ICT Acceptable Use Policy

Document control	
Document title	**ICT Acceptable Use Policy**
Document status	Approved by SLT
Author	Mr Sean Hatton
Effective date	September 2026
Version	V.9
Date of next review	September 2027
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
V8	HD	18.09.2025	Names – CGB removed as DSL Explicit mention that students are not allowed to use their own laptops in school
V9	SH	Sept 2026	Change of roles

CONTENTS

1. Policy Statement

This policy defines the acceptable use of the School's IT systems and applies to all pupils, staff, Governors, Trustees, contractors, volunteers, visitors, agency staff and other users who access the School's IT systems, devices, networks or data.

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. Legal framework and guidance

- Keeping Children Safe in Education 2026
- Education (Independent School Standards) Regulations 2014
- DfE Meeting Digital and Technology Standards in Schools and Colleges
- Prevent Duty Guidance
- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Equality Act 2010
- DfE Generative AI: Product Safety Standards

3. Online Behaviour

Users should not have an expectation that communications or activity undertaken using School systems are private. School systems may be subject to appropriate filtering, monitoring, logging and access in accordance with this policy, the School's safeguarding arrangements and data protection requirements. 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, harmful, discriminatory, abusive, threatening, sexually inappropriate or otherwise unsuitable for the School environment (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
- do not respond to suspicious emails, messages or links, or provide passwords, authentication codes or other confidential information in response to unsolicited requests. Suspected phishing, social engineering or other cyber-security incidents must be reported immediately in accordance with the School's cyber-security procedures.

If a user accidentally accesses material that is illegal, harmful, inappropriate or otherwise concerning, they should not download, save, copy or share the material. They should report the incident immediately to the appropriate member of staff or, where appropriate, the DSL/IT Support.

Staff should not use their personal email or social media accounts to contact pupils or parents. Staff must use approved School communication channels when communicating with pupils or parents about School matters. Pupils and parents are advised not to attempt to discover or contact the personal email addresses or social media accounts of staff.

4. 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
- Where multi-factor authentication (MFA) is provided or required by the School, users must use it and must not share authentication devices, codes or approval requests 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.

Staff and pupils must confirm that they have read, understood and agree to comply with this policy at the start of each academic year and whenever significant changes are made.

5. 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. Users must report suspected compromise of their account immediately to IT Support.

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.

6. 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.

7. 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.

Users should be aware of the School's right to monitor and access web history and email use.

8. Artificial Intelligence

Generative AI tools may only be used where they have been approved or permitted by the School. Users must not enter confidential, sensitive or personal information into generative AI tools unless the School has specifically approved the tool and its use for that purpose. Users must follow the School's AI Policy and any instructions issued by the School regarding the use of AI in teaching, learning, assessment or administration.

AI-generated content must not be used to create, access, share or distribute harmful, discriminatory, abusive, sexually explicit or otherwise inappropriate material.

9. 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.

10. 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 and conduct 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. All pupils are equipped with a Microsoft Surface. To effectively filter and monitor, use of personal laptops is not permitted.

Where a pupil requires a personal device or alternative technology as a reasonable adjustment for a disability or additional need, the School will consider appropriate arrangements to ensure that the device can be used safely and securely.

Staff must not use personal accounts or devices for School business unless this is expressly permitted by the School. Where a personal account or device has been used for School business in breach of this policy, the School may take appropriate steps to secure, retrieve or investigate School information, in accordance with applicable law, the School's data protection procedures and relevant employment policies. Any examination of personal information or devices will be limited to what is necessary, lawful and proportionate.

Where generative AI tools are used within the School, the School will consider whether its filtering and monitoring arrangements can identify relevant risks associated with AI-generated content.

The Governing Body/proprietor has strategic oversight of the School's ICT, filtering, monitoring and cyber-security arrangements and will receive appropriate assurance that these systems are effective and reviewed regularly.

11. Filtering and monitoring

The School operates appropriate filtering and monitoring systems to safeguard pupils and staff from illegal, inappropriate and potentially harmful online content and activity. Filtering prevents access to identified illegal, inappropriate or harmful content. Monitoring identifies and alerts the School to potentially concerning activity. Neither system is guaranteed to prevent all harmful online activity, and filtering and monitoring are therefore part of a wider safeguarding approach.

The Designated Safeguarding Lead has lead responsibility for safeguarding aspects of filtering and monitoring and works closely with IT Support and senior leaders.

Filtering and monitoring provision is reviewed at least annually and following significant changes to technology, working practices or safeguarding risks. The School conducts regular checks of its filtering and monitoring systems and records the checks undertaken, findings and resulting actions.

Monitoring alerts and reports are reviewed by appropriately trained staff. Safeguarding concerns identified through filtering or monitoring are referred to the DSL and managed in accordance with the Child Protection and Safeguarding Policy.

All users are informed that filtering and monitoring systems are in operation. Monitoring is undertaken lawfully, proportionately and transparently and in accordance with the School's data protection policies and privacy notices.

The School's filtering and monitoring arrangements form part of its wider Prevent strategy and are informed by the School's Prevent risk assessment. Concerns relating to radicalisation, extremism or terrorist content will be managed in accordance with the Child Protection and Safeguarding Policy and Prevent procedures.

12. Compliance with Related School policies

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

13. Retention of Digital Data

School email and other digital records will be retained in accordance with the School's Records Retention Schedule and applicable data protection requirements. Deletion of an email by an individual user does not necessarily result in its immediate deletion from School systems where retention is required for legitimate operational, legal, safeguarding or regulatory purposes.

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. This helps ensure that important information is retained appropriately and remains accessible to authorised staff.

14. Breach Reporting

The School must assess all suspected personal data breaches in accordance with its Data Protection and Data Breach Procedures. Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the School will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, the School will consider whether those individuals must also be informed without undue delay. The School will

keep a record of all personal data breaches, including those that do not require notification to the ICO.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
- insecure disposal.

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.

Cyber-security incidents, including suspected phishing, malware, ransomware, unauthorised access or compromised accounts, must be reported immediately to IT Support in accordance with the School's Cyber Security Incident Response Procedure.

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

15. Breaches of Policy

A deliberate or serious breach of this policy may result in appropriate action under the School's relevant disciplinary, behaviour, safeguarding or contractual procedures. In addition, a deliberate breach may result in your access to School IT systems being restricted.

Safeguarding concerns should be reported to the DSL or a Deputy DSL. Technical concerns, including suspected cyber-security incidents or filtering/monitoring failures, should be reported to IT Support. Where a concern involves both safeguarding and technical issues, both routes should be used. 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, Director of HR

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: ……