Perryfields Enterprise Academy Trust

Bring Your Own Device Policy
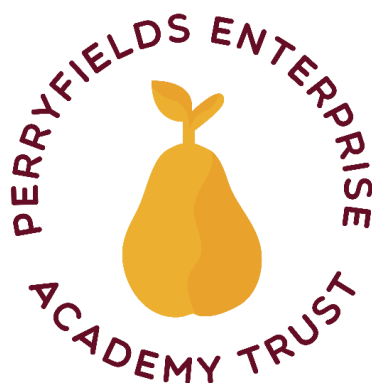
Adapted From:	SBM Services model policy
Reviewed:	March 2025
Approved By:	P.E.A.T Board
Approved Date:	27th March 2025
Review:	Annually
Next Review Date:	March 2026
Communicated to Staff	By: email Date: 28th March 2025

SUMMARY OF CHANGES – March 2025	
Section	**Detail**
Roles & Responsibilities	Reference to not using mobile phones for personal reasons by staff and visitors has been added.
Detailed Arrangements	Reference to not using mobile phones for personal reasons by staff and visitors has been added.
Security of staff personal devices	Removed that automated log on processes to store passwords must not be used.

CONTENTS

Bring Your Own Device Policy

Part 1 Introduction

Perryfields Enterprise Academy Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of guest devices.

- This policy applies to any/all non-school owned electronic devices, which access the internet via the school's network or to access school information. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'guest devices' in this policy.
- Guest devices include laptops, tablets, smart phones, USB sticks, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to WiFi and the Internet which is not school owned or on the school asset list, including staff personal devices. If you are unsure whether your device is covered by this policy, please check with the Data Protection Officer.
- This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of guest devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- The School reserves the right to refuse staff and visitors permission to use their guest devices on school premises.
- This applies to all guest devices connecting to school systems.
- This policy should be read in conjunction with the school HR advice and guidance. This policy does not stand alone, it is essential to follow the requirements set out in the PEAT Code of Conduct, Social Media Policy and ICT Acceptable Use Agreement, which provide more details.

Part 2 Organisational Arrangements

Overall Responsibility

The Board of Directors of Perryfields Enterprise Academy Trust (PEAT) is responsible for the approval of this policy and for reviewing its effectiveness.

Roles & Responsibilities

All staff are responsible for reading, understanding and complying with this policy if they are using their guest devices connected to the school Internet, or using guest devices to access information held on school systems.

If any person has concerns surrounding the use of guest devices, please contact the Headteacher or Designated Safeguarding Lead.

Staff, Directors and Governors will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of school information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.

- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- Staff must not store personal data about pupils or others on any guest devices, or on cloud servers linked to their guest accounts or devices.
- Report the loss of any device containing school information, or any security breach immediately to the Headteacher or Data Protection Officer.
- Ensure that no school information is left on any guest device indefinitely. Particular care must be taken if a device is disposed of / sold / transferred to a third party.
- Only use personal devices for work purposes when in front of pupils during the school day.

Visitors will:

- Familiarise themselves with this Policy.
- Only use guest devices for agreed purposes at the school and with parental or the relevant permission.
- Not share information from guest devices via social media and will not keep school information indefinitely.

Part 3 Detailed Arrangements & Procedures

Use of guest devices at the school and in front of pupils

Staff and visitors to the school may use their own devices in the following locations:

- In the classroom with the permission of the teacher.
- In the school environments e.g. libraries, sports pitches and outdoor spaces.

Guest devices must be switched off when in a prohibited area, and / or at a prohibited time, and must not be taken into controlled assessments and / or examinations unless special circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own device on school premises.

In line with the school's policy on the use of mobile phones, staff and visitors should not use their own mobile phone for personal reasons in front of pupils throughout the school day. This should empower staff to better challenge pupils to meet the school expectations and effectively enforce the prohibition of mobile phones throughout the school day.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own guest devices to take photographs, video, or audio recordings in school provided they have checked that parental permission has been received by the School. This includes people who may be identifiable in the background.

Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the school's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school network.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way 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 devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

Access to the schools' internet connection

The school provides a wireless network that staff and visitors to the school may use to connect their guest devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access for anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's network. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

Access to the school's systems

Staff are permitted to connect to or access the following school services from their device:

- The school email system.
- The school management information system.

Staff may use the systems to view school information via their guest devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their guest devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the school as soon as possible.

Staff must not send school information to their guest email accounts.

Monitoring the use of guest devices

The school may use technology that detects and monitors the use of guest and other electronic or communication devices which are connected to or logged on to the school's wireless network or IT systems. By using a device on the school's network, staff and visitors agree to

such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the Headteacher / Designated Safeguarding Lead as soon as possible.

Security of staff/governor/director guest devices

Any person wishing to use their own device must be aware that they have a direct guest responsibility for ensuring that the device they choose to use has the benefit of encryption or password protection. Staff must ensure that guest devices are set to lock with passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that appropriate security software is installed on their guest devices and must keep the software and security settings up-to-date.

Staff must ensure that passwords are kept securely and are not accessible to third parties.

Support

The school takes no responsibility for supporting staff's own devices, nor does the school have a responsibility for conducting annual PAT testing of guest devices. However, the school will support staff in ensuring that they have appropriate levels of security in place.

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, the Staff Disciplinary & Misconduct policy will be applied.

Incidents and reporting

The school takes any security incident involving a staff member's or visitor's guest device very seriously and will always investigate a reported incident. The school must be notified as soon as possible of any loss, or theft of a guest device that has been used to access school systems, and these incidents will be logged with the DPO. Data protection incidents should be reported immediately to the school's Headteacher or Data Protection Officer.