Bring Your Own Device Procedure (BYOD)v6

MUNDY C OF E JUNIOR SCHOOL

Last Reviewed	**JULY 2021**
Reviewed By	**GOVERNING BODY**
Next Review Date	

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 likely to “BYOD”.

Our Data Protection Officer provides assistance and further guidance on BYOD with regards to data protection.

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.

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 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 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.

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 mobile devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of 'phishing' attacks – that would be blocked by school security, but allowed through on mobile devices. Therefore, attachments must not be opened from mobile 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 the device. 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 (you will be issued with these details as appropriate).

6.6 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. 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.