FETTES COLLEGE
ICT Acceptable Use Policy (Student)

The policy below sets out the expectations of all users of the school's network. It applies to any device connected to the Fettes College network, including but not limited to laptops, tablets and mobile phones.

Student Safety

The school has a responsibility for the welfare of you and other students. In using the school's ICT system you agree:

1. The school may monitor your use of the ICT systems. This may include but is not limited to monitoring websites visited, emails sent/received and files stored.
2. You will keep your password private, never share it with anyone and never use anyone else's.
3. You will take care with whom you are communicating online and not disclose information about yourself or others.
4. To report immediately to your House Parent, tutor or teacher any unpleasant or inappropriate material or anything that makes you feel uncomfortable online.
5. Under no circumstances to use the school's system to access illegal or pornographic content, online gambling, peer to peer file sharing or for the purchase of illegal goods.
6. You must not use any software, VPN, proxy service, browser extension or other tool to bypass the School's filtering, monitoring or security systems, or in any way that could compromise the security or integrity of the School network and its ability to keep you safe.

Network Integrity

The network's primary function is to serve the educational needs of students in the school. In order to ensure it fulfils this in using the system you must agree:

1. Not to use the network for games or recreational video streaming during lesson times or prep.
2. You are responsible for the software, apps and browser extensions installed on your own device. You should only save, run or install software from legitimate and reliable sources.
3. You will not open attachments to emails from people/organisations you don't know.
4. You will not try (unless you have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
5. You should ensure you have adequate virus and malware protection on your computer. In the case of Windows machines, Windows Defender is on by default and should not be switched off.
6. You will immediately report to ICT Support if you suspect you have clicked on a suspicious link, opened a malicious attachment, or lost your device or login details.

Responsible Use

In using the school's system you must agree:

1. You will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
2. During lessons, you must only use apps and visit websites that your teacher has instructed you to use.
3. You will not attempt to access areas of the network for which you do not have permission.
4. You will be polite and responsible when you communicate with others. You will not use strong, aggressive or inappropriate language and should appreciate that others may have different opinions.
5. You will not take or distribute images of anyone without their permission.
6. You will ensure that you have permission to use the original work of others in your own work and attribute it as necessary.
7. You will not attempt to copy/download works where not permitted to by copyright.
8. You are aware that when using your school email you are a representative of Fettes College and as such the tone and content of your emails, whether internal or external, must reflect this.
9. You should not use computer systems, whether attached to the network or not, that bring the name of Fettes College into disrepute.
10. You will check work carefully before printing and only print as necessary. Work is retrievable from the printer via your unique print code. Instructions on how to retrieve your print code, should you forget it, are provided on Firefly. Any document with personal or confidential details on should be collected from the printer immediately.

Use of Smart Devices

Smart devices are defined as wearable technology capable of communication, data storage, or audio and/or video recording, including smart watches, smart glasses, fitness trackers, and smart rings.

1. Smart devices are not permitted during class tests, school exams, or public examinations.
2. Smart devices must not be used to access messaging services or social media during periods when mobile phones are not permitted.
3. Smart devices may not be used to record audio or video in lessons without the express permission of the supervising teacher. Recording elsewhere on site is prohibited unless permission has been granted by the House Parent and all individuals recorded have given prior consent.
4. Students should remove a smart device during a lesson if requested by a member of teaching staff.

Use of Artificial Intelligence

We expect students to use Artifical Intelligence safely and responsibly inline with the School's AI Charter.

- You must not submit AI generated work as your own, or use AI in a way that misrepresents what you have understood or produced independently. Its use must be in line with the School's Academic Honesty Policy.
- You must not enter personal information about yourself or others, confidential School information, or assessment material into AI systems unless you have been told to do so by a member of staff.
- You should treat AI as a tool that can make mistakes, and should check information carefully rather than assuming it is accurate.

Breach of the Policy

Breaches of this Acceptable Use Policy, depending on severity, could result in:

1. Loss of or restricted access to the school network/internet
2. Contact with Parents
3. Detention / Gating
4. Suspension /Exclusion
5. In the case of illegal activities, involvement with the police

Monitoring and Complaints

This policy is reviewed on an annual basis to evaluate its effectiveness and eliminate unlawful discrimination. Anyone who feels that the School has breached this policy should appeal in accordance with the School's Complaints Policy.

JJP, Director of IT
Updated June 2026
Review June 2027