Bring Your Own Devices Procedure (BYOD)

GDPR LA POLICY

Review: Annually

Next Review Date: May 2022

Role	Name
Headteacher	**Caroline Rodgers**
Chair of Governors	**Linda Mosley**
Designated Governor	**Linda Mosley – GDPR Governor**
Designated Senior Lead	**Caroline Rodgers – Headteacher** **Jayne Saxton – SBO**

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

CONTENTS

6.1 Introduction

We recognise that 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 procedure 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 (GDPR) and the Data Protection Act 2018 (DPA 2018).

6.2 Scope and Responsibilities

This procedure 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, pupils or visitors. This is known as “Bring Your Own Device”, or “BYOD”. The mobile devices in question include laptops, tablets, smart phones, wearable technology and any similar devices.

All staff are responsible for reading, understanding and complying with this procedure if they are using their own personal devices or using personal devices to access information held on school systems.

If you have any data protection concerns surrounding the use of personal devices, please contact our Data Protection Officer.

6.3 Use of mobile devices at school

Staff, pupils 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.

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 or Ethernet connections. The school reserves the right to refuse staff, pupils 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.

6.4 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 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, pupils 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.

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.

6.5 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 the notifications, for these services, must be turned off the lock screen.

Staff must 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 mobile devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of 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 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.

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

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

6.6 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 / IT Lead as soon as possible.

6.7 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 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.

Date	Details of Changes	Name	Approval Date	New Version No	Website
23.7.20	New policy cover sheet added Content page numbers amended Paragraph 6.5 text addition which reads: *The School IT systems are managed through an external provider, all users with personal devices must request access via the IT helpdesk. Users, which include staff, visitors and volunteers must request permission from the Headteacher to access the school internet from external devices. The WiFi password will be shared when approval has been obtained.*	ES JS JS		One	
13.5.21	Sentence added to policy cover sheet - This document will be reviewed annually and sooner when significant changes are made to the law Section 6.2- second/third paragraphs re-written Section 6.3 - Fourth/fifth paragraphs - added Section 6.4 – wording added to first paragraph - with permission Section 6.4 – Paragraph 3 – updated and amended Section 6.4 – Paragrapg 4 – new section added Section 6.5 – Paragraph 3, first sentence – wording changed from mobile to personal Section 6.5 – Paragraph 3 – wording changed from phishing to cyber Section 6.5 – Wording added to paragraph 3 - . 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. Section 6.5 – Wording added to paragraph 4 - which may contain personal information Section 6.5 – Information removed from final paragraph - The School IT systems are managed through an external provider, all users with personal devices must request access via the IT helpdesk. Users, which include staff, visitors and volunteers must request permission from the Headteacher to access the school internet from external devices. The WiFi password will be shared when approval has been obtained. Section 6.6 – Wording added to first paragraph - school reserves the right to use	JS		Two	