Bring Your Own Device Policy for Staff and Visitors

School update	
Responsible for review of policy	Deputy Head Pastoral
Last school update	May 2025
Governor Sub-Committee approval	
Sub Committee to review and approve	Pastoral
Review Period	Annual
Scheduled review	May 2026
Approved by Sub Committee (Meeting date)	1 May 2025
Related policies	Safeguarding Behaviour Online Safety Policy IT Acceptable Use Policy

Uploaded to Staff Shared	May 2025
Uploaded to Website	May 2025

1 Introduction

We recognise that many of our staff and visitors have personal mobile devices (such as tablets, smartphones and handheld computers), which they could bring to the school and, in the case of staff, occasionally use these devices for work purposes. However, the use of personal mobile devices within the school introduces increased risks in terms of the security of our IT resources and communication systems, the protection of confidential and proprietary information, and compliance with legal obligations (including child safeguarding).

This policy sets out rules on the use of personal devices in order to:

- protect our systems, as further defined below;
- protect school data (including personal data), as further defined below; and
- set out how we will manage and monitor your access to our systems.

The school reserves the right to prohibit bringing personal devices into the school and/or using them for work purposes (as applicable). The school also reserves the right to require personal devices to be switched off at certain times and/or within certain areas of the school.

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our IT Acceptable Use Policy, Online Safety Policy, Data Protection Policy, Equal Opportunities Policy, all of which are available on the policy directory.

2 Scope and purpose of the policy

This policy applies to staff and visitors who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) within the school and/or for work purposes. Note that it applies to use of the device for work purposes both during and outside school hours and whether or not use of the device takes place at school.

For staff, this policy applies to all devices used to access our IT resources and communication systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

When you access our systems, you may be able to access data about the school, including information which is confidential, proprietary or private (collectively referred to as **school data** in this policy).

As part of granting your personal device access, the school will take steps to keep your personal device's wider data and systems separate from our systems and school data which you access from that device.

When you access our systems using a device, we are exposed to several risks, including from the loss or theft of the device, the threat of malware and the loss or unauthorised alteration of school data. Such risks could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy. This could also result in damage to our systems, our business and our reputation.

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal. Disciplinary action may be taken whether the breach is committed during or outside school hours and/or whether or not use of the device takes place at school. You are required to co-operate with any investigation into

a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

Relatedly, this policy also applies to visitors (and staff) who access our wireless networks on their own devices for personal use (see further below).

3 Access to our wireless internet networks (visitors and staff)

We provide a wireless network that you may use to connect your device to the internet. Access to the wireless network is at the discretion of the school. It should under no circumstances be used to access or distribute content that is unlawful, harmful, explicit, offensive or otherwise inappropriate. We may withdraw access from anyone we consider is using the network inappropriately.

We cannot guarantee that the wireless network is secure, and you use it at your own risk. In particular, you are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto your own device whilst using our wireless network. This activity is taken at your 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.

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. By using a mobile device on the school's wireless network, you agree to such detection and monitoring.

The information that we 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 peer-to-peer traffic transmitted via the network].

Staff should also refer to the Monitoring section below for further information.

4 Images and recordings (staff and visitors)

You are not permitted under any circumstances to use your personal devices when taking images, videos or other recordings of any pupil nor to have any images, videos or other recordings of any pupil on your personal devices. Please read this in conjunction with the Online Safety Policy, Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies.

5 Connecting devices to our systems (staff)

Connectivity of all devices to the school's systems is centrally managed by the IT Department. We reserve the right to refuse or remove permission for your device to connect with our systems.

6 Monitoring (staff using systems)

The contents of our systems and school data are our property. All materials, data, communications and information, including but not limited to email (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and

printing of transactions, messages, communications, postings, logins, recordings and other uses of the device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. You should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential and to avoid processing any personal data relating to non-school related third parties (for example, your family and friends) on our systems.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate school purposes, including, without limitation, in order to:

- prevent misuse of the device and protect school data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- monitor performance at work; and
- ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage the school, its systems or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

You acknowledge that the school is entitled to conduct such monitoring where it has a legal obligation or legitimate basis to do so, and that (without further notice or permission) we have the right to copy, erase or remotely wipe the entire device (including any personal data stored on the device).

Whenever we monitor personal data it will be carried out in line with the Data Protection Policy and Privacy Notices and government guidance such as KCSIE.

You acknowledge that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

7 Security requirements (staff)

You must comply with the IT Acceptable Use and E-Safety / Online Safety Policies when using your device to connect to our systems.

In addition to the requirements set out in the above-mentioned policies and set out above in this policy, you must also:

- in no circumstances use your personal email or other personal messaging account to transfer, attach, discuss, or otherwise use school data or any other information which may be contained in our systems. To the greatest extent technically possible, our systems and our data must be kept separate from the rest of your personal device;
- protect the device with a PIN or strong password, and keep that PIN or password secure at all times. The PIN or password should be changed regularly . If the confidentiality of a PIN or password is compromised, you must change it immediately;

- not download or transfer any school data to the device, for example via email attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device;

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate business purposes.

You must cooperate with us to enable such inspection, access and review, including providing any passwords or PINs necessary to access the device or relevant applications.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly backup any personal data contained on the device.

You acknowledge that, without further notice or permission, we may need to inspect a device and applications used on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data on or from a device for legitimate purposes.

8 Lost or stolen devices and unauthorised access (staff)

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the IT Department immediately.

Appropriate steps will be taken to ensure that school data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work email account, even if such emails are personal in nature). As noted above, although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly backup all personal data stored on the device.

9 Procedure on termination of employment (staff)

On your last day of work, all school data (including work emails), and any software applications provided by us for work purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the IT Department for wiping and software removal. You must provide all necessary cooperation and assistance in relation to this process.

10 Personal use (staff)

We have a legitimate basis or legal obligation to access and protect school data stored or processed on your device, including the content of any communications sent or received from the device. Where we are relying on our legitimate interests, we recognise the need to balance our need to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

- consider whether the action is proportionate in light of the potential damage to the school, its pupils or other people impacted by school data;
- consider if there is an alternative method of dealing with the potential risks to the school's interests (recognising that such decisions often require urgent action);
- take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data, which is also school data, including all personal emails sent or received using our email system).

As noted above, it is important to separate your personal data from school data. To reduce the likelihood of the school inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps to separate school data from your personal data on the device:

- do not use work email for personal purposes;
- regularly backup all personal data stored on the device;

11 Appropriate use (staff)

You should never access or use our systems or school data through a device in a way that breaches any of our other policies, in particular our IT Acceptable Use Policy, Online / Safety Policy, Data Protection Policy, Equal Opportunities Policy,. If you breach any of the above policies, you may be subject to disciplinary action up to and including dismissal.

You should also minimise the amount of school data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer required.

You must not talk, text, email or otherwise use a device while operating a school vehicle or while operating a personal vehicle for school purposes. You must comply with any applicable law concerning the use of devices in vehicles.

12 Who is responsible for this policy?

The DFO in conjunction with the Head of the IT Department shall have overall responsibility for the effective operation of this policy and shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice. If you have any questions about this policy or other queries related to use of your own device for work purposes please contact the IT Department.