"Caring & sharing as part of God's family"

"Loving our neighbour as we love ourselves" - Luke 10:27

Bring Your Own Device Procedure (BYOD)

Hartington C of E Primary School

Last Reviewed	**April 2026**
Reviewed By (Name)	**Tracy Blackwell/ Morag McNulty**
Job Role	**Head teacher / SBO**
Next Review Date	**April 2027**
EDH April 2025	Minor amends indicated in green text KCSiE 2024 (also updated paragraph references) Updated the words 'must' and 'should' to **'will'** where necessary throughout.

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

Contents

1. Introduction

The school recognises that mobile technology can support teaching, learning and communication. Our school embraces this technology but requires that it is used in an acceptable and responsible way. However, personal mobile devices also present safeguarding, data protection and cyber security risks.

This policy sets out the conditions under which personal devices may be used on school premises or connected to school systems.

The school will not require staff to use personal devices for school business. Where permission is granted for use, all users **will comply with this policy at all times.**

The school reserves the right to refuse or withdraw permission for any personal device to be used on site or connected to school systems.

Guest devices (any device which is not school owned or on the school asset list) will only be connected to a secure segregated network for access.

This policy supports:

- Safeguarding duties
- Data Protection legislation (UK GDPR and Data Protection Act 2018)
- Cyber security standards
- Acceptable Use of IT Policy
- Staff Code of Conduct
- Behaviour Policy

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)

This policy will be read in conjunction with the school 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 staff, pupils, visitors, volunteers and contractors using personal devices on school premises or to access school systems. This is known as “Bring Your Own Device”, or “BYOD”.

Devices include but are not limited to:

- Mobile phones
- Tablets
- Laptops
- Smart watches / wearable technology
- USB storage devices
- Any Wi-Fi enabled portable device

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 Head teacher or Designated Safeguarding Lead.

Users will be aware of the need to;

• Protect children from harm

• Understand what constitutes misuse

• Minimise risk from BYOD

• Protect the organisation from cyber incident

• Report suspected misuse immediately

• Be responsible for their own professional behaviour

• Respect professional boundaries

3. Safeguarding Expectations

Safeguarding is the school's highest priority.

Personal mobile phones will not be used in classrooms or learning areas. Staff will store personal phones securely during teaching time.

Devices will not be used in toilets, changing rooms or other sensitive areas.

Staff will not use personal devices to contact pupils or parents unless in an emergency and no school communication system is available.

Personal devices will not be used to take photographs, video or audio recordings of pupils unless permission has been given by the Head teacher.

Any images or recordings must be transferred to the secure school system and deleted from the personal device as soon as possible.

4. Use of mobile devices at school

Permission will 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 will 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 will be reported immediately to the school's Data Protection Officer.

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

Where applicable, anti-virus and anti-malware software will be installed onto any device intended to access school systems.

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

5. Access to the school's Internet connection

The school provides a wireless network that staff, pupils and visitors may, with permission, use to connect their mobile 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.

At Hartington C of E Primary School there is a guest wireless network for visitors to access rather than using the schools own internet connection. The password for this is changed every month and is controlled by the IT technician.

The school does not permit the downloading of apps or other software whilst connected to the school network and users and must not attempt to bypass filtering or proxy controls. The school is not to be held responsible for the content of any downloads 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.

6. Access to School IT systems

Where staff are permitted to connect to school IT services from their own devices, a second layer of password protection and/or encryption will be in place and the notifications, for these services, will 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 will **not** store personal data about pupils or others on any personal devices, or on cloud servers linked to their 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 will 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 device which may contain personal information. Should the device be transferred to another user it should be cleansed of all school related data, systems and apps.

School information must not be sent to or from personal email accounts.

School data must not be uploaded to generative artificial intelligence tools or unapproved online platforms.

Before transferring ownership or disposing of a device, all school data and system access must be permanently removed.

7. Monitoring the use of mobile devices

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

Monitoring will be proportionate, lawful and in line with the school Privacy Notice.
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 will be reported to the Head teacher / IT Lead / Designated Safeguarding Lead as soon as possible.

8. Security of staff mobile devices

Staff will take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time. Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

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

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

9. Permissible and non-permissible use

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

- Visitors and contractors to the school site will be informed of the policy regarding personal devices upon arrival.
- Personal devices will not be taken into controlled assessments and/or examinations, unless special circumstances apply.
- Staff, volunteers and contractors will 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 will be taken to avoid disturbance or disorder to the running of the school.

10. Use of cameras and audio recording equipment

The school's position in relation to KCSiE 2024 –particularly in relation to paras 432, 97, 137 is that

Visitors and staff subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings in the school. Recordings in these circumstances will be carried out in line with our HR policies and procedures. Ensure you refer to the Recording Guidance Note when setting up a recorded meeting.

In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings will 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 will use mobile devices to record people at times when they do not expect to be recorded, and devices will not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school.

