Family Digital Center

IT Charter

General section for all students

Foreword

This charter sets out the rules and expected behaviour for the use of technological equipment, whether provided by Collège Champittet or personal. It applies to all iPads, computers and other digital devices used on campus or connected to the school network.

The aim is to ensure the safe, respectful, responsible and innovative use of technology in order to promote learning and student well-being.

Vision

At Collège Champittet, technology is seen as a tool for learning and creativity, enabling students to:

- Develop their digital and critical skills,
- Interact and collaborate effectively,
- Prepare for an interconnected world where digital skills are essential,
- Adopt a responsible and ethical approach in their daily use of technology.

We want every student to become an informed digital citizen capable of combining innovation, safety, critical thinking and respect for others.

1. User rights and responsibilities

1.1. Digital citizenship

The use of technology comes with responsibilities:

- Respect netiquette rules (courtesy, respect, kindness).
- Use the Internet thoughtfully, checking sources and exercising critical thinking.
- Do not publish any content that is offensive, discriminatory, or likely to damage the image of others.
- Behave online in the same way you would offline.

1.2. Cyberintimidation

Any form of cyberbullying is strictly prohibited (harassment, exclusion, identity theft, dissemination of offensive content, image manipulation, deepfakes, etc.).

- Any violation of another person's physical, psychological, or moral integrity will result in sanctions.
- Cyberbullying may constitute a criminal offence and be subject to legal action.
- Online activities are monitored and recorded.

1.3. Plagiarism and intellectual property

Plagiarism and copyright infringement are serious offences that undermine academic integrity and respect for the work of others.

- Plagiarism (text, images, videos, music, code, generative AI) is strictly prohibited.

- Students must always cite their sources (author, website, book, AI, etc.) and comply with licences (Creative Commons, copyright, related rights).

- Simply copying and pasting content without citation constitutes plagiarism.

- The use of generative AI tools (Copilot, etc.) is only permitted if the student:
  o specifies that they have used AI,

  o verifies the accuracy of the information produced,

  o rephrases and integrates the content in a personal way.

- Any attempt to present work produced by others or by AI as their own will be penalised.

- Students must also respect the intellectual property of their classmates (not appropriating their work, projects, images or ideas).
- In an academic setting, respect for intellectual property is a way of developing academic integrity, an essential value at Collège Champittet.

1.4. At home

The use of technology at home must be supervised by families in order to maintain a balance between learning, leisure and personal life. The model family agreement on digital use is highly recommended (appendix to the website).

- Parents are encouraged to establish clear rules regarding screen time, particularly before bedtime.

- It is recommended that common areas (e.g. common areas such as the living room, dining room, kitchen, etc.) be prioritised for the use of appliances in order to promote transparent and responsible use.

- Families should make students aware of the risks associated with social media, online gaming and prolonged screen exposure.

- Students are encouraged to **disconnect from digital devices** at certain times of the day (mealtimes, family time, before bedtime) to maintain their wellbeing.

- Parents are encouraged to talk regularly with their children about their digital lives and how they use technology (games, social media, AI, influencers, etc.).

1.5. Digital footprint and environmental responsibility

Every online action leaves a trace: searches, posts, downloads, shares. Students must be aware that:

- Their digital footprint can influence their academic and professional future.
- Deleting content published online does not guarantee that it will disappear completely.
- Intensive use of digital technology also has an environmental impact (energy consumption, data storage in data centres).

Students are therefore encouraged to:

- Think before you post, comment or share.
- Prioritise respectful and useful digital practices.
- Avoid unnecessary storage of large files and remember to sort through your data regularly.

2. WiFi and cybersecurity

2.1. WiFi

- WiFi access is filtered and monitored to ensure educational and secure use.
- Bypassing filters is strictly prohibited.
- In the event of unjustified blocking, the student must inform the IT team.
- Abusive use of streaming (videos, music, online games) outside of an educational context is prohibited, as it overloads the network.
- The use of social media in class is strictly prohibited.

2.2 Digital security

- Do not download or open suspicious files, or install unauthorised software.
- Never share your login details, passwords or sensitive data.
- Use strong, unique passwords for each service.

Website for generating: https://www.lastpass.com/fr/features/password-generator

- Immediately report any attempts at phishing, identity theft or other suspicious activity.
- The use of unauthorised personal VPNs is prohibited.
- The student must lock their device (code, Face ID, Touch ID) to prevent fraudulent use.
- Sharing an Internet connection (hotspot) between students is prohibited unless specifically authorised by the teacher.

2.3 Data Protection

- Comply with Swiss data protection law (nLPD).
- Do not collect or disseminate other people's personal data without authorisation.
- Photos and videos taken on campus must respect everyone's privacy.
- It is prohibited to create or disseminate **deepfakes** or any modification of images/videos that could undermine a person's integrity.

2.4 Digital Responsibility

- Each student is responsible for their connection to the school network. They are responsible for any suspicious activity carried out under their account or device.
- Students must use the network solely for educational and constructive purposes.
- The use of hacking software, security bypassing software or cryptocurrency mining software is strictly prohibited.

3 Digital safety and wellbeing

3.1 Personal Security

- Never share your personal details (address, telephone number, financial information) without permission.
- Report any worrying content or behaviour to a trusted adult.
- Never agree to meet someone in person whom you have only met online.

3.2 Digital wellbeing

- Take care of your health by limiting screen time and taking regular breaks.
- Avoid excessive or inappropriate use (video games, social media during lessons, etc.).
- Maintain a balance between school, personal and digital life.

3.3 Prohibited activities

- Non-educational video games in class.
- Connecting to Apple TV or other people's devices without permission.
- Hacking, digital vandalism, spreading viruses or malware.
- Any illegal or unlawful activity.
- Activities such as scientific research, spell and grammar checking, exploring new fields, learning through play, and visiting museum or other cultural institution websites are encouraged.

4 E mails, platforms, and social media

The use of emails, learning platforms and social networks must always be within an educational and respectful framework.

Students must use correct and appropriate language in their communications, whether by email or via school tools. It is forbidden to share sensitive personal information by email or school messaging.

Sending unnecessary messages, spam or chain emails is prohibited. Similarly, clicking on suspicious links or opening files from unknown senders is a security risk and should be avoided.

On social media, students must bear in mind that anything they post can be found and may have an impact on their reputation, both now and in the future. Posts must therefore be respectful, responsible and in line with the values of Collège Champittet.

Finally, the school's official accounts and platforms must only be used in accordance with the instructions given by teachers or the administration.

5 Personal devices and iPads

The iPad and other personal or school-provided digital devices are considered educational tools. Each student is responsible for bringing their iPad to school every day, fully charged, so that they can use it in class.

The iPad must be handled with care and protected by the cover provided by the school. Any loss, damage or theft must be reported immediately to the IT department or the school administration. Misuse or non-educational use of the device, such as installing games, accessing social networks without authorisation, or viewing inappropriate content, will result in sanctions.

Students are also responsible for regularly backing up their files and work. To do so, they must use the solutions provided by the school, such as OneDrive or Showbie (primary). The school cannot be held responsible for any loss of data caused by a failure to back up.

Finally, personal devices connected to the school network must comply with the same rules as those provided by the school. Their use must remain in accordance with the charter in order to ensure a safe, responsible and learning-focused digital environment.

6 Software and applications

Applications installed by the school on iPads must remain in place to ensure their proper educational functioning. Students are not permitted to delete them or install software that has not been approved by the school. Similarly, it is prohibited to synchronise the iPad with a personal account or other iTunes accounts.

Students are required to keep their applications and iPads up to date in order to benefit from the latest versions, fixes and security measures. Regular checks may be carried out by the school to ensure that the device remains compliant with the charter and that no inappropriate or illegal applications have been installed.

In the event of a technical problem, the presence of unauthorised software or inappropriate applications, the iPad may be reset by the IT team. The school cannot be held responsible for the loss of data or documents that have not been backed up by the student prior to this reset.

7 Liability and penalties

Failure to comply with the charter will result in consequences commensurate with the seriousness of the situation. In the event of a breach, the student may be temporarily or permanently suspended from accessing the school's digital services, learning platforms or technological equipment.

Disciplinary measures may also be applied in accordance with the Collège Champittet's internal regulations. In most cases, a warning will be sent to parents to inform them of the inappropriate behaviour.

In the most serious situations – for example, in cases of cyberbullying, hacking, fraud or threats to the safety of others – sanctions may include temporary or permanent exclusion from the school. If a violation of the law is found, the school reserves the right to take legal action.

_____

Written by:

Ravivarman Kandasamy
IT Manager