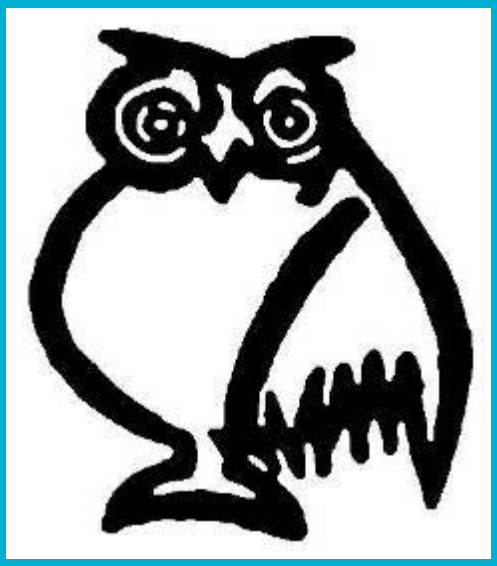
Danbury Park Community Primary School



Bring Your Own Device Policy

Last revision dated:	Summer 2022
This revision completed during:	Summer 2024
Agreed by the governing body:	11/07/2024
Next revision due:	Summer 2026

sbm services
school business management

Version History

V24.1	May 2024	Review of policy. In line with DfE guidance on the use of mobile phones by staff, the following changes have been made: 'Roles and Responsibilities' in section 2 - reference to not using mobile phones for personal reasons by staff and visitors has been added. Part 3 'Detailed Arrangements' - reference to not using mobile phones for personal reasons by staff and visitors has been added. Part 3 'Security of staff personal devices' - removed that automated log on processes to store passwords must not be used.

Bring Your Own Device Policy

Part 1 Introduction

Danbury Park Community Primary School recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices.

This policy describes how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Headteacher.

Part 2 Organisational Arrangements

Overall Responsibility

The governing body of Danbury Park Community Primary School is responsible for the approval of this policy and for reviewing its effectiveness.

Roles & Responsibilities

Staff members 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.
- Report the loss of any device containing school information, or any security breach immediately to the Headteacher who will report to the school's Data Protection Officer.
- Ensure that no school information is left on any personal 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 the use of personal devices at the school.
- Only use personal devices for agreed purposes at the school and with parental or the relevant permission.
- Not share information from personal devices via social media and will not keep school information indefinitely.
- Only use personal devices for work purposes when in front of pupils during the school day.

Part 3 Detailed Arrangements & Procedures

Use of personal devices at the school
Staff and visitors to the school may use their own devices in the following locations:

- In the classroom with the permission of the Headteacher.
- In the school environments e.g. school hall, playground, school field and outdoor spaces.

Personal 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 statutory tests 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 personal devices to take photographs, video, or audio recordings in school provided they have permission from the Headteacher and 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 the school's website or for use on *Tapestry*, the school's online Early Years Foundation Stage learning journey. 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 school's internet connection
The school provides a wireless network that staff to the school may use to connect their personal devices to the internet. Visitors are not permitted to connect to the school's network or internet without permission and access rights from the Headteacher.

Access to the wireless network for staff and visitors is at the discretion of the Headteacher, 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;
- Sonar;
- Tapestry;
- Curriculum related subscriptions.

Staff may use the systems to view school information via their personal 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 personal 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. Emails should not name individual pupils and any attached documents containing personal details of pupils, should be encrypted. 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 personal email accounts.

Monitoring the use of personal devices

The school may use technology that detects and monitors the use of personal 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 school as soon as possible.

Security of staff personal devices

Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted 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 personal 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. Automated log on processes to store passwords must not be used.

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 personal 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 personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the school's Data Protection Officer.