BRING YOUR OWN DEVICE (BYOD) POLICY FOR STAFF AND VISITORS

In this policy the following members of staff are referred to:

TITLE	NAME OF MEMBER OF STAFF
Head Teacher	Claire Murdoch
E-Safety coordinator	Adam Wright
NMS Privacy and Compliance Officer	Deborah Livsey

INTRODUCTION

This policy applies to all adult members of the School community, including staff, parents, and visitors. Pupils are not permitted to use personal mobile devices in school. For the purposes of this policy 'staff' includes teaching staff (permanent, part-time, peripatetic, specialist and agency) and non-teaching staff, directors, advisors and regular volunteers. (Access to systems and records at the School is subject to controls but not exclusive to employees, and although certain workers and visitors at the School may therefore have access to systems and records, this is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

The School recognises that mobile technology offers valuable benefits from an administrative and teaching and learning perspective. 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 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's e-safety coordinator. These devices are referred to as 'mobile devices' in this policy.

Sections one to 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 of I.T. and Remote Working Policy.**

POLICY STATEMENTS

1. Use of mobile devices at the School.

Please note that there are different rules depending on how the mobile device is being used when the device is being used as a camera or as an audio recording device - please see 2. below**.**

When the mobile device is being used for anything other than as a camera or recording device the following protocol must be observed:-

- Staff personal mobile devices must be switched off or put on silent mode during working hours.
- Staff may only use their mobile devices during break time, lunchtimes and after school, either in the School staff room or in their classroom only when no children are present.
- Visitors to the School should keep their use of mobile phones to a minimum during a normal school day but in any event, the use of a mobile device in the EYFS setting or in any classroom when children are present is prohibited and all devices must be switched to silent and kept out of sight.
- A mobile device must not be taken into controlled assessments and/or examinations unless special circumstances apply.

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

The School reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

2. Use of mobile devices as cameras and audio recording equipment

The use of mobile phones or cameras by parents or visitors anywhere within the EYFS setting is not permitted unless prior approval has been given by the Head Teacher. EYFS staff may only use school devices to take images of Reception children.

Parents and carers may take photographs, videos or audio recordings **of their own children** at school events **only** for their own personal use.

Unless the visitor is a photographer appointed by the School, other visitors and staff may **NOT** use their own mobile devices to make photographs, video, or audio recordings of children at the School.

To respect everyone's privacy and in some cases for child protection reasons, 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 children in photographs, video, or audio, and other visitors and staff should not comment either.

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.

3. 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.

4. 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 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 that usage is appropriate.

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's e-Safety coordinator and the IT manager (Soft Egg) as soon as possible.

5. Access to school IT services

School staff are permitted to connect to or access the School email system and servers from their mobile devices:

Staff may use these systems to view school information, 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.

Staff must exclusively use for work purposes the School's IT services and any information accessed through them. 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, and so at a minimum all personal devices must be encrypted using a password. Any inadvertent and/or unauthorised access to, or distribution of, confidential information should be reported to the School's e-Safety coordinator immediately; this would constitute a data breach and must be logged, referred to the NMS Privacy and Compliance Officer and investigated.

Staff must not send school information to their personal email accounts.

If in any doubt, a device user should seek clarification and permission from the School's e- Safety coordinator before attempting to gain access to a system for the first time.

6. Security of personal 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 over school systems or over others' own devices.

Staff are reminded to familiarise themselves with the School's **e-Safety**, and **Acceptable Use of IT and Remote Working** 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.

7. Compliance with Data Protection Policy

Staff compliance with this policy is an important part of the School's compliance with the General Data Protection Regulations 2018 and the Data Protection Act 2018. Staff must therefore apply this policy consistently with the School's **Acceptable Use of IT and Remote Working Policy** and the NMS **Staff Data Protection and Handling Policy.**

8. Support

The School takes no responsibility for supporting a staff member's own devices; nor has the School any responsibility for conducting annual PAT testing of personally-owned devices.

9. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance with this policy exposes both staff and the School to risks. If a breach of this policy occurs, the School will respond immediately by issuing a verbal warning, then a written warning on any subsequent breach, to the staff member concerned. 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 personal devices in school.

10. Incidents and Responses

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 the mobile device should be reported to the School Office in the first instance. Data protection incidents should be reported immediately to the Head teacher and the School's e-safety coordinator for recording and referral to the NMS Privacy and Compliance Officer.

Claire Murdoch
Head Teacher
September 2023

Review approved by Deborah Livsey CEO
The New Model School Company Limited
September 2023

Next review date: August 2024