COGNITA

Florence Bilingual School

Policy on the Use of Information Technology Devices and Digital Security

Updated June 2023

1 Introduction

1.1. The use of technology as a tool has become an integral part of school life.
1.2. Cognita Schools are committed to the effective use of technology for teaching, learning, and school administration. They are also committed to protecting staff, students, parents and visitors from the dangers of misuse of technology. The school aims to develop pupils' autonomy and make them responsible for using electronic devices. Devices are taken home and to school daily by pupils in the secondary school and may be taken home at the discretion of the teacher in the elementary school.
1.3. The school actively promotes parental participation to help safeguard the welfare of students and to promote the safe use of technology.
1.4. This policy applies to:
- All technology devices and equipment connected to the school network.
- All technology devices provided by the school to employees and contractors, both on and off-site.
- All technology devices provided by the school to students through our 1-to-1 personal device programme, both on and off-site.
- All IT applications and services provided by the school for teaching, learning and administration.
- All computer applications and services available online and accessible through the school network
1.5. A copy of this policy is available to staff, students, parents and visitors upon request and on the school website.
1.6. If this policy and its requirements are violated, failure to read this policy will not be accepted as a defense/excuse.

2 Policy Objective

2.1 Promote responsible use of technology and information services by staff, students, parents and visitors.
2.2 Define the limits and possibilities of using the information technology and services offered by the school, both on and off site.
2.3 Define the responsibilities of all staff, students, parents and visitors.
2.4 Educate and encourage students to make the most of the educational opportunities provided by the use of technology in school.

2.5 Safeguard and promote the welfare of students by anticipating and preventing risks from:
- Exposure to harmful or inappropriate material (such as pornographic, racist or offensive material).
- Inappropriate contact by strangers.
- Cyberbullying and abuse.
- Copying and sharing of personal data and images.

2.6 Define Digital Filtering and Monitoring on school devices and school network.
2.7 Specify requirements for reporting misuse of technology.

3 Application of the Policy

3.1 This policy applies to all staff, students, parents, and visitors to the school.
3.2 This policy applies to all technological, IT, and communication devices, network hardware and software, as well as the services and applications associated with them, including:

- The school network, WIFI access, and internet access.
- Tablets, desktops, and laptops.

- Mobile phones, smartphones, and smartwatches.
- Audio, still image, and video devices (e.g., personal music players and GoPro devices).
- Digital displays and Interactive Whiteboards.
- Printers.
- Communication and collaboration applications (e.g., Outlook and Teams, Google Apps).
- Virtual Learning Environments.
- Mobile messaging apps (e.g., Snapchat and WhatsApp); and social media (e.g., Facebook, Instagram, TikTok).

3.3 This policy applies to the use of technology provided by the school both inside and outside of school premises.
3.4 This policy applies to any member of the school community.

4 Contacts

4.1 The main contact for any kind of technical problem, theft, loss, damage, questions and clarification is it@florencebilingualschool.it.
4.2 For any other information, reference should be made to the Front Desk of the relevant office.

5 Roles and Responsibilities

5.1 This policy document has been drafted and approved under the supervision of the School Director and the President's Council/Senior Leadership team. The School Council is informed of this.
5.2 The School Director is responsible for the publication of this policy and the implementation and ongoing monitoring of this policy.
5.3 Cognita's European IT Director is responsible for ensuring that IT technology and services are implemented and monitored in accordance with this policy.
5.4 All staff, students, parents, and visitors must comply with this policy.

6 Safe Use of Technology

6.1 The school is committed to the safe use of technology for teaching, learning, and school administration.
6.2 The use of technology must be responsible, respectful to others, and follow all legal aspects. Staff, students, parents, and visitors are responsible for their own actions, conduct, and behavior.
6.3 The school will support the use of technology and provide as broad access to the Internet as possible, balancing the educational needs of students, the safety and well-being of staff, students, parents, and visitors, and the security and integrity of our systems.
6.4 Monitoring and recording tools are in place to ensure the safety and security of staff, students, parents, and visitors.
6.5 For child and youth protection purposes, students' personal 1-to-1 devices are equipped with pre-installed monitoring software. The software provides real-time and historical data on device usage, such as web browsing.
6.6 We want students to enjoy the use of technology and become competent users, as technology has become a fundamental part of education, not only as a vehicle to provide excellent teaching and facilitate learning, but also as a platform for collaboration and productivity.
6.7 Students will be taught the importance of safe and responsible use of technology to help them protect themselves and others.

6.8 The school actively encourages the participation of parents to help promote their children's safe use of technology.
6.9 Any concerns regarding the unsafe or inappropriate use of technology should be reported to the school as soon as possible.
6.10 Any serious incident involving the unsafe or inappropriate use of technology should be reported promptly to the school, which will record and investigate the matter.

7 Right to Use School Network and Equipment

7.1 School employees and students will be given a user name and password to access the devices.
7.2 Some shared resources may have a generic username and password for access.
7.3 All school devices remain the property of the school. The school has the right to withdraw an assigned device or revoke access at any time.
7.4 School devices must be connected to the dedicated school network. Personal devices must be connected to the guest network only.
7.5 Any attempt at unauthorized access is prohibited.
7.6 School employees and students may be assigned devices for teaching, learning or school administrative purposes:

- Students who have been assigned a 1-to-1 device may use the device in classes under the direction of their teacher.
- School employees and students are responsible for the proper use and safekeeping of the device when it is taken off school premises.
- Devices and accessories provided by the school must be returned in good condition (subject to wear and tear from normal use) and fully functional.
- Staff and parents of students are responsible for the cost of repair/replacement of devices if they have damage caused by misuse or neglect. See item 16.
- Staff and parents of students are responsible for replacement costs of devices in case of loss of possession caused by misuse or neglect. See item 16.

7.7 The school provides additional devices in case there are special needs such as laboratories or extra activities.
7.8 School employees and students may not use or attempt to use computing devices and resources assigned to another person except when explicitly authorized.

8 Appropriate Use of Technology for Digital Security

8.1 The school provides access credentials to various platforms/devices to staff, students, and parents. For the safety of everyone, it is important to:

- Do not allow other people to use your account.
- Do not use someone else's account.
- Lock the device or log out of your account when not in use.
- Use only authorized school applications and email for official school activities and digital correspondence.

8.2 The school provides technological hardware and software to support the school's instruction and administration.
• Those using any school equipment or devices are required to take care of them and behave responsibly.
• School devices and equipment must not be taken off the school premises except in the following cases:
- The device is assigned to a staff member;

- The device is assigned to a student through the 1-to-1 programme;
- There is written authorization from a member of the School Board/Senior Leadership team.

• The school's technological equipment assigned to staff and students is the responsibility of the assignee.
• Portable devices should never be left unattended.
• Loss or damage to school devices must be reported to the school as soon as possible.
• Theft of a school device assigned to a staff member or a student through the 1-to-1 programme must be reported to the police and communicated to the school as soon as possible. See point 16.
• Abuse or damage to school equipment will incur the full cost of repair or replacement by the responsible party.

Not allowed:

• Attempting to install software on school-owned or provided devices without explicit approval from the school.
• Downloading or accessing illegal software.
• Downloading school network software to portable storage or personal devices.
• Attempting to copy or remove software from a school-owned or provided device.
• Attempting to alter the configuration of hardware or related software.

8.3 The school provides tools for data access and storage.

Not allowed:

• Accessing or attempting to access data for which authorization has not been granted.
• Damaging digital documents belonging to other users.

It is the responsibility of each individual user to ensure they do not violate intellectual property rights, including copyrights, trademarks, patents, design rights, and moral rights.

8.4 The school is committed to safeguarding its students and, as far as possible, mitigating all technology-associated security risks.

• **The school employs filtering systems to block access to inappropriate material**.
• Not allowed:
- Attempting to bypass filtering systems.
- Using software or resources designed to bypass filters and access blocked sites.

• The possibility of accessing inappropriate content on a school device or school network must be reported as soon as possible.
• The school has security systems in place to block and protect against computer viruses or other harmful software such as spyware.
• Concerns regarding viruses and other harmful software can be reported to the school, which will provide clarification and intervene to ensure cybersecurity.

8.5 It is the responsibility of all users to approach the online experience carefully and responsibly, for the well-being of themselves and others, both on personal and school devices.

• Cyberbullying: Students must not use computer tools to harm others.
• Strangers: Students must not use computer tools to contact or interact with unknown individuals.
• Sharing sexual images/videos: Students must not use computer tools to create or share sexualized content, including images, audio, video, and texts.
• Concerns regarding well-being associated with technology usage must be reported to the school as soon as possible.

8.6 The school provides appropriate access to the Internet and social media to support education and school affairs management.

• The Internet offers unprecedented opportunities to obtain information, participate in discussions, and collaborate with individuals, organizations, and groups worldwide to enhance skills, knowledge, and capabilities.

• The school actively supports access to the widest variety of available informational resources, accompanied by the development of skills necessary to filter, analyze, interpret, and evaluate encountered information.
• Staff, students, and visitors must not use a school device or school network to visit websites containing obscene, illegal, offensive, pornographic, extremist, or inappropriate material.
• Staff, students, and visitors must not use a school device or school network to access gambling sites.
• Staff, students, and visitors are responsible for reporting to the school any inappropriate material that may be accessed on a school device or school network so that it can be promptly blocked.
• Privacy of staff, students, and visitors must always be recognized and respected on websites and social media.
• Staff should not be in contact with any student under the age of eighteen on any social networking site or via personal smartphones.

9 Access to Assigned Devices and IT Content

School devices assigned to staff and students are intended for the exclusive use of the assignee. Student devices may contain a classroom management application that allows the teacher to monitor and view students' screens during class.
Cognita devices may have remote support applications that allow IT support staff to access the devices to provide remote assistance.
Cognita reserves the right to access an assigned device and monitor its use and content under special circumstances, including but not limited to:

- To identify and/or prevent crimes.
- To ensure system security (e.g., viruses, malware, hacking, or other risks).
- To investigate possible misuse, abuse, and/or illegal activities.
- To ensure the integrity of school devices and IT systems.

Data on a Cognita device or accessible through a Cognita device complies with Cognita's and the school's privacy policies.

10 Photos and Images

10.1 The school considers photos and videos as personal data. Written consent from parents is required to publish images or videos for external advertising purposes, such as on the website, and for internal purposes, such as in a yearbook or on a parent portal. Parents and guardians can revoke this permission at any time by informing the school's Administrative Team in writing.
10.2 The Cognita Code of Conduct for staff states that "Cognita does not allow the use of personal mobile phones and cameras by staff in the presence of students."
10.3 Staff, students, parents, and visitors are not allowed to use devices such as mobile phones, cameras, smartwatches, or digital recorders to photograph or record staff or students without their permission. Permission may be granted in writing by a member of the School Board/Senior Leadership Team for school-organized shows/events.
10.4 Parents are requested to adhere to the following when recording videos or taking photographs during school events: refrain from posting material about other students on public portals without the consent of the involved family. Selling or distributing recordings of events without the consent of those involved is illegal.

11 Use of School Equipment for Personal Use

11.1 School devices and computer systems are provided exclusively for school-related activities. If you choose to use the equipment or computer systems for personal use, please note that it will be at your own risk and may be considered a violation of the Digital Security Policy. Additionally, as indicated in Section 9 of this Policy, Cognita has the right to access and monitor the use of school devices, including personal communications that may have been made through such means.
11.2 Only approved software and applications may be installed on a school device.
11.3 School devices and network must not be used for illegal commercial activities.
11.4 Conducting private or financial transactions on shared equipment poses risks, and your personal data may not be secure.

12 Use of Personal Devices at School

12.1 Personal devices of staff are not authorized to connect to the school network except through the guest Wi-Fi network.
12.2 Students are not allowed to bring other personal devices to school, regardless of whether they are for educational purposes or not.

13 Procedures

13.1 School staff, students, parents, and visitors who have concerns or incidents related to any IT aspect must take the following actions:
- Immediately cease harmful activity.
- Refrain from disclosing the incident to others.
- Preserve evidence to facilitate potential investigations.
- Report the incident or concern to the school.

13.2 Any concerns regarding unaware or inappropriate use of technology or technology-related well-being should be reported to the school as soon as possible.
13.3 Access to inappropriate material and concerns regarding viruses and other harmful software on a school device or school network must be reported to the school as soon as possible.
13.4 Loss, damage, or theft of school equipment must be reported to the school as soon as possible; theft must also be reported to the police.
13.5 Students are responsible for the use of IT equipment both at school and at home; in case parents or guardians have concerns or are aware of an issue, prompt communication with the school is strongly encouraged to provide advice and support.
13.6 The school has the duty to report serious concerns/abuse to the relevant child protection authorities or the police, in compliance with legal requirements.

14 Network Access Revocation/Sanctions

14.1 Anyone found to violate this Policy may have their network access rights revoked and may be subject to further disciplinary action.
14.2 The school reserves the right to revoke network access at any time.
14.3 The school may inform the police or other authorities in case of suspected illegal activities.
14.4 The school takes its responsibilities regarding digital security and the use of technology by staff, students, parents, and visitors seriously and understands the importance of regularly monitoring, evaluating, and reviewing its policies and procedures.

15 Rules for Proper Device Use

15.1 Students and staff are responsible for the device assigned to them by the school.
15.2 Students and staff must use the device correctly, meaning that:

- The device must always be used on a table or desk and never on the floor, chair, etc.
- The device must not have stickers or other markings, except a small sticker (approximately 5 centimeters) with the student's name and must not, under any circumstances, be engraved, painted, or decorated.
- When the computer is not in use, it must remain inside the case provided to the student along with the device. In the case of the iPad, the cover must be closed.
- The device and case must be handled carefully and treated with respect.
- The device may only have applications and software allowed by the school. Students should only use educational websites approved by the school. If a student has doubts about the suitability of an application or website, they should seek guidance from their teacher.
- The device, when taken home, must be returned to school already charged.
- The device cannot be left unattended at school (e.g., under a desk or, in the case of school staff, in the teachers' room or on a shelf) but can only be explicitly handed to a front desk or the IT technician.
- The student can use headphones if authorized by a teacher.
- Staff and students can use an external mouse as long as it is compatible with the device. Any other external device must be approved by prior request via email to the IT department (it@florencebilingualschool.it).
- The use of external storage devices (USB, external hard drives) is not allowed.
- All devices must be connected to the "Cognita Students" Wi-Fi network while at school. Under no circumstances is the use of other networks allowed.
- Staff and students must not use a VPN under any circumstances.
- Staff and students must lock their device when leaving their desk, even for a short time.
- The use of passwords to access the computer and software must be strictly personal and non-transferable. Staff and students must ensure to keep their password confidential. If this password is compromised, it must be reported as soon as possible to the IT department.

16. Damage, Theft, and Loss

[To be read carefully]

16.1 Any issues or damage to the device, whether affecting its functionality or not, must always be promptly reported to the IT department via email (it@florencebilingualschool.it). Secondary school students can directly inform the IT department, but this does not exempt the family from making a written report.
16.2 If the device is damaged, and the student is responsible due to negligence, carelessness (including accidental), or if they have not adhered to the rules described in this policy, parents or guardians will be required to pay the repair cost up to a maximum total amount of €500. If the device is irreparably damaged, parents or guardians will be responsible for the full replacement cost. Each case will be assessed individually. Responsibility and associated costs may be contested, but the final decision lies with the school and cannot be appealed.
16.3 If the computer is lost, the student's parents or the employee must cover the full cost of replacement.
16.4 If the computer is stolen, the family or the employee must file a police report and provide a copy to the school. Regarding replacement costs, circumstances will be taken into account. If the theft is in no way attributable to the student, family, or employee, for instance, if it was stolen from a securely locked locker, the device will be replaced free of charge. If it was stolen due to negligence or carelessness, parents or the employee will be responsible for the full replacement cost.

16.5 If a device is lost or stolen, it must be immediately reported to the IT Department as it might be possible to locate the device.
16.6 Pens and chargers are accessories provided with Laptops/iPads, and if lost, stolen, or damaged (both deliberately or accidentally), the full cost of replacement will be borne by the family.

17 Device Distribution and Return

17.1 Device distribution occurs in the first weeks of the school year.
- Laptops are provided with a charger and protective cover.
- iPads are provided with a protective cover and an iPen. iPads are typically kept at school.
17.2 Devices may show minor signs of wear that do not affect their functionality.
17.3 For devices delivered to homes, staff, students, and families:
- will have one week to check the proper functioning and aesthetic integrity of the devices.
- If there are obvious defects or conditions that impair normal usage, they must report it immediately within the aforementioned week, and the school will arrange for a replacement.
17.4 The above does not apply if the device was already assigned to the student or employee from the previous school year.
17.5 Regular checks on the condition of the devices will be conducted throughout the year to ensure their status, efficiency, and durability.
17.6 Upon device return at the end of the school term, before the summer break, or for other reasons determined by the school:
- Devices must be returned in the condition they were provided in, except for signs of wear from normal use.
- Accessories must be returned in the condition they were provided in, except for signs of wear from normal use.
17.7 The return must be made to the front desk or the IT department technician, unless otherwise communicated by the school in writing. Specifically, the device cannot be left unattended at school (e.g., under a desk or, in the case of school staff, in the teachers' room or on a shelf). In case of abandonment at school and not being found, the loss will be treated as described in point 16 "DAMAGE, THEFT, AND LOSS."
17.8 All devices must be returned before the staff member or student leaves Florence Bilingual School, or the full replacement cost will be charged, unless otherwise indicated.

18 Malfunctions and Repair Procedure

18.1 In case a technical intervention is necessary, the staff member, student, or family can leave the device at the Front Desk of the respective location or with the IT department technician.
18.2 Under no circumstances should devices be left in other areas of the school (e.g., under a desk or, for staff, the teachers' room) or entrusted to third parties.
18.3 Following the initial assessment, if problem resolution requires an extended period, the staff member or family will be informed through official communication channels about the return/replacement times and procedures. The school may decide to provide a temporary replacement device for the duration of the repair. The device will be returned directly to the student or staff member, or it will be available for pickup at the Front Desk of the respective location.

18.4 For any inquiries or reports, the school's IT Department contact can be reached at it@florencebilingualschool.it