ACCEPTABLE USE OF I.T. AND REMOTE WORKING POLICY

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

TITLE	NAME OF STAFF MEMBER
Head Teacher	Claire Murdoch
NMS Privacy and Compliance Officer	Deborah Livsey

SCOPE OF THIS POLICY

This policy applies to all adult members of the School community, including staff, parents and visitors. For the purposes of this policy 'Staff' is widely defined and includes both 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.

A separate Pupil Contract **School Pupil Agreement for the Acceptable Use of Email, IT and mobile technology** is part of the **e-Safety policy** and is signed by pupils before they are permitted to use the School's network. Pupils are not permitted to bring mobile devices to school (with the exception of Year 6 pupils who are travelling to and from school alone, but these must be retained by their teacher or the School office during the school day).

ONLINE BEHAVIOUR

As a member of the School community you should follow these principles in all of your online activities:

- The School cannot guarantee the confidentiality of content created, shared and exchanged via the School systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

USING THE SCHOOL'S I.T. SYSTEMS

Whenever you use the School's I.T. systems (including by connecting your own device to the network) you should follow these principles:

- Only access school I.T. systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's I.T. systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school I.T. systems without prior permission from the Head Teacher.
- Do not use the School's I.T. systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's I.T. systems, and that the School can view content accessed or sent via its systems.

PASSWORDS

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

The School's I.T. system will force users to change their password every 120 days, and will require the password to meet stipulated complexity requirements.

USE OF PROPERTY

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the School's external I.T. provider, Soft Egg.

USE OF SCHOOL SYSTEMS

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff should keep their personal, family and social lives separate from their school I.T. use and limit as far as possible any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

USE OF PERSONAL DEVICES OR ACCOUNTS

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Head Teacher.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including encryption as a standard minimum and preferably two factor authentication.

REMOTE WORKING POLICY

If you have received permission from the Head Teacher to work away from school premises, the following protocols must be adhered to:-

1. If using a school device off school premises

It is your responsibility to take measures to ensure the physical security of the device at all times, the device should not be left unattended in a public place and at home it should be in an area of the home where it could not be accidentally damaged.

Ensure that no one (including members of your own household) can overlook your screen when you have any personal or confidential data displayed.

Only download files from the school server or drive when you are using a secure network (indicated by the padlock symbol).

Do not download any software application, school-related or otherwise, onto your school device when away from the school premises.

2. If using a personal device off school premises for school related work

Only in exceptional circumstances and with the Head Teacher's permission may a personal device be given the capability of accessing the school network via a RDS (Remote Desktop Server). This access must be enabled by Soft Egg.

It is your responsibility to keep your personal device maintained with the latest security software updates. Using out of date software leaves a device vulnerable to malware, which in turn exposes the school systems.

It is your responsibility to ensure the cyber security of the device, both in terms of encryption as a minimum, and preferably two factor authentication; and also in terms of the physical security of the device.

Only access the school systems when you are using a secure network (indicated by the padlock symbol).

We would expect staff to access the school servers and drives in the usual way using their password to carry out their work and not save any files on a non-school device. If for any reason files are saved on a non-school device they must be deleted from that device as soon as they have been saved on the school server or drives.

MONITORING AND ACCESS

Staff, parents and visitors should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, as due to evidence of extremism, and/or the protection of others.

The deletion of web browsing history which was carried out using the school's internet access and your school device is forbidden and would be considered a disciplinary matter. Any such deletion would in itself be cause for suspicion that the access and device had been used for non school related business.

The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

The use of personal devices by pupils is not permitted within the School. However pupils in Year 6 (with permission) may bring in mobile phones for safety purposes if they walk to and from school alone. The devices must be handed to their class teacher or the School office at the start of the day and collected as the pupil leaves school. If any devices are found anywhere on the School premises, other than the School office or in a teacher's desk, these will be confiscated and examined if deemed necessary.

COMPLIANCE WITH RELATED SCHOOL POLICIES

You will ensure that you comply with the School's **e-Safety, Bring your own Device, Safeguarding, Anti-Bullying, Staff Code of Conduct policies** and the NMS Staff Handbook**.**

RETENTION OF EMAILS

Staff must be aware that all emails sent or received on school systems will be routinely deleted after 3 years and email accounts will be suspended and the contents archived within 1 year of that person leaving the School. Important information, for example related to safeguarding or disciplinary matters that is necessary to be kept, should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Head Teacher.

REPORTING OF DATA BREACHES

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. As a result of:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, eg through the use of malware;
- opening a phishing email;
- application of the wrong privacy settings when using online systems;
- misdirected post or email;
- failing to mask the identity of recipients of a mass email; and
- unsecure disposal of paper records or redundant hardware.

NMS as data controller must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the NMS and the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If staff become aware of a suspected breach, the Head Teacher must be notified immediately, who will in turn record, investigate and take the necessary steps to contain and mitigate the breach, liaising where necessary with the NMS Privacy and Compliance officer.

Data breaches may happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, if they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff. The School's primary interest and responsibility is in protecting

potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, may not always result in a serious conduct issue or breach of policy; but failure to report a breach will always be a disciplinary offence.

BREACHES OF THIS POLICY

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to school I.T. systems.

If you become aware of a breach of this policy or the **e-Safety Policy**, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Head Teacher. Reports will be treated in confidence wherever possible.

Claire Murdoch
Head Teacher
September 2023

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

Next review date: August 2024