HATHEROP CASTLE
PREP SCHOOL & NURSERY

Bring Your Own Device Policy for Staff, Pupils and Visitors

Reference:	B03
Version number:	1.2
Last updated:	February 2023
Date of next review:	Februrary 2025 or if legislation/statutory requirements change

Summary of changes and reviews

Version	Date	Summary of amendments	By
1.0	1 Feb 20	Initial version	SB
1.1	11 Mar 21	Amendments to integrate rollout of Censornet and withdrawal of school-provided insurance for personal devices	SB
1.2	12 Feb 23	Reviewed, no changes	SB

Contents

BRING YOUR OWN DEVICE POLICY FOR STAFF, PUPILS AND VISITORS

Introduction

Hatherop Castle School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. The school embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff members, pupils and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the School Business Manager. These devices are referred to as 'mobile devices' in this policy.

Sections one to three and five of this policy apply to all school staff, pupils and to visitors to the school. The rest of the policy is only relevant to school staff.

This policy is supported by the Acceptable Use Policy.

The Wishford Schools' IT Department is responsible for the approval of this policy and for reviewing its effectiveness. The IT Department will review this policy at least annually.

Use of mobile devices at the school

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

- In the classroom with the permission of the teacher
- In areas where no children are present i.e. meeting rooms

Staff, pupils and visitors to the school are responsible for their mobile device 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. The School Business Manager must be notified immediately (via the school office) of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off and kept in pockets and/or handbags 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 mobile devices on school premises, and may insist that such devices are handed into reception before entering the school.

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 where this does not include children from Nursery or Reception. Under no circumstances are photographs, videos or audio recordings to be made that include Nursery or Reception children.

Other visitors and staff may use their own mobile devices to make photographs, video, or audio recordings in school provided they first obtain permission to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background. Note that under no circumstances are staff to take photographs, videos or audio recordings of Early Years and Foundation Stage children on personal devices.

To respect everyone's privacy and in some cases protection, 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. Parents or carers should avoid commenting on activities involving pupils other than their own in photographs, video, or audio, and other visitors and staff should not comment on these.

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. Staff must comply with the school's social media policy and anti-bullying policy when making photographs, videos, or audio recordings.

Access to the school's internet connection

The school provides a wireless (WiFi) network that staff, pupils and visitors to the school may use to connect their mobile devices to the internet. Access to the wireless 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 and visitors are advised not to use the wireless network for online banking or shopping.

By default, all devices connect to the internet via the school's monitoring system, Censornet. A security certificate is required in order to access websites; instructions for downloading the certificate onto personal devices varies by device type, can be found here. An exception can be made for specific devices to circumvent Censornet where there is a genuine need, and is usually constrained to resident staff only. Any such device is therefore not to be brought out in areas where and when children are present. To request exceptions for specific devices, individuals should complete this form. Please note that this privilege will be withdrawn if devices are taken out in the presence of children.

The school network should NOT under any circumstances be used to connect Payment Card Infrastructure (PCI) devices such as card machines.

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 wireless network. This activity is taken at the owner's own risk and is discouraged by the school. 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 wireless network.

Access to school IT services

School staff are permitted to connect to or access the following school IT services from their own mobile devices:

- 3SYS
- Complete-Ed
- Google Calendar
- Office 365 (including Outlook, SharePoint and OneDrive)
- PASS
- PRS
- Mailchimp
- Tapestry
- Timetabler

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on non-Wishford cloud

servers (including, but not limited to, Google Drive, Dropbox etc.) linked to their mobile devices. In some cases it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above 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 dataprotection@wishford.co.uk soon as possible.

Staff must not send school information to their personal email accounts or cloud-based storage.

If in any doubt a device user should seek clarification and permission from the Wishford IT helpdesk before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

Monitoring the use of mobile devices

The school may 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. By using a mobile device on the school's IT network, staff, parents and visitors to the school 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, tracking school information and safeguarding children in accordance with Annex C to Keeping Children Safe in Education 2020

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 (including passwords), 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.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the Wishford Schools' IT Helpdesk as soon as possible; pupils should report it to a teacher.

Virtual private networks

The use of Virtual Private Networks (VPNs) on devices is strictly prohibited in school. Should any pupil or staff-owned devices be found to have a VPN loaded onto them, disciplinary action will be taken against that individual, the sanctions for which will be severe. The school may also withdraw permission for that staff member or pupil to bring devices into school. By bring a device into school, you consent for the school to conduct random checks of your devices for VPNs. Any queries about this should be raised with the School Business Manager.

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 be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

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

Staff are reminded to familiarise themselves with the school's e-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

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

Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the school's compliance with the Data Protection Act 1998. Staff must apply this BYOD policy consistently with the school's Data Protection Policy.

Support

Hatherop Castle School takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned devices which is an individual responsibility.

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 school will consider its response in accordance with the school's Performance Management Policy. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breaches of this policy, the school will permanently withdraw permission to use user-owned devices in school.

Incidents and Response

The school takes any security incident involving a staff member's, pupil's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the Wishford Schools' Data Protection Officer, Paul Easterbrook.