BRING YOUR OWN DEVICES (BYOD) POLICY	Revision No	2
	Date Issued	January 2024
	Authorised by	Highfields Governing Board
	Date approved	1 February 2024
	Minute number	31/23
	Implementation Date	2 February 2024
	Review Date	Annually

Contents

Purpose, Values and Aims of Highfields School 2

1. Introduction 3
2. Scope and responsibilities 3
3. Use of mobile devices at school 3
4. Access to the school's internet connection 4
5. Access to school IT systems 4
6. Monitoring the use of mobile devices 5
7. Security of staff mobile devices 5
8. Permissible and non-permissible use 5
9. Use of cameras and audio recording equipment 6

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

Purpose, Values and Aims of Highfields School

Our Core Purpose
To be an inclusive, happy community that values every individual and inspires them to achieve their full potential.

Our Values
Inclusion, fairness and equality
Respect and tolerance
Celebration of achievement
Personal reflection, honesty and mutual trust
Care for our environment

Aims – to achieve our core purpose and values we aim to:

- Respect all students and staff as individuals
- Celebrate diversity and promote equality
- Provide appropriate levels of challenge
- Develop understanding and enjoyment of learning
- Support and encourage individuals to make a valuable contribution to society
- Be a reflective school seeking continuous improvement
- Play an active part in our community
- Nurture physical and emotional well being
- Promote a happy, safe and stable environment

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.
- This policy is designed to support the use of personal devices 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 non-school owned electronic mobile 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 own mobile devices on school premises.
- This applies to all users connecting to school systems.

2. Scope and responsibilities

This policy applies to all use of non-school owned mobile devices to access the internet via the school's internet connection or to access school information, by staff, students or visitors. This is known as “Bring Your Own Device”, or “BYOD”. Mobile devices include laptops, tablets, smart phones, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to WIFI and the Internet.

All staff are responsible for reading, understanding and complying with this policy if they are using their own 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
• 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

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

The school must be notified immediately of any damage, loss, or theft of a mobile 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.

Devices used to access school systems must receive regular security patches from the supplier. Applications installed on the device must also be subject to regular security updates, be supported by the supplier and be appropriately licensed.

Permission must be sought before connecting personal devices to the school's wireless connection. The school reserves the right to refuse staff, students and visitors' permission to use their own mobile devices on school premises.

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

Where the school uses Multi Factor Authentication, personal mobile phones can be used to receive the necessary authentication code.

4. Access to the school's internet connection

The school provides a wireless network that staff, students 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, students and visitors use it at their own risk. In particular, staff, students and visitors are advised not to use the wireless network for online banking or shopping.

The school does not permit the downloading of apps or other software whilst connected to the school network and 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.

It is not permissible for any user to bypass proxy server settings unless written permission from the headteacher is sought and the purpose is documented. Users of mobile devices must not circumvent on site filtering through the use of 4G/5G services.

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.

5. 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 must be in place and notifications, must be turned off the lock screen.

Staff must **not** store personal data about students 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 Headteacher 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.

Before selling or giving your mobile device to someone else, including a family member or spouse, it must be cleansed of all school related data, emails, systems and apps.

Staff must not send school information or personal data to/from their personal email accounts or social media or similar accounts.

Users must follow the procedures for connecting to the school systems.

6. 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.

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.

Anyone who receives any inappropriate content through school IT services or the school internet connection should report this to the Headteacher / Designated Safeguarding Lead/ IT Network & Systems Manager as soon as possible.

7. Security of staff mobile devices

Staff must 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 unlock the device, and ensuring that the device auto-locks if inactive for a short 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 their own devices.

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.

- The Headteacher has the right to locally enforce storage of staff or visitor devices to a secure location such as the school office
- The Headteacher can decide if devices can or cannot be taken to classrooms.
- 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).
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
- The school or setting should agree and inform users of devices regarding what areas would be expected to be "BYOD free". We do not allow the use of personal devices in toilets, bathrooms and changing rooms.
- Mobile 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.
- When driving on behalf of their organization, any staff member or volunteer should ensure the safe use of any personal device.

9. Use of cameras and audio recording equipment

Parents and carers may not take photographs, videos or audio recordings of their children at school events for their own personal use. Other visitors and staff may not use their own mobile devices to take photographs, video, or audio recordings in school provided they have checked that parental permission to take photographs, films or recordings of the relevant individuals has been received by the school. This includes any individual who might be identifiable in the background.

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 students and, in some cases their safety and wellbeing, photographs, video, or audio recordings should 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 e-safety policy regarding social media).