École européenne de Bruxelles IV (Laeken)
European School of Brussels IV (Laeken)

WHOLE SCHOOL POLICY

CHARTER FOR USE OF IT RESOURCES AND DEVICES BY PUPILS

CREATION: 01-09-2020

LAST REVISION: 12-07-2022

VALIDATION: Approved by the SAC (meeting on 23 June 2022)

DIFFUSION: School Community

TABLE OF CONTENTS

CHARTER FOR USE OF IT RESOURCES AND DEVICES BY PUPILS

1. Preamble

The European Schools endeavour to offer pupils the best possible working conditions in terms of IT and multimedia services. This Charter (hereafter “the ICT 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 School’s internal Rules (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, WIFI connection for use of the Internet in the School premises and remotely, as well as 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 and educational 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. The School reserves the right to revoke this privilege if need be.

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 ’s IT Department monitors the School’s network traffic to verify that IT resources and school-owned devices are being used in compliance with the provisions of this ICT Charter[2].

[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).

[2] The conditions of such monitoring are laid out in Article 9 of this ICT Charter.

Use of the IT resources and devices at school or remotely at the request of a teacher 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 and workstations,
- 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,
- To a WiFi connection, as suitable and in accordance with educational needs.

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 present rules of good behaviour when using the resources and devices made available by the School for pedagogical and educational 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, screens, workstations, equipment 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[3] tunnels or tools enabling to create VPNs.

[3] 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.

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, work, text or data irrespective of the medium (table, graph, equation, article of a legal act, image, text, hypothesis, theory, opinion, etc), which are 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 (see the School's Anti-Bullying Policy).
- Using other people's lists of email addresses or personal data for purposes other than those intended by pedagogical or educational objectives.
- Using improper language 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. While the School encourages debate and fosters critical thinking, pupils are reminded that freedom of speech is not absolute and should therefore be exercised within the limits set out by the relevant regulations and with due regard to the rights and freedoms of others.
- 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 or to social media 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 or any sites spreading discrimination or hate speech towards other communities.

  Pupils are reminded that racism is an attitude of systematic hostility or contempt for particular individuals or groups of individuals based on their nationality, skin colour, origin, national or ethnic origin[4]. Aside from race, the law also prohibits discrimination based on other grounds such as: gender, political/religious beliefs, sexual orientation, language and disability[5].
- Downloading or installing any program whatsoever, unless otherwise authorised by a member of the educational team, on account of their pedagogical purpose.

Unless otherwise authorised by a member of the educational team, pupils should under no circumstances mention their name, display a photo, mention their address, telephone number or any other information facilitating their identification on the Internet while using the School’s IT resources.

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 et assistance de la session des élèves dans l’École

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.

[4] Article 4, 4°, of the *Act of 10 May 2007 amending the Act of 30 July 1981 punishing certain racist or xenophobic acts.*

[5] For a complete list of the discriminatory grounds, please refer to the *Law of 10 May 2007 to combat certain forms of discrimination.*

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) remotely or in school premises 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. Cyber-bullying is subject to disciplinary sanctions.

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 ICT 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’), in particular 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.

Online learning or teaching involves voluntary use of the camera by either teacher or pupil. It is obligatory that the audio is switched on at the teacher’s request, but the use of camera is a personal choice. It is clear that communication is more effective if teacher and pupil can see each other, but the choice of camera operation remains with the individual.

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. The invitation of parents/legal representatives in primary during distance learning should be accepted as a rule.
- 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 pupil or his legal guardian 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

This reporting should be carried out using the following e-mail address: LIST-LAE-ICT@eursc.eu.

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.

Any questions regarding the processing of pupils’ personal data under this ICT Charter can be addressed to the School's Data Protection Officer at the following e-mail address: LAE-DPO-CORRESPONDENT@eursc.

8. Responsibility

the legal representatives of the pupils concerned, in accordance with Article 32 of the General Rules of the European Schools. Other legal consequences may follow, including appearance before the School’s disciplinary councils.

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. For devices brought under the School’s BYOD policy, pupils should exert special care.

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. The school will pursue and sanction all cases of such intentional damage or theft for such devices.

9. Monitoring

The IT administrator [6]must constantly ensure to his/her satisfaction that IT resources are operating properly and being properly used. To that end, monitoring of the School’s network traffic and of the mac-addresses connecting to the Edu Wi-Fi as well as the school-owned devices allow for anomalies to be detected (e.g. abnormal use of the network, excessive amount of storage space, attempted cyberattack, malicious program, etc.)

Should anomalies be detected, the IT administrator will approach the School's Director 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 School’s Director.

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 impact 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, equipment and premises
- Compliance in good faith with the principles and rules for use of the technologies, equipment material and devices available, and with this Charter.

10. 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, when applicable, the sanctions and criminal proceedings provided for by Belgian law.

[6] At School, each member of the IT Department is an IT Administrator.

The use of sanctions must be reasonable and proportionate to the circumstances of the case. In that regard, the seriousness of the pupil’s misconduct shall be assessed on the basis of factors such as the pupil’s age, intentionality, repetition of the breach or lack of respect for the members of the School community.

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.

11. Review

This Charter will be reviewed in the light of the experiences gained in the 2022/2023 school year.