ICT Acceptable Use Policy

Document control	
Document title	**ICT Acceptable Use Policy**
Document status	Approved by SLT
Author	Mrs Claire Gilding-Brant (SDH)
Effective date	September 2024
Version	V.7
Date of next review	September 2025
Location	Website/OneNote/Network

Version	Author	Date	Changes
V6	CGB	Jan 2024	Reference to Prevent Duty added following Prevent Risk Assessment
V.7	CGB	22.08.24	Reviewed No change needed

CONTENTS

1. Policy Statement

This policy defines the acceptable use of the School IT systems and applies to all members of the School community.

Access to the School IT systems is not intended to confer any status of employment on any contractors.

Adherence to the policy is a condition of access.

2. Online Behaviour

The School cannot guarantee the confidentiality of content created, shared and exchanged *via* School systems.

As a member of the School community, you should adhere to the following principles:

- ensure that online communications, and any content shared 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 (e.g. content that is obscene, promotes violence, discrimination, extremism or raises safeguarding issues)
- 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. Pupils and parents are advised not to attempt to discover or contact the personal email addresses or social media accounts of staff.

3. Using the School's IT systems

Whenever you use the School IT systems (including by connecting your own device to the network) you should adhere to the following principles:

- only access School IT systems using your own username and password, and do not share your username or password with anyone else
- do not attempt to circumvent the content filters or other security measures, 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
- remember that the use of the School IT systems is monitored and that the School can view content accessed or sent *via* its systems.

4. Passwords

Passwords protect the School network and computer system and are your responsibility. They should not be obvious (e.g. password, 123456, a family name or birthdays) and they should not be the same as your widely-used personal passwords.

You should not let anyone else know your passwords or keep a list of passwords where they may be accessed. Passwords must be changed immediately if they appear 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.

5. Use of Property

Any property belonging to the School should be treated with respect and care and used only in accordance with any training provided. You must report any faults or breakages without delay to the IT Technician.

6. Use of 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, be aware of the School's right to monitor and access web history and email use.

7. Use of Personal Devices or Accounts and Working Remotely

There may be times when it is necessary or convenient to access Office 365 on a personal device.

Please observe the following rules when doing so:

- School data should not be transferred to commercial cloud service providers (e.g. DropBox) that have not been approved for School use due to the potential data protection risks (Office 365 is the cloud storage, e-mail and communications system used by the School)
- do not download any School data to your computer hard drive
- do not choose to 'remember' usernames and passwords when signing in to Office 365
- always log out when finished.

8. 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 specifically the Prevent Duty) and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. 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.

9. Compliance with Related School policies

You should ensure that you comply with the School E-Safety Policy.

10. Retention of Digital Data

Staff and pupils must be aware that all emails sent or received on School systems will be kept in archive whether or not deleted, and email accounts will be closed and the contents archived within one month of that person leaving the School.

Important records should not be kept in personal email folders, archives or inboxes, nor in local files. 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 email deletion protocol.

11. Breach Reporting

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

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 includes 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 such as:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data
- any external hacking of the School 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 it is necessary to notify the ICO.

If either staff or pupils become aware of a suspected breach, it should be reported immediately to 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. 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.

The School's primary interests and responsibilities are in assessing the effectiveness of its policies and procedures and to protect potential victims.

12. Breaches of Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter. In addition, a deliberate breach may result in your access to School IT systems being restricted.

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 DSL, Mrs Claire Gilding-Brant.

Reports will be treated in confidence.

Acceptance of this policy

Staff:

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Mrs Narene Hall, HR Manager

I understand and accept this Acceptable Use policy:

Name: …….

Signature: ……

Date: ……

Pupils:

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Mrs Crombie, Registrar

I understand and accept this Acceptable Use policy:

Name: …….

Signature: ……

Date: ……