i.e. deliberately interfering with the network's operation or subverting protection systems, etc.)
- It is forbidden to download or make illegal copies of material protected by intellectual property rights.
- Plagiarizing is forbidden. Sources should always be included.
- It is forbidden for students to access, display, publish or exchange defamatory, abusive, extremist, xenophobic, antisemitic or pornographic content within the school community, whether based upon racist, ethnic, political religion philosophical beliefs, state of health or sexual orientation.
- Intentional damage to the school's devices and IT resources may result in disciplinary sanctions and repair costs for the legal representatives[2].

The student must inform staff in the event of a problem with his/her account and/or loss, theft or compromising of his/her school account or any suspicious software or device.

[1] The general IT Charter can be consulted here or in Annex 1.
[2] In accordance with Article 32 of the General Rules of the European Schools.

Bring Your Own Device

The Bring Your Own Device (BYOD) policy provides guidelines and expectations for students bringing personal electronic devices to school for educational purposes.

Every student develops digital competences in his/her European School education to foster confident, critical, responsible and creative use of and engagement with digital technologies for learning.

Devices should be charged when students come to school.

Students who choose to bring a device to school do so at their own risk. They are personally responsible for the safety of their device.

Usage of devices per year level

Cycle-level	Device type	Distribution	Configuration	Ownership
S1 – S3	Laptop or computer	Devices can be booked by teachers in the library or in the ICT rooms. Computer can be used by students in the library, the study hall or the ICT rooms		School
S4 -S5	Laptop, tablet, or computer	Every student must possess his/her own laptop Computer can be used by students in the library, the study hall or the ICT rooms	Laptops can only be used for schoolwork in the library, canteen, or study hall	Student School
S6 - S7	Laptop, tablet, or computer Mobile Phones	Every student must possess his/her own laptop Computer can be used by students in the library, the study hall or the ICT rooms	Laptops can only be used for schoolwork in the library, canteen, or study hall See Point 'Mobile Phones'	Student School

Choice of the BYOD tool

The parents are free to choose a device, but it is advisable to choose a laptop or tablet with the following specifications:

- Operating system: Windows 10,11 or Mac OS X
- Android devices and/or Chromebooks are not recommended because they do not support all the software in use in school.
- Connections: Integrated Wi-Fi, Minimum 2 USB-A port, or integrated USB-C port with adaptor for USB-C to USB-A
- Processor: recommended at least Intel Core i3 10th gen or AMD E2/A4 Dual Core, equivalent or better
- Memory: At least 8GB RAM and at least a 256 GB hard drive and/or an SSD is recommended
- Screen: At least 10.8 inch, a maximum of 15 inch.
- Touch screen and stylus pen are strongly recommended.
- Battery life: A long battery life and/or spare battery
- Keyboard: Integrated or external
- General: Lightweight, for ease of transport and use, a protective case, virus protection and a PDF reader should be installed
- Note: Office 365 can be used free of charge by using the school account

Software that needs to be installed:

- Every student has a license to install Microsoft Office 365 on at most 5 different devices. (If needed, ask the teacher for help with installing the software)
- Virus protection
- PDF reader (e.g. Acrobat Reader)
- Teams
- OneNote

Network Access

Students must connect their devices to the school's Wi-Fi Network, which is filtered and monitored for educational purposes. Any attempt to bypass security measures or access unauthorized websites is strictly prohibited.

Privacy

Students are responsible for protecting their personal data. Therefore, access codes and access to network accounts are confidential and should not be shared. Any breach of privacy should be reported to the ICT department.

Students are also responsible for respecting the privacy of others. **We demand therefore that cameras on all students' devices are covered while being on school campus.**

Discipline

Students who (attempt to) violate the rules and guidelines set out in this BYOD policy are subject to disciplinary consequences. Staff have the right to confiscate devices temporarily for investigation purposes if there is suspicion of a violation.

Calculators

Cycle-level	Device type	Distribution	Configuration	Ownership
S1 – S4	Basic calculators	By parents	Teachers	Student
S5 – S7	Numworks calculator *Students who possess a different calculator and meet the conditions of the OSG, should be ready to discover it independently*	By parents	Normal mode during lessons Exam mode during tests and examinations	Student

Headphones and air pods

Only S4, S5, S6 and S7 students can bring a headphone or air pods to school. **Headphones or air pods can only be used in the library, outside school buildings and aula while studying or during free periods.** In all other locations, headphones or air pods must be put away in their bags or their locker.

Cycle-level	Device type	Configuration	Location	Ownership
S1 – S3	No headphones or air pods			
S4 – S5	Headphones and air pods allowed	Only connected to laptop or computer while studying	Library, aula, outside	Student
S6 - S7	Headphones and air pods allowed	Connected to phone or laptop	Library, aula, outside	Student

Social media

On school premises and during lessons students are not allowed to access social media. Only under the supervision of a staff member, students can post school related content on the social media of our school (website, Instagram, Linkedin, etc.).

As a European school we must implement the national regulations of the Netherlands. We want parents to be aware that some social media platforms have a legal minimum age. For example, Facebook, Instagram, Tiktok, Youtube, Snapchat, etc. children must be 13 years or older. For Whatsapp, the minimum age is 16 years old.[3]

During school trips, specific arrangements for the use of mobile phones and social media will be communicated by the school trip coordinator. No photos should be posted on social media, including Whatsapp.

Mobile Phones

Cycle-level	Device type	Rules	Location
S1 – S5	Mobile Phone or Smart watches	Not allowed on school premises	Storage: locker Switched off or on silent mode
S6 - S7	Mobile Phone or Smart watches	Allowed for pedagogical purposes inside the classroom. Allowed for music, studying and homework. It is strictly prohibited at all times to film, take, distribute or share pictures on school premises. *Exceptions: school project with written permission of a teacher or an approval by school management.*	Classroom Aula, library, study hall and outside the school buildings

The school is not responsible for smartphones or other electronic devices pupils bring to school.

[3] More information : https://www.kinderombudsman.nl/leeftijdsladder or https://www.kliksafe.nl/blogs/mediaopvoeding/hoe-oud-moet-mijn-kind-zijn-voor-social-media/

Consequences of (mis)use of mobile phones

In the case of violation of this policy, the following measures will be taken.

Type	Consequence(s)
Use of phone or smartwatch when or where this is not allowed	1 X = verbal warning 2 X = phone confiscated until end of school day + student copies smartphone policy (handwritten) 3 X = phone confiscated until end of school day + parents informed More than 3 times = phone confiscated until end of school day + parents need to pick up the phone at security
Repetitive use of phone or smartwatch when or where this is not allowed	The consequence will be tailored to the individual student depending on previous and current disciplinary measures. Example: detention, red school pass, etc.
Having your phone with you and/or use of Mobile phone or Smartwatch during a test or exam	This will be seen as an attempt of cheating. The student will receive a zero for the test.
Taking pictures/selfies on school premises Recording/filming on school premises *with* knowledge of people involved	1 X = phone confiscated until end of school day + student copies smartphone policy (handwritten) 2 X = phone confiscated until end of school day + parents informed 3 times or more = phone confiscated until end of school day + parents need to pick up the phone at security The consequence will be tailored to the individual student depending on previous and current disciplinary measures. Example: detention, red school pass, etc.
Recording/filming on school premises *without* the knowledge of people involved Hate speech/cyberbullying on school-related platforms (Teams, SMS, Mail, etc.)	Possible consequence(s): - Detention - Internal exclusion with reflective task - Official warning letter - Discipline council The consequence will be tailored to the individual student depending on previous and current disciplinary measures.
Hate speech/cyberbullying on social media (not on school-related platforms)	The victim's parents are advised to file a complaint at the police station and there is a guidance track at school.

Annex I: IT Charter

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.

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.

The pupil is only allowed to access apps and software which have been approved by the school, and should check with a member of staff in case of doubt.

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. 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 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 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.

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),
- subverting or attempting to subvert the protection systems installed (firewall, antivirus programs, etc.),
- using VPN tunnels.

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 that connection.

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 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 authorised 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 pornographic, xenophobic, anti-Semitic or racist sites,
- downloading or installing any program whatsoever.

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 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 authorised 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).

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.

The only time when social media apps (including WhatsApp) should be actively used for school related activities is when pupils are on school trips, and on instructions from the accompanying teachers. The rules are laid out relating to the GDPR.

No photos should be posted on social media/WhatsApp.

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, 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.