

# BYOD<sup>1</sup> policy of the European School of Varese

## Table of Contents

1. INTRODUCTION.....	2
2. ACCESS TO THE SCHOOL'S NETWORK.....	2
3. CONFIDENTIALITY.....	2
4. ACCEPTABLE USE POLICY.....	3
5. DEVICES AND SUPPORT.....	3
6. SECURITY.....	4
7. RISKS AND LIABILITIES.....	4
8. PENALTIES.....	5
9. PROTECTION OF PERSONAL DATA.....	5
10. SIGNATURES.....	5

---

<sup>1</sup> Bring Your Device

## 1. INTRODUCTION

The European School Varese, in accordance with the “Bring-Your-Own-Device Policy” of the Central Office, wishes to clarify what may or may not be considered as an acceptable use of the devices pupils of S5 are requested to bring to school as of school year 2020 - 2021. The present BYODP outlines the rules for the proper use of personal devices from an ethical and legal point of view. It is also meant to protect the security and integrity of the School’s data and technology infrastructure.

This policy constitutes an annexe to the internal rules of the School and is part of the binding regulatory framework to which students are subject. For it, the term "device" refers to a mobile digital device (tablet or laptop computer) which can be connected to the School’s Wi-Fi.

## 2. ACCESS TO THE SCHOOL’S NETWORK

Students may access the School’s network for pedagogical purposes only. It entails having access to:

- Internet and Wi-Fi.
- Office365 (including the e-mail service) managed by the European Schools.
- proprietary or open-source software.

Accessing the School’s network is a privilege, not a right. The School reserves the right to revoke this privilege if students do not abide by the rules outlined in the present policy.

Access codes are granted by and under the supervision of a member of the educational team.

## 3. CONFIDENTIALITY

Access to network accounts are personal and individual, and may not be shared.

Access codes are confidential, and may not be divulged to third parties, except for the student’s legal representatives. Students must report any problem they would encounter with their account to their education adviser or course-teacher.

As regards confidentiality, the following will be regarded as a breach of the present policy (it being understood that the list is not exhaustive):

- trying to find out another person’s password;
- logging in with another person’s username and password;
- opening, editing, or deleting the files belonging to another person and/or generally trying to access;
- another person’s account.

#### 4. ACCEPTABLE USE POLICY

Each student is personally responsible for his/her actions in accessing and using a device on the School's network. Failure to comply with the rules for acceptable use will result in disciplinary action, which may also include suspension of computer privileges, resulting in a failing grade for work requiring the device in class.

The School defines acceptable use of personal devices as school-related activities in connection with the mission of the European Schools. Students are blocked from accessing certain websites<sup>1</sup> during school hours/while connected to the School's Wifi network at the discretion of the School and are not authorised to connect to chat services, discussion forums, or social networks.

Devices may not be used at any time to illegal or harmful purposes.

The following list, though not exhaustive, specifies some of the conduct that violates the acceptable use of the device:

- intentional damage to hardware or software, or the creation or distribution of viruses, worms or other forms of digital mayhem;
- creating, displaying or transmitting threatening, racist, sexist, pornographic, abusive or harassing language or materials;
- storing or transmitting illicit materials;
- unauthorised use of a computer account or distribution of a password;
- plagiarism or intruding into other people's files;
- using electronic mail to harass or threaten others, including sending repeated, unwanted emails;
- to another user (this is in line with the School's anti-bullying policy);
- using e-mail lists or personal information for purposes other than those that are pedagogical;
- or educational in nature;
- giving your name, address, or phone number to anyone over the Internet;
- downloading and/or installing any software including, but not limited to, executable files;
- games, MP3 files or players, video files, zip files, where these are not authorized by a teacher authorised to connect;
- viewing a website/film which was not approved by your teacher or viewing a website/film not in line with instructions for your work during class.

#### 5. DEVICES AND SUPPORT

Smartphones (multifunction mobile phones) are NOT allowed to use in the BYOD-project.

Tablets and laptops which meet the school requirements and recommendations are allowed.

Connectivity issues will be supported in different levels:

- First level: the course-teacher
- Second level: Educational adviser
- Last level: System Administrator

Devices' camera and/or video capabilities must be disabled while on-site, except in the case of a request from teachers in the pedagogical framework.

## 6. SECURITY

In order to prevent unauthorised access, devices must be password protected using the features of the device. A strong password is required to access the School's network.

The School's password policy is:

- a) The access name is given by the school and cannot be changed.
- b) The password must be at least 8 characters long (better 12 characters)
- c) There must be at least one character from three of the following character groups in the password be included:
  - i. Capital letters (A-Z)
  - ii. Lowercase letters (a-z)
  - iii. Digits (0-9)
  - iv. Special characters (! "§ \$% & / () =? \* + - \_ #)

As regards security, the following is strictly prohibited policy (it being understood that the list is not exhaustive):

- installing software or making a copy of software present on the network;
- deliberately disrupting network operation, including the use of programs to circumvent;
- security or introduce malware (viruses, spyware or others);
- diverting or attempt to bypass protection systems in place (firewalls, antivirus...);
- using VPN.

## 7. RISKS AND LIABILITIES

Students maintain complete responsibility for their device. As stipulated in Article 34 of the General Rules of the European Schools: *“The school shall not be responsible for objects brought to school by pupils”*.

While the School will take every precaution to prevent the student's personal data from being lost, it is the student's responsibility to take additional precautions, such as backing up email, contacts, etc.

The School reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to the School within 24 hours. Students are responsible for notifying their mobile carrier immediately upon loss of a device.

Students are liable for all costs associated with their device.

Students assume full liability for risks including, but not limited to, the partial or complete loss of personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

The School reserves the right to take appropriate disciplinary action up to and including definitive exclusion for noncompliance with this policy.

## **8. PENALTIES**

Any student who violates the present policy will be subject to disciplinary proceedings as per the General Rules of the European Schools and the internal rules of the School, as well as penalties and criminal proceedings prescribed by law. Teaching staff will exercise strict control in order to ensure respect of the rules by the students they are responsible for.

## **9. PROTECTION OF PERSONAL DATA**

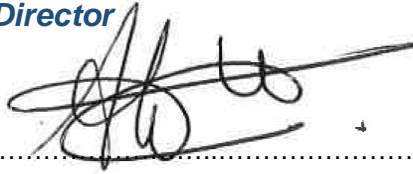
The School undertakes to process personal data collected in connection with the use of personal devices in strict compliance with the General Data Protection Regulation.

## **10. SIGNATURES**

The signature of this policy is mandatory for any student willing to connect a personal device to the School's network.

The school commits itself to provide the services mentioned:

For the School: **Ariane FARINELLE, Director**



Date and signature: .....25/09/2020.....

The student commits to respect the terms of this policy:

Surname and first name: .....

Date and signature: .....

Seen and read by the student's legal guardian:

Surname and first name: .....

Date and signature: .....