



FELIXSTOWE
INTERNATIONAL COLLEGE
FRIENDSHIP THROUGH EDUCATION

Bring Your Own Device (BYOD) Usage Policy

Version Date:	July 2026 (see below)
Signed:	Principal
Review cycle:	1 year (usually)
Date of next review:	September 2026 (see below)

This version replaces the September 2025 BYOD Policy. It introduces the School's new filtering and monitoring system, which applies to all devices used for school work, including personal devices, from September 2026 (see Section 6).

Contents

Contents	2
1. Introduction and Aim.....	3
2. Roles and Responsibilities	3
3. Scope	3
4. Policy Statement	4
5. Definitions	4
6. Filtering and Monitoring (New from September 2026).....	4
7. Minimum Device Security.....	5
8. Guidelines for Use	6
9. Unacceptable Use	6
10. Use in School, Images and Recordings	7
11. Independent Study	7
12. College Liability: Damaged, Lost or Stolen Devices	8
13. Reporting.....	8
14. Sanctions	9
15. BYOD Permission	9
16. Network User Agreement.....	9
Appendix 1: Policy Summary	11

1. Introduction and Aim

The purpose of this policy is to ensure that all staff, pupils, parents and visitors of Felixstowe International College understand when and how personal devices may be used at school, and to establish guidelines that protect the safety of pupils, the security of school data and systems, and the privacy of all members of the school community.

Felixstowe International College uses technology as one way of teaching the skills, knowledge and standards of behaviour students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways, and the School strives to provide appropriate and adequate technology to support educational purposes. The Bring Your Own Device (BYOD) approach supports flexible learning by allowing selected personal devices on the school network.

The challenge is to achieve the right balance between appropriate use of devices for learning and the School's statutory safeguarding and security duties. This policy should be read alongside the Acceptable Use Policy. It aims to ensure that ICT facilities and the internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk.

Felixstowe International College has taken account of guidance issued by the Department for Education, including Keeping Children Safe in Education (KCSIE) and the DfE filtering and monitoring standards for schools and colleges, and guidance from the NCSC.

2. Roles and Responsibilities

- The Principal is responsible for approving this policy and for determining sanctions for misuse.
- The Designated Safeguarding Lead (DSL), with the IT Network Manager, is responsible for updating this policy, for ensuring it is followed, and for oversight of the School's filtering and monitoring provision.
- The IT Network Manager is responsible for registering devices, installing and maintaining the School's filtering and monitoring software, and managing network access.
- The Senior Leadership Team (SLT) and the IT Network Manager are responsible for monitoring pupil use of the network.
- All staff members are responsible for applying this policy, for the safety of school information, and for maintaining their own devices appropriately.
- Teachers have discretion to allow and regulate the use of personal devices in their lessons.
- Parents, carers and guardians are responsible for reading and agreeing to this policy with their child, for insurance of devices, and for decisions about which device their child brings to school (see Section 6).
- Visitors will only use personal devices for agreed purposes with relevant permission. They will not share information from personal devices via social media and will not keep school information indefinitely.

3. Scope

This policy applies to all staff, pupils and visitors who bring their own device onto school premises or use a personal device to access school resources from any location.

Students and staff are permitted to bring their own devices into school for educational purposes only. Devices must comply with this policy to be permitted access to the wireless network on school grounds.

Acceptable devices: laptops, netbooks, MacBooks, Chromebooks, tablet computers, and smartphones (boarders only).

Unacceptable devices: smartphones (day students), internet-enabled handheld games consoles, and any other internet-enabled devices not listed above.

Please note that from September 2026, the choice of device is also affected by the School's filtering and monitoring requirements described in Section 6. Parents of pupils using Apple iPads or iMacs should read that section carefully before the start of term.

4. Policy Statement

Staff and pupils are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the School's provision, all users are agreeing to this policy.

Before being set up as a user on the school network, all users are expected to read this policy and sign to accept its contents. For younger pupils in Key Stage 3, parents are expected to read the policy with them and sign alongside their child.

Student access to the School's wireless network is a privilege and not an entitlement. Users are responsible and personally accountable for their use and activity on the School's ICT systems. Any use that contravenes this policy will be dealt with under the standard disciplinary procedures and may result in removal as a user from the school network. This applies to both staff and pupils.

Access to the School's wireless network is filtered, monitored and logged in compliance with this policy and the Acceptable Use Policy. In using the network or any other school resources, users acknowledge and accept that the School may investigate inappropriate use at any time.

5. Definitions

In this policy, "device" includes laptops, netbooks, MacBooks, Chromebooks, tablets (including iPads), iMacs, smartphones, e-readers, USB storage devices and any other equipment capable of connecting to the internet, the school network or school resources in the cloud.

"Filtering and monitoring system" means the software and services the School uses to filter internet content and monitor device activity in order to meet its safeguarding duties.

6. Filtering and Monitoring (New from September 2026)

To strengthen the School's statutory safeguarding duties under Keeping Children Safe in Education and the DfE filtering and monitoring standards, the School is introducing a new filtering and monitoring system across school devices from the start of the autumn term 2026. Because our students bring their own personal devices rather than using school-supplied ones, this system must also be installed on personal devices used for school work.

6.1 Requirements

- All BYOD devices must have the School's filtering and monitoring software installed before they can be registered on the school network and used for school work.
- Installation will be arranged by the IT Network Manager as part of device registration.
- The software must remain installed, enabled and up to date at all times. Removing, disabling or attempting to circumvent it will be treated as a breach of this policy and will result in the device's network access being revoked.
- The device's MAC address (unique identifier) will be provided to the IT Network Manager, registered for identification purposes and added to the filtering system to enable wireless access.

6.2 Important information for Apple iPad and iMac users

The new system has been trialled successfully on most device types with no issues. However, on iPads and iMacs specifically, installing the required software resets the device to a school-only configuration, and any personal data or apps will be removed.

The School consulted other schools and its sector association before taking this step. Most schools avoid this issue by supplying pre-configured, school-only devices to students. As our students bring their own personal devices, we are not able to take this approach; however, a device enrolled in the system and used for school work only will be no different in practice to a device purchased through school.

Families who would like their child to keep an iPad or iMac for personal use have the option of purchasing a lower-cost Windows device for school use instead. Parents should decide before the start of the autumn term which option works best for their family, and are welcome to contact the School with any questions.

6.3 Why we filter and monitor

- Safeguarding pupils.
- Protecting school systems and data.
- Meeting legal and statutory duties.

7. Minimum Device Security

Any personal device used on school premises, on the school network or to access school resources must:

- Run a supported operating system version with the latest security updates installed.
- Have appropriate, fully functioning and up-to-date antivirus protection (Chromebooks are exempt as this is built into the operating system).
- Use a device lock (PIN, password or biometric).
- Have the School's filtering and monitoring software installed (see Section 6).
- Not be rooted or jailbroken, and not run software that compromises security.

Any device that does not comply with these requirements, or poses a security, safeguarding or operational risk, will be denied access until it is made compliant. The IT Network Manager may immediately restrict, block or remove network access for any device posing such a risk, without prior notice.

8. Guidelines for Use

Staff, students and parents/guardians participating in BYOD must adhere to the Acceptable Use Policy and all other relevant policies. Each teacher has the discretion to allow and regulate the use of personal devices in lessons. Users must not:

- Attempt to circumvent the School's firewall, internet filtering or monitoring systems, including through VPN (Virtual Private Network) apps, proxy servers or proxy websites. This includes accessing inappropriate material via 3G/4G/5G mobile networks.
- Continue to use an item of networking software or hardware after a member of staff has requested that its use cease because it is disrupting the correct functioning of the School's ICT systems.
- Attempt to deny ICT services to other users by deliberately or recklessly overloading access links or switching equipment.
- Introduce a virus or other harmful software to the School's ICT systems.
- Monitor data or traffic on the School's network or systems without the express authorisation of the owner of the network or system.
- Connect any network-enabled personal device to the school network without the express permission of the IT Network Manager, or connect any personal device to the wired network.

9. Unacceptable Use

The School expects all users to use the ICT facilities and the internet responsibly. Users must not use the School's ICT systems or the internet:

- For the creation or transmission of obscene, abusive, offensive or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- To access online gambling sites. If such action is found, serious action to safeguard the pupil will be taken, and this may also require a disciplinary response.
- To access gaming sites when not appropriate.
- To harass, bully or abuse any other person. Any such activity will be treated in the same way as physical bullying and will be subject to the anti-bullying policy.
- To corrupt or destroy other users' data, violate the privacy of other users, or disrupt the work of others.
- For the creation of material with intent to defraud, or the creation or transmission of defamatory material.
- For the creation or transmission of content that promotes extremist activity, including terrorism and weapons.
- To post any information on websites or social media that could cause any other member of the school community distress or bring the School into disrepute.
- For private financial gain, or any political or commercial activity.
- To copy or attempt to copy any of the School's software, copy the work of another user, or engage in plagiarism.

- To store any files in their personal storage area which require copyright permission where that permission is not held.
- To download, copy or attempt to install any software onto school computers.
- To deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network.

10. Use in School, Images and Recordings

Student use of the network will be monitored carefully by SLT and the IT Network Manager through the School's filtering and monitoring system. The purpose of personal devices at school is to support learning during lessons and broader learning during independent study. Using the device for other reasons, such as games, social networking or messaging, is not allowed.

- The use of devices in lessons is at the complete discretion of the teacher.
- Devices must have their volume set to silent inside school buildings and classrooms unless express permission has been granted by a member of staff.
- Devices may not be used to cheat on assignments, quizzes or tests, or for non-instructional purposes such as personal phone calls and text messaging.
- Devices must not be used to take video or photographic material of students or staff within school, unless it directly connects to the lesson being taught and is allowed by the teacher.
- Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after use (for example, after uploading to Google Drive). Recordings to be retained for further legitimate use should be stored securely on the school network.
- Photographs, video or audio recordings must not be published on blogs, social networking sites or elsewhere without the permission of the people identifiable in them.
- Devices must not be used to record people at times when they do not expect to be recorded, and must not enable a third party acting remotely to take photographs, video or audio recordings in school.
- Internet use on devices connected to the school network must be for research and appropriate educational purposes only. Failure to comply will result in removal of internet access or complete revocation of BYOD permission.

Artificial Intelligence (AI)

The use of AI tools on personal devices for school work is guided by principles of ethical use, data privacy and academic integrity. AI tools must not be used to upload personal or sensitive data, or to complete assessed work unless explicitly allowed by the teacher. Breaches will be treated as academic misconduct (pupils) or a disciplinary matter (staff).

11. Independent Study

Students may use personal devices in timetabled and supervised private study areas outside of lessons. Independent use must always be for educational purposes and not, for example, to play games or engage in social media. Times and places where independent use is permitted include timetabled study lessons and break times.

Students should not use their devices in transit between lessons or in corridors, minimising the chance of damage and disruption.

12. College Liability: Damaged, Lost or Stolen Devices

Users bring their own devices to school at their own risk. Devices are the sole responsibility of the student using them, and troubleshooting issues should be done outside of school. The only issue the School will assist with is initial connectivity (connecting to the network) and installation of the filtering and monitoring software; for any further issues, the device manual or manufacturer should be consulted. The IT Network Manager is not responsible for maintaining or troubleshooting student devices.

The School will not be responsible for:

- Devices that are broken, damaged, lost, stolen or malfunction while at school or during school-related activities.
- Storage or security of a personal device. As there are no secure storage areas unless the student has an allocated locker, it is the student's responsibility not to lose the device and the parents'/guardians' responsibility to ensure it returns home after school hours.
- Maintenance or upkeep of any personal device, including software updates, hardware upgrades or compatibility issues.
- Personal data or apps removed from iPads or iMacs as a result of installing the required filtering and monitoring software (see Section 6). Families should back up and remove any personal data they wish to keep before enrolment.
- Work saved locally to a device. School work completed on the device should be saved to the Student Drive so that it is backed up.
- Any charges incurred to bank accounts or credit cards linked to the device. It is the parent's/guardian's responsibility to remove such accounts or ensure the student does not use them without permission.

Any issues or concerns should be reported to the main office by telephone or email as soon as possible. Parents are responsible for adequate insurance cover for the device.

Charging

Personal devices must be charged prior to school and run on battery power while at school. Charging will not be permitted for health and safety reasons, as device chargers will not have been PAT tested (Portable Appliance Tested) for use in school. Chargers for boarding students' devices must be PAT tested.

13. Reporting

Any breach of this policy should be reported to the DSL or the IT Network Manager. If a personal device that has accessed school systems is lost or stolen, the user must report this immediately to the IT Network Manager so that appropriate steps can be taken to protect school data and accounts; access may be revoked or accounts reset as a precautionary measure.

This policy will be reviewed annually or following a significant incident.

14. Sanctions

The School is authorised to collect and examine any device that is suspected of causing technology problems, of being the source of an attack or virus infection, or of containing inappropriate content or material. Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct; if the device is locked, the student will be required to unlock it at the request of a school administrator. Failure to comply will lead to device removal and BYOD privileges being revoked.

The sanctions imposed on a pupil will vary depending on the severity of the misuse and are at the discretion of the Principal. For a pupil they may include:

- Removal of internet privileges for 24 hours.
- Removal of the privilege to bring your own device.
- Detention.
- Suspension.
- Exclusion.

Misuse of the ICT provision by a member of staff may result in disciplinary action being taken by the Principal, as set out in the staff handbook. Serious incidents may be referred to safeguarding or external authorities depending on severity.

15. BYOD Permission

Permission to bring a device into school will only be granted once a student's parent/carer reads and agrees to this BYOD Policy and other relevant school policies available in the student planner, and once the device has been enrolled in the School's filtering and monitoring system by the IT Network Manager (see Section 6).

By signing this policy, parents/carers are agreeing that their child understands and will abide by the policy and its guidelines, and that they understand the implications of enrolment for their child's device, including the reset to a school-only configuration on iPads and iMacs. They further understand that any misuse may result in the loss of network and/or device privileges as well as other sanctions. Please also refer to the Acceptable Use of ICT Policy for Staff and Pupils.

16. Network User Agreement

Users should strive to maintain appropriate bandwidth for school-related work and communications. All students will use the "FIC" wireless network and staff will use the "Staff Only" wireless network to access the internet. Printing from students' personal devices is not permitted.

I understand and will abide by the above policy and guidelines, including the requirement for the School's filtering and monitoring software to be installed on my device. I further understand that any violation or misuse may result in the loss of my network and/or device privileges as well as other sanctions. During the course of the school year, additional rules regarding the use of personal devices may be added.

Name of Student:

Signature of Student:

Parent / Carer / Guardian Signature (required for Key Stage 3 pupils):

Date:

Appendix 1: Policy Summary

Felixstowe International College allows staff and students to bring their own personal device(s) for educational use. The School provides the infrastructure and access needed to use personal devices safely and securely, but does not provide technical support for personal devices. The use of personal devices in lessons is at the discretion of the teacher.

By using the school network you agree that usage will be filtered, monitored and recorded. We monitor to safeguard pupils, protect school systems and meet our legal duties under Keeping Children Safe in Education and the DfE filtering and monitoring standards.

New from September 2026: all personal devices used for school work must have the School's filtering and monitoring software installed. On iPads and iMacs, installation resets the device to a school-only configuration and removes personal data and apps. Families who wish to keep an Apple device for personal use may provide a lower-cost Windows device for school use instead.

To assist you, please ensure that:

- Your device is fully charged before school – charging is not permitted in school (boarders' chargers must be PAT tested).
- Your device has the latest security updates, antivirus protection and a device lock applied.
- The School's filtering and monitoring software is installed and remains enabled.
- You do not take any video or photographs without express permission.
- You do not attempt to circumvent the School's security, filtering or monitoring, including via VPNs or proxies.
- You only have licensed software installed on your device.

What BYOD does not allow:

- No smartphones for day students.
- No access for devices without the filtering and monitoring software installed.
- No bypassing of filtering, monitoring or security controls.
- No printing or charging from personal devices.
- No games, social media or messaging – school work only.

The School is not responsible for damage, loss, theft, maintenance, lost data (including personal data removed during enrolment of Apple devices), or any financial loss arising from use of a personal device. Failure to comply with this policy will result in appropriate action in line with the School's disciplinary procedures.