THE WHITE ROSE FEDERATION

BRING YOUR OWN DEVICE (BYOD) POLICY

Document Status			
Date of adoption by the Governing Body		**Date of next review**	
Autumn 2023		Autumn 2024	
Responsible officer			
J. Marwood			
Signed:			
Headteacher	**S. MacDonald**	**Chair of Governors**	**A. Edwards & A. Burr**

Links to Other Policies	
Online Safety Policy	
Staff IT User Agreement	

Bring Your Own Device (BYOD) Policy for Staff and Visitors

Introduction

The school recognises that mobile technology offers valuable benefits to staff 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 intended to address the use by staff members and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection or to access or store school information. 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 schools' leadership team.

These devices are referred to as 'mobile devices' in this policy. Sections one, two and four of this policy apply to all school staff and to visitors to the school. The rest of the policy is only relevant to school staff. This policy is supported by the school's Acceptable Use Policy.

Policy statements

Use of mobile devices at the school

Staff must only use mobile devices in the staff room, or in an office, during free time, unless as part of a planned lesson, with authorisation from the Head of School. Mobile phones should be left on silent. Should a staff member be wearing a smartwatch for telling the time purposes, they should be switched to a mode whereby calls, texts and other notifications do not ping through. Staff should not be using the school electricity to charge their mobile devices on a routine basis; an ad hoc emergency is acceptable to ensure they have sufficient charge if driving home. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office. Staff must not use their phones to capture photos or videos of pupils or staff members.

Visitors to the school are asked to keep their phones in their pocket or bag, ideally switched to silent if they are working in the classroom. They may use their mobile in the non-teaching areas, if it is a work-related call. They must have permission from the class teacher to use their phones for work purposes in the classrooms and this must never include taking photos or videos of staff and children.

Parents collecting their children from the school site are also asked to keep their phones in pockets or bags. Photos must not be taken of children or staff on the school site unless permission has been granted at school events.

Pupils should not bring their mobile phone or tablet to school. Should a child not be going home after school and needs their phone that evening, parents should hand over the phone to a member of staff on the school gate. The office will sign for the receipt of this and will keep the phone secure during the day. At the end of the day, the office will sign over the phone to the class teacher for them to return it to the pupil on the gate as they leave. This eliminates the risk of any online safety incidents in school when the phone is not connected to the school's Wi-Fi and is therefore not subject to the school's filtering system. The school is not responsible for the loss, of theft of, or damage to a pupil's mobile phone or tablet whilst we are looking after them.

Staff 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. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off 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.

Access to the school's Internet connection

The school provides a wireless network that staff 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 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.

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 mobile devices:

• the school email system (where appropriate encryption technologies have been deployed)

• the school virtual learning environment (Office 365 and Teams

• official school apps.

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 cloud servers 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. Where personal or sensitive data is used in this way devices or files MUST be encrypted.

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 the School Business Manager as soon as possible in line with the school’s data protection policies.

Staff must not send school information to their personal email accounts. If in any doubt the user should seek clarification and permission from the School Business Manager 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 uses 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 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 and for tracking 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 (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 School Business Manager as soon as possible.

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 Online 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 laws. Staff must apply this BYOD policy consistently with the school's Data Protection guidelines. Where such devices are used to process data of a personal or sensitive nature appropriate encryption of files or devices must be used. All such data should be backed up to the school's Office 365 accounts and deleted from mobile devices as soon as work has been completed.

Support

The school cannot support users' own devices but will offer advice to users in their use where practically possible. The school takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned device.

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 may discipline staff in line with the school's Disciplinary Procedure. Guidance will also be offered to staff to support them in complying with this policy.

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 breach 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 or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of a mobile device should be reported to the office in the first instance. Data protection incidents should be reported immediately to the School Business Manager.