St Mary's School
CAMBRIDGE

IT Acceptable Use Policy

This policy is the responsibility of the IT Director.

Applies to: Whole School and all staff.

Last review: June 2022

Next review: Summer Term 2023

Overview

This Policy applies to all staff working at St Mary's School, Cambridge ('the School') and 'staff' (for the purposes of this Policy) is defined as any person working at the School, whether under a contract of employment or contract for services, whether paid or unpaid, whatever their position, role, or responsibilities. Staff includes (but is not limited to) teachers, peripatetic teachers, teaching assistants and support, coaches, part -time staff, graduate/language assistants, sports/gap year assistants, all support staff, supply staff, temporary staff and casual workers, exam invigilators, work experience students and volunteers.

This policy applies to those who use the School IT systems as a condition of access. Access to the School IT systems is not intended to confer any status of employment on any contractors. Pupil access to the School IT systems is covered in the *Pupil Internet and IT Acceptable Use Policy*.

Online behaviour

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

- The School cannot guarantee the confidentiality of content created, shared, and exchanged via 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 IT systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- *Do not leave your device logged on and unlocked if you are not present*
- *Do not use external storage devices unless they have been checked and approved by the IT support team*
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT 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 IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the school's IT 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.

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 your line manager and the IT department.

Use of the School systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration, and education. Staff and pupils should keep their personal, family, and social lives separate from their school IT 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. Please be aware that where necessary and following consideration and approval by the IT Director and notification to the individual, we may use auto-forwarding on a school email account. We may wish to use this where, for example, a person is off sick or on holiday and we need to monitor email traffic from prospective parents.

Use of personal devices or accounts and working remotely.

All official school business of staff and governors 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 IT Director.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including two-factor authentication, encryption etc. and in accordance with the *Bring Your Own Device to Work Policy* (BYOD).

Monitoring and access

Staff, parents, and pupils 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, extremism, and the protection of others.

Please be aware that where necessary and following consideration and approval by the IT Director and notification to you, we may use auto-forwarding on your school email account.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined. 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, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the School's *Online Safety Policy, Retention and Deletion guidelines, Safeguarding and Child Protection Policy, Equal Opportunities Policy* and *Data Protection Policy*. The Retention and deletion guidelines can be found in SMC, All staff, data protection.

Retention of digital data

Staff should be aware that all emails sent or received on school systems will be deleted after 2-3 years of them leaving and email accounts will generally be deleted within one year of leaving the School.

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g., for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives, or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information 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 retention and deletion guidelines.

If you consider that reasons exist for the retention and deletion guidelines not to apply or need assistance in how to retain and appropriately archive data, please contact the IT Director and Assistant Bursar.

Breach reporting

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. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data.
- any external hacking of the school's systems, e.g. through the use of malware
- application of the wrong privacy settings to online systems.
- misdirected post, fax, or email.
- failing to bcc recipients of a mass email.
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (i.e., 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 School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, please notify the Assistant Bursar, Director of IT and the Bursar.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. 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, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence (where relevant).

Please see the *Data Breach Guidance* on SMC, All staff, data protection.

Breaches of this policy

A deliberate breach of this policy by staff will be dealt with as a disciplinary matter using the School's usual applicable procedures. In addition, a deliberate breach by any person may result in the School restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the *Online Safety Policy*, or you are concerned that a member of the School community is being harassed or harmed online you should report it to a Designated Safeguarding Lead and HR. Reports will be treated in confidence wherever possible.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to HR. I understand and accept this acceptable use policy:
Name: ……

Signature: ……
Date: ……