Bring Your Own Device Policy (BYOD)

Brookfield Primary School

[Version 1.0]

Last Reviewed	**January 2025**
Reviewed By (Name)	**Victoria Hardy**
Job Role	**School Business Manager**
Next Review Date	**January 2026**
Version produced Spring 2024	Minor amends indicated in green text to reflect DfE Cyber Standards and KCSIE 2023 Policy & section numbering changed JCC & DCC Reviewed in light of: 1. Mobile phones in schools - February 2024 (publishing.service.gov.uk) 2. Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

This document will be reviewed annually and sooner when significant changes are made to the law

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

Contents

1. Introduction 3

2. Scope and Responsibilities 3

3. Use of mobile devices at school 4
4. Access to the school's Internet connection 4
5. Access to School IT systems 5
6. Monitoring the use of mobile devices 5
7. Security of staff personal devices 5
8. Permissible and non-permissible use 5
1.9 Use of cameras and recording equipment

Copyright: Education Data Hub

1. Introduction

- We recognise that mobile technology offers valuable benefits to staff and students from a teaching and learning perspective and to visitors. Our school embraces this technology but requires that it is used in an acceptable and responsible way. The School will not compel school staff to use their own personal devices to access school systems, but if staff choose to use their own devices, this policy should be adhered to.
- Guest devices (any device which is not school owned or on the school asset list) should only be connected to a secure segregated network for access.
- This policy is designed to support the use of guest devices (any device which is not school owned or on the school asset list) in school in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use and misuse of the BYOD policy.
- 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).
- This applies to all guest devices connecting to school systems.
- The purpose of this policy is to preserve the security and integrity of school data and systems. It does not expressly or by implication provide permission to use any non-school device. Rather, it sets out the organisational and technical measures in place where such permission is granted in the staff code of conduct, pupil behaviour policy and any documents setting out expectations in relation to visitors. It has been reviewed in light of the Mobile phones in schools - February 2024 (publishing.service.gov.uk)
- The School reserves the right to refuse staff, pupils and visitors permission to use their personal devices on school premises.
- This policy should be read in conjunction with the schools HR advice and guidance. This policy has been the subject of formal negotiation and consultation between Derbyshire County Council and the recognised Trade Unions and Professional Associations. Agreement and adoption were only reached by Schools Joint consultative Committee where it is used in conjunction with the DCC LA Acceptable Use of IT Advice and Guidance.

2. Scope and Responsibilities

This policy applies to all use of guest devices to access the internet via the school's guest network or to access school information, by staff, pupils or visitors. This is known as “Bring Your Own Device”, or “BYOD”. 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.

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

If you have any concerns surrounding the use of personal devices, please contact our Headteacher or Designated Safeguarding Lead.

Users should be aware of the need to;

• Protect children from harm

Copyright: Education Data Hub

- Understand what constitutes misuse
- Minimise risk from BYOD
- Report suspected misuse immediately
- Be responsible for their own professional behaviour
- Respect professional boundaries

3. Use of mobile devices at school

Permission must be sought before connecting personal devices to the school's network. The school reserves the right to refuse staff, pupils and visitors permission to use their personal devices on school premises.

Staff, pupils and visitors are responsible for their personal devices at all times. The school is not responsible for the loss, or theft of, or damage to the personal device or storage media on that device (e.g. removable memory card) howsoever caused, including lost or corrupted data.

The school must be notified as soon as possible of any loss, or theft of a personal 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 Data Protection Officer.

Personal devices used to access school systems must enable automatic updates for security patches from the supplier. Applications installed on the device must also be subject to regular security updates, be supported by the supplier and licensed.

The school cannot support users' personal devices, nor has the school a responsibility for conducting annual PAT testing of personal devices.

4. Access to the school's Internet connection

The school is in the process of providing a guest network connection that staff, pupils and visitors may, with permission, use to connect their personal devices to the Internet. Access to the network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff, pupils and visitors use it at their own risk. In particular, staff, pupils and visitors are advised not to use the wireless network for online financial transactions.

The school does not permit the downloading of apps or other software whilst connected to the school network and the school is not responsible for the content of any downloads onto the user's own device whilst using the school's network.

The school accepts no liability for any loss of data or damage to personal devices resulting from use of the school's network.

Copyright: Education Data Hub

5. Access to School IT systems

Where staff are permitted to connect to school IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption and notifications must be turned off the lock screen. It is the responsibility of the owner of that device to ensure it is safe for the purposes for which they wish to use it.

Staff must **not** store personal data about pupils or others on any personal devices, or on cloud servers linked to their personal accounts or devices.

With permission, it may be necessary for staff to download school information to their personal devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of cyber-attacks. Please follow staff guidance on cyber security and email protection and be aware that personal devices are not subject to the same security controls and safeguards that protect the school network and devices.

Any unauthorised access to, or distribution of, confidential information should be reported to the Head Teacher and Data Protection Officer as soon as possible in line with the school's data protection policies. This includes theft or loss of a personal device which has been used to connect to school information systems or which may contain personal data.

Before selling or giving your personal device which has been used to access the school network including cloud-based systems to someone else, including a family member or spouse, it must be cleansed of all school related data, emails, systems and apps.

6. Monitoring the use of mobile devices

The school reserves the right to use technology that detects and monitors the use of personal devices, which are connected to or logged on to our network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and 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 to 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.

Any inappropriate content received through school IT services or the school internet connection should be reported to the Headteacher / IT Lead / Designated Safeguarding Lead as soon as possible.

7. Security of staff personal devices

Staff must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN, pattern or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period of time.

The school's Acceptable Use of IT and IT Security policies set out in further detail the measures to ensure responsible behaviour online.

8. Permissible and non-permissible use

Staff and visitors participating in BYOD must comply with the ICT Acceptable Use Policy.

Copyright: Education Data Hub

- Where there are particular safeguarding or safety requirements in some settings, for example, in special schools and nurseries, the Headteacher has the right to require storage of staff or visitor devices in a secure location such as staff lockers.
- The Headteacher can decide if devices can or cannot be taken into areas around the school where there are particular safeguarding issues (such as changing rooms). In such cases, the school should agree with and inform staff, pupils and visitors the areas which are expected to be "BYOD free".
- Visitors and contractors to the school/site should be informed of the policy regarding personal devices upon arrival (please refer to our Visitors and Contractors Policy).
- Personal devices must not be taken into controlled assessments and/or examinations, unless special circumstances apply.
- Staff, volunteers and contractors should not use their own personal mobile phone for contacting children and young people or parents/ carers, unless it is an emergency and they are unable to use or access the school's telecommunication systems.
- If it is necessary for a phone call or text to be taken or received, care should be taken to avoid disturbance or disorder to the running of the school.

9. Use of cameras and audio recording equipment

Visitors and staff subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings in school.

If staff are not permitted to use their own mobile device for photographs, then delete this next sentence] Photographs, video or audio recordings made by staff on their own mobile 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. If photographs, video or audio recordings are to be retained for further legitimate use, they should be stored securely via the School network.

In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings must not be published on blogs, social networking sites or disseminated in any other way without the permission of the people identifiable in them.

No one must use mobile devices 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 (for further information, please refer to our Social Media Policy).

Copyright: Education Data Hub