Merchant Taylors' School

ONLINE SAFETY, DIGITAL SAFEGUARDING AND ACCEPTABLE TECHNOLOGY USE POLICY (E-SAFETY)

Policy Custodian: *Senior Master*
Approving Body: *MTS Senior Leadership Team*
Approved: *May 2026*
(This policy does not apply to Merchant Taylors' Prep.)

Contents

1. Purpose

This policy sets out how Merchant Taylors' School safeguards pupils, staff, systems and data in the use of digital technology, online services, AI tools and connected devices. It addresses safeguarding, conduct, data protection and educational risks arising from generative AI, mobile devices, social platforms, cloud services and off-site access, and ensures compliance with statutory guidance including KCSIE, September 2025.

2. Scope

This policy applies to all members of Merchant Taylors' School community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of School ICT systems and connectivity, both within and outside of the grounds of Merchant Taylors'.

3. Definitions

Core Safeguarding and Technical Terms

For the purposes of this policy, the following definitions apply to ensure clarity and consistency in the interpretation of online safety, safeguarding and technology use.

Online Safety (E-Safety)
The protection of pupils and staff from harm when using digital technologies, including the internet, mobile devices, social platforms, gaming environments and emerging technologies such as artificial intelligence.

Filtering
The restriction of access to online content through technical controls designed to block harmful, illegal or inappropriate material.

Monitoring
The active or retrospective review of user activity on School systems and devices to identify safeguarding concerns, misuse, or security risks.

Safeguarding Incident
Any online or digital activity that may pose a risk to the safety, wellbeing or welfare of a pupil or member of staff, including but not limited to bullying, exploitation, exposure to harmful content, or inappropriate contact.

Cyber Security Incident
An event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of the School's systems or data.

Devices and Access

School Systems
All ICT infrastructure, networks, cloud services, platforms and applications provided, managed or approved by the School.

Personal Device (BYOD – Bring Your Own Device)
Any device not owned or managed by the School but brought onto site or used to access School systems, including smartphones, tablets and personal laptops.

Remote Access
Access to School systems from outside the School network, including via VPN, cloud services or web-based platforms.

AI and Emerging Technologies

Artificial Intelligence (AI)
Computer systems capable of performing tasks that typically require human intelligence, including generating text, images, audio or code.

Generative AI
A form of AI that creates new content (e.g. text, images, video or audio) based on user prompts.

Approved AI Tools
AI systems that have been reviewed and authorised by the School for use by staff and/or pupils.

Data Protection

Personal Data
Any information relating to an identified or identifiable individual.

Sensitive or Safeguarding Data
Personal data that requires a higher level of protection due to its nature, including safeguarding records, health information, behavioural records and pastoral concerns.

Behaviour and Conduct

Acceptable Use
Use of School systems and devices in a manner that is safe, lawful, respectful and aligned with School policies.

Misuse
Any use of School systems or devices that breaches School policy, including attempts to bypass filtering, access inappropriate content, or engage in harmful behaviour.

Online safety is a shared responsibility across the School. Specific roles have defined accountability to ensure that safeguarding, monitoring, filtering and the appropriate use of technology are implemented effectively and consistently.

4. Roles and Responsibilities

Strategic Oversight

Role	Key Responsibilities
Governing Body / Proprietor	• Provides strategic oversight of online safety and digital safeguarding • Receives regular assurance that filtering and monitoring systems are effective • Ensures policies, procedures and training are compliant with statutory

Role	Key Responsibilities
	guidance (including KCSIE) • Reviews serious incidents and emerging risks where appropriate
Senior Master	• Leads on the implementation and review of the School's online safety policy. • Ensures alignment between safeguarding, IT systems and pastoral processes. • Works with the DSL to ensure effective oversight of filtering and monitoring.

Safeguarding Leadership

Role	Key Responsibilities
Designated Safeguarding Lead (DSL)	• Leads on online safety in line with KCSIE. • Reviews and acts on monitoring reports (e.g. SENSO). • Ensures safeguarding concerns are recorded in CPOMS and followed up. • Identifies trends and informs pastoral and curriculum responses.
Pastoral Team	• Follows up safeguarding concerns identified through monitoring. • Supports pupils affected by online safety incidents.

Technical & Operational Management

Role	Key Responsibilities
Head of IT	• Ensures filtering and monitoring systems are effective and compliant. • Maintains security of School systems and data. • Reports safeguarding or misuse concerns to the DSL immediately. • Supports investigations with technical evidence.
IT Technical Support Team	• Implements and maintains monitoring and security systems. • Supports reporting and system updates. • Assists with safeguarding investigations where required.

Educational Delivery

Role	Key Responsibilities
Director of Digital Strategy	• Leads delivery of online safety and digital literacy in the curriculum. • Oversees safe and appropriate use of AI in teaching and learning.
Teachers	• Embed online safety within teaching and learning. • Supervise pupil use of technology. • Report concerns in line with safeguarding procedures.

Users

Role	Key Responsibilities
Pupils	• Use technology safely and responsibly. • Report concerns or inappropriate content. • Follow School rules on AI and acceptable use.
Parents / Carers	• Support the School's online safety expectations. • Report concerns to the School promptly. • Reinforce safe and appropriate technology use at home. • Do not attempt to access pupil accounts without permission.

5. Network Security

- The School expects that devices remain powered on during the School day where required to support updates, monitoring and operational continuity. Devices are powered down at the end of the day in line with School procedures and energy management controls.
- The School requires that staff and pupils read and sign the School's IT Acceptable Use Policy before being granted access to systems. Access to the School network is provided through unique, auditable usernames and passwords.
- The School provides all pupils with an individual network username and requires them to use and protect a personal password, which must not be shared with others (including parents).
- The School provides all pupils with access to the Internet and a School-approved email account through their individual login credentials.
- The School requires that all email accounts are protected with multi-factor authentication, in line with the School's cyber insurance requirements.
- The School requires that users do not access systems using another individual's account, and that pupils must not use staff login credentials.
- The School provides shared network areas for staff and pupils and supports users in storing and accessing their work appropriately.
- The School expects users to log off devices when not in use or when leaving them unattended.
- The School expects devices to be used appropriately during the School day and powered down at the end of the day in line with operational and energy-saving requirements.
- The School requires that devices issued to staff are used solely for professional purposes.
- The School restricts remote access to School systems and permits access only through approved and secure methods.
- The School restricts third-party or external access to systems to cases where there is a clear professional need and ensures such access is controlled through approved secure arrangements.
- The School provides staff and pupils with access to approved resources via School systems (including SharePoint) using secure authentication.
- The School maintains a wireless network secured to appropriate enterprise-level standards suitable for educational use.

Password Policy

The School requires all staff and pupils to keep passwords private at all times. Passwords must not be shared with others, written down where they can be found, or used by anyone other than the authorised account holder.

All users are issued with unique usernames and are responsible for maintaining the confidentiality of their login credentials.

Passwords for School systems must:

- Be at least 15 characters in length.
- Be strong and difficult to guess.
- Avoid obvious personal information, common words or predictable patterns.
- Comply with any additional technical requirements applied by the School.

Users must not reuse any of their previous three passwords.

The School follows current security guidance in requiring password changes only where there is reason to believe that a password has been forgotten, disclosed or compromised, or where a reset is otherwise required for security reasons.

Where required or available, multi-factor authentication must be enabled in accordance with School security requirements.

Security and Resilience Measures

The School implements a range of technical and organisational measures to reduce cyber risk and support the security, availability and resilience of its systems and data. These measures are designed to be proportionate to the School's size, infrastructure and risk profile.

Key controls include:

- **Access Control and Authentication**
  The School enforces secure access to systems through unique user accounts, strong password requirements and multi-factor authentication where appropriate.
- **Network Security**
  The School uses appropriate network security controls, including firewalls, filtering systems and endpoint protection, to protect against unauthorised access, malware and cyber threats.
- **Monitoring and Threat Detection**
  Systems are monitored to detect suspicious activity, misuse and potential security incidents. Alerts and logs are reviewed and acted upon where necessary.
- **Data Backup and Recovery**
  The School maintains regular backup arrangements to ensure that critical systems and data can be restored in the event of system failure, data loss or cyber incident.
- **System Maintenance and Updates**
  Systems, software and applications are kept up to date to reduce vulnerabilities and maintain security.
- **Access Restrictions and Least Privilege**
  Access to systems, data and administrative functions is restricted to authorised users based on role and necessity.
- **Remote Access Security**
  Remote access to School systems is restricted and secured through approved methods and authentication controls.
- **Security Testing and Review**
  The School undertakes periodic security reviews and testing, including external assessment where appropriate, to identify and address vulnerabilities.
- **User Awareness and Phishing Protection**
  The School provides ongoing awareness and training to reduce the risk of phishing and other user-targeted attacks.

These measures are reviewed regularly to ensure they remain effective and aligned with current threats, best practice and statutory guidance.

Business Continuity and Resilience
To support business continuity in the event of a system outage or cyber incident, the School maintains secure, segregated access to a limited set of non-sensitive operational documents required to support the immediate running of the School.

These documents are:

- Strictly limited to operationally essential, non-sensitive information.
- Stored separately from the main School network.
- Subject to appropriate access controls and periodic review.

No personal, confidential or safeguarding data is stored within this provision.

6. Expected Conduct and Acceptable Use

In the School, all users:

- Are responsible for using the School ICT systems in accordance with the relevant Acceptable Use Policy.
- Must understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Must understand the importance of adopting good E-Safety practice when using digital technologies out of School and realise that the School's E-Safety Policy covers their actions out of School, if related to their membership of the School.

Staff

Staff must read and comply with the School's Online Safety Policy and use the School ICT systems accordingly, including the use of School smartphones, and hand-held devices including touch-screen tablets issued to staff. WhatsApp groups that are created by staff on School smartphone for the purposes of communication during a School trip must be deleted upon return of the trip to the School.

Pupils

Pupils must use School systems and digital technologies safely, responsibly and in accordance with the School's Acceptable Use requirements.

Pupils are expected to:
develop appropriate research skills and respect copyright and academic integrity.

- Use artificial intelligence tools in accordance with School rules and guidance.
- Use School-provided systems, including email, as part of their routine learning.
- Report any concerns, misuse or harmful content immediately to a member of staff.
- Not attempt to bypass filtering, monitoring or device controls.

Pupils must confirm that they understand and will comply with these expectations through the School Agreement.

Any misuse of School systems will be addressed in line with the School's behaviour and safeguarding procedures.

7. Filtering and Monitoring

The School implements appropriate filtering and monitoring systems to safeguard pupils, staff and systems, in line with statutory guidance including *Keeping Children Safe in Education (KCSIE)*.

The School's approach to filtering and monitoring is informed by the DfE *Filtering and Monitoring Standards* and is subject to regular review to ensure it remains effective and proportionate.

These systems are designed to:

- protect users from harmful or inappropriate content
- identify safeguarding concerns and misuse
- support a safe and secure digital environment

7.1 Filtering

The School uses appropriate filtering systems to restrict access to harmful, illegal or inappropriate online content.

Filtering is applied to all School-managed networks and devices and is proportionate to the age and needs of users. Staff are provided with less restrictive access than pupils where appropriate for professional purposes.

Filtering controls include, but are not limited to, the restriction of content relating to:

- **Illegal:** content that is unlawful, including material related to criminal activity, child abuse or terrorism
- **Bullying:** content that involves harassment, intimidation or abusive behaviour
- **Child Sexual Exploitation:** content that involves or promotes the exploitation or abuse of children
- **Discrimination:** content that promotes prejudice or discrimination against individuals or groups
- **Drugs / Substance Abuse:** content that promotes or facilitates the use of illegal or harmful substances
- **Extremism:** content that promotes extremist ideologies, terrorism or intolerance
- **Gambling:** content that promotes or facilitates gambling activities
- **Malware / Hacking:** content that promotes or enables unauthorised access to systems or malicious activity
- **Pornography:** content that depicts explicit sexual material
- **Self-Harm:** content that promotes or depicts self-harm, including eating disorders
- **Violence:** content that promotes or depicts physical harm or aggression
- **Suicide:** content that encourages or provides guidance relating to suicide
- **AI-Generated Harmful Content:** misleading or harmful content created using artificial intelligence, including deepfakes
- **Anonymous Communication Platforms:** platforms that enable anonymous interaction and may present increased safeguarding risk

The School regularly reviews filtering effectiveness and maintains records of requests to unblock content for legitimate educational purposes.

7.2 Monitoring

The School implements monitoring systems to identify safeguarding concerns, misuse and potential security risks.

Monitoring is proportionate, risk-based and operates in line with safeguarding and data protection requirements.

Monitoring arrangements include:

- the review of user activity on School devices and systems
- automated alerts for concerning language, behaviour or activity
- escalation of safeguarding concerns to the Designated Safeguarding Lead (DSL)
- recording of incidents in safeguarding systems (e.g. CPOMS)

The School uses appropriate systems and external services, where necessary, to support effective monitoring and timely response to concerns.

7.3 Network and Web-Based Monitoring

The School uses monitoring systems across its network and cloud services to support safeguarding, behaviour management and system security.

Monitoring arrangements include:

- Monitoring of activity on School-managed devices during the School day to support safeguarding and classroom management.
- Monitoring of cloud-based platforms (including Microsoft Teams), where user activity may be subject to review when accessed via a School account.
- Automated alerts to identify concerning language, behaviour or activity.
- Escalation of high-risk alerts to safeguarding staff for immediate action; and
- Periodic review of monitoring data to identify trends and inform safeguarding, pastoral and curriculum responses.

Monitoring is:

- Proportionate and limited to what is necessary.
- Applied in line with safeguarding and data protection requirements; and
- Subject to appropriate oversight and review.

Monitoring may apply where a user accesses School systems or platforms using their School account, including on devices not owned by the School.

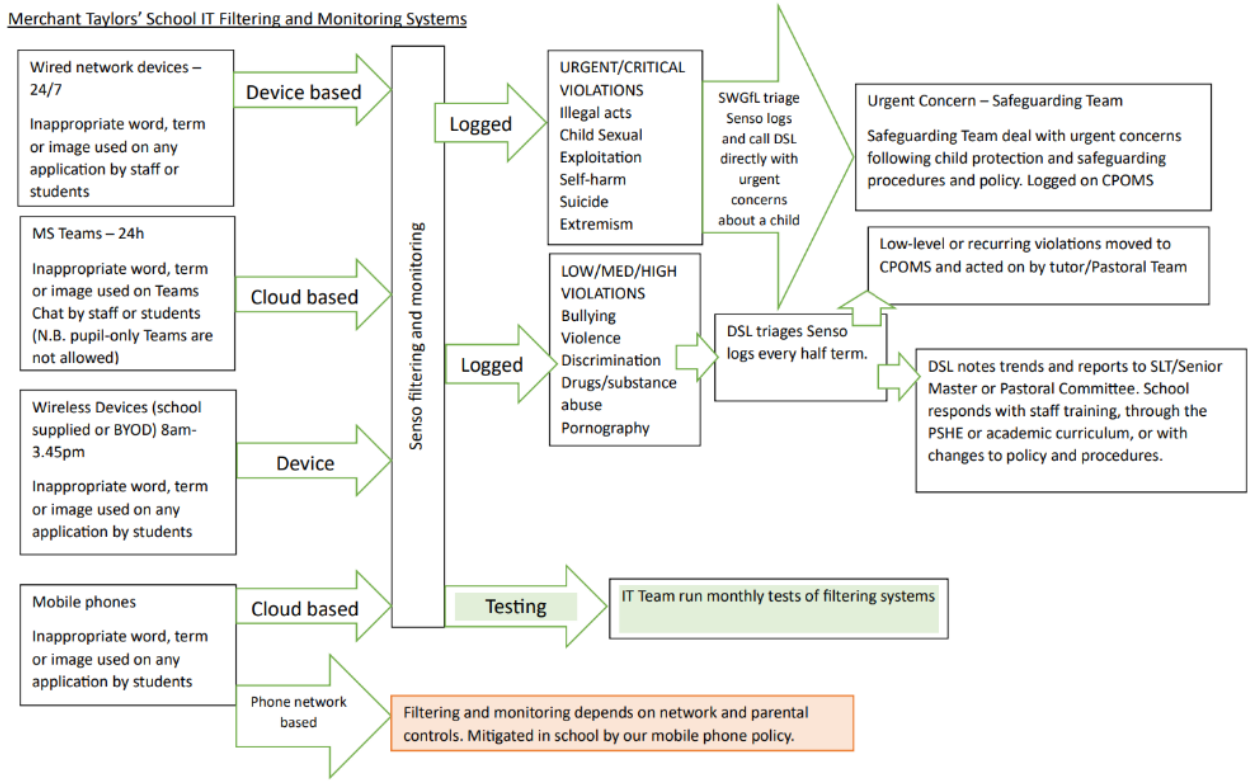
Safeguarding Response and Oversight

The School uses monitoring systems, including endpoint and cloud-based monitoring tools, to identify potential safeguarding concerns and misuse.

Monitoring alerts are reviewed and, where appropriate:

- Escalated to the Designated Safeguarding Lead (DSL).
- Recorded in safeguarding systems (e.g. CPOMS).
- Followed up by safeguarding and pastoral teams.

Where external monitoring support services are used, high-risk alerts are escalated promptly to enable timely safeguarding action.



Monitoring data is also reviewed periodically to identify trends and inform safeguarding strategy, including pastoral interventions and curriculum development.

Scope of Monitoring

Monitoring is applied to School-managed devices and systems and may extend to School platforms accessed using a School account.

This includes:

- Monitoring of pupil activity on School devices during the School day to support safeguarding and classroom management.
- Monitoring of School devices and platforms, including cloud-based systems such as Microsoft Teams.
- Application of monitoring controls where School systems are accessed on non-School devices.

Where a pupil accesses School platforms using their School account, activity may be subject to monitoring even when using a device not owned by the School.

Safeguarding Protocols

A summary of the School's safeguarding monitoring and response processes is illustrated below:

7.4 Review and Oversight

Filtering and monitoring arrangements are reviewed regularly to ensure they remain effective, appropriate and aligned with statutory guidance.

The Governing Body receives assurance that filtering and monitoring arrangements are in place, effective and reviewed regularly in line with statutory guidance.

The Designated Safeguarding Lead (DSL), Senior Master and IT team work together to:

- review monitoring reports and trends
- ensure appropriate safeguarding responses
- maintain oversight of system effectiveness

8. AI and Emerging Technologies

The School recognises that artificial intelligence (AI), including generative AI, presents both educational opportunities and safeguarding risks. The use of AI must be safe, ethical, and aligned with the School's expectations on academic integrity and data protection.

Use of AI by Pupils

Pupils may use AI tools for learning purposes where permitted by the School and under staff guidance. Acceptable uses may include:

- Supporting revision and independent study
- Generating ideas or explanations
- Improving understanding of subject content

Pupils must not:

- Submit AI-generated work as their own unless explicitly permitted
- Use AI tools to cheat, plagiarise, or misrepresent authorship
- Use AI to generate harmful, inappropriate or misleading content
- Input personal, sensitive or safeguarding-related information into AI tools

Use of AI by Staff

Staff may use AI to support teaching, administration and professional practice where appropriate. Staff must:

- Use only approved AI tools where these are specified by the School
- Ensure that AI use does not compromise safeguarding, confidentiality or data protection
- Not input personal, confidential or safeguarding data into public AI systems
- Review and validate AI-generated outputs before use

Safeguarding and Risk

The School has regard to current Department for Education guidance on the use of generative AI in education.

The School recognises safeguarding risks associated with artificial intelligence, including:

- misinformation, disinformation and bias
- over-reliance on AI tools
- impersonation, deepfakes and synthetic media
- inappropriate or harmful content generation

Any misuse of AI which impacts safeguarding, wellbeing or academic integrity will be treated as a serious matter and managed in line with the School's safeguarding and behaviour policies.

Governance

The School will:

- Maintain oversight of AI use and emerging risks
- Provide guidance and education to staff and pupils
- Review approved tools and practices regularly in line with national guidance, including DfE publications

9. Mobile Phones, BYOD and Personal Devices

The use of mobile phones and personal devices is governed by the ***MTS Code of Use for Mobile Telephones*** policy. The use of personal devices must also comply with this policy, including expectations relating to safeguarding, acceptable use, filtering and monitoring.

10. Staff Communication and Professional Boundaries

Staff must not use personal devices to communicate with pupils or parents unless authorised and using approved systems.

Staff must not use personally owned devices, such as smartphones or cameras, to take photos or videos of pupils and must only use work-provided equipment unless there is an exceptional and unavoidable operational reason. Where a member of staff is required to use a personal device in exceptional circumstances, any images or recordings must be transferred to the School network and deleted from the device as soon as practicable.

Where staff members are required to use a mobile phone for School duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a School mobile phone can be provided and requested.

In an emergency where a staff member doesn't have access to a School-owned device, they must use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Staff must use School-provided email systems for professional purposes. Limited personal use is permitted where appropriate.

Staff must not use email to transfer personal or sensitive data outside approved School systems.

All external communications must be written professionally, may require authorisation, and must comply with the School's communication standards.

Users must:

ensure attachments are appropriate in size and content, in line with system and provider limits;
not send chain messages or unsolicited bulk communications; and
not include advertising or non-School-related promotional content.

Social Media and Online Communication

Staff must not use personal social media or communication platforms to interact with pupils. Communication with pupils must only take place through approved School systems.

Staff must not:

- Reference pupils, parents or colleagues on personal social media.
- Engage in online discussions relating to members of the School community.
- Use personal platforms in a way that could compromise professional boundaries.

Staff must ensure that privacy settings on personal accounts are appropriately configured to reduce risk.

Appropriate use of social media and online communication is addressed through safeguarding induction and reinforced through regular staff guidance and communications.

11. Data Protection and Information Handling

The School is committed to ensuring that all personal data is handled securely, lawfully and in accordance with data protection legislation and safeguarding obligations.

All staff, pupils and users of School systems must ensure that information is handled appropriately and only accessed, used or shared where necessary and authorised.

Handling of Personal and Sensitive Data

Personal data must:

- Only be accessed by authorised users for legitimate School purposes.
- Be kept secure and not disclosed to unauthorised individuals.
- Only be shared using approved School systems and methods.
- Not be transferred to personal devices, personal email accounts or unauthorised platforms.
- Be retained and deleted in accordance with School data retention requirements.

Sensitive or safeguarding data must be treated with a higher level of care and must only be accessed, shared or stored in approved systems with appropriate access controls.

Use of Systems and Storage

School data must only be stored and processed using systems and platforms approved by the School.

Users must not:

- Store School data on personal devices unless explicitly authorised.
- Use personal cloud storage, email accounts or unapproved applications for School business.
- Download, copy or transfer data unnecessarily or without appropriate safeguards.

All access to School systems must be secure and in line with the School's access control and authentication requirements.

Use of Email and Communication Systems

Staff must use School-provided communication systems for professional purposes.

Users must:

- Ensure that emails and communications are appropriate, accurate and professional.
- Take care when sending information externally, particularly where personal data is involved.
- Verify recipients before sending sensitive information.
- Avoid sending personal or sensitive data unless it is necessary and appropriately protected.

Use of Artificial Intelligence and Third-Party Tools

Personal, confidential or safeguarding-related information must not be entered into public or unapproved AI tools or third-party platforms.

Where digital tools are used:

- Only approved systems may be used for School-related activities.
- Data sharing must comply with School policies and data protection requirements.
- Users must ensure that the use of such tools does not compromise confidentiality or safeguarding.

Data Security and Incident Reporting

All users must:

- Report any suspected data breach, loss of data, or unauthorised access immediately to the School.
- Take reasonable steps to protect data from loss, theft or misuse.
- Follow School procedures in the event of a security or data protection incident.

Data protection incidents will be managed in line with the School's incident response procedures and, where necessary, reported in accordance with legal and regulatory requirements.

Business Continuity and Resilience

To support business continuity in the event of a system outage or cyber incident, the School maintains secure, segregated access to a limited set of non-sensitive operational documents required to support the immediate running of the School.

These documents are:

- Strictly limited to operationally essential, non-sensitive information.
- Stored separately from the main School network.
- Subject to appropriate access controls and periodic review.

No personal, confidential or safeguarding data is stored within this provision.

12. Incident Reporting and Response

The School takes all online safety, safeguarding, cyber security and data protection incidents seriously. All users have a responsibility to report concerns promptly so that appropriate action can be taken.

Reporting Concerns

All staff and pupils must report any safeguarding, misuse, or security concern immediately in accordance with the School's safeguarding procedures.

This includes, but is not limited to:

- Exposure to harmful or inappropriate content.
- Online bullying, harassment or inappropriate communication.
- Suspected grooming, exploitation or radicalisation.
- Misuse of School systems or attempts to bypass filtering or monitoring.
- Suspected data breaches or unauthorised access to information.
- Loss or theft of devices containing School data.
- Inappropriate or unsafe use of artificial intelligence tools.

Staff must report concerns to the Designated Safeguarding Lead (DSL) or, where appropriate, the Senior Master or IT team. Pupils must report concerns to a member of staff.

Incident Response

All reported incidents will be assessed and managed in a timely and proportionate manner. The School will take appropriate action to safeguard individuals, secure systems and prevent further harm.

The response to an incident will typically include:

- Identification and initial assessment of the concern.
- Safeguarding action where there is risk to a pupil or member of staff.
- Containment of any technical or data-related issue.
- Investigation of the incident, including review of monitoring data where appropriate.
- Recording of the incident in accordance with School procedures (e.g. CPOMS).
- Follow-up actions, including support, sanctions or further safeguarding measures as required.

Roles and Responsibilities in Incident Management

The **DSL** is responsible for leading safeguarding responses and determining appropriate action where pupil welfare is at risk.

The **IT team** is responsible for investigating technical aspects of incidents, securing systems and providing evidence where required.

The **Senior Master** oversees the implementation of policy and ensures appropriate coordination between safeguarding and technical response.

Where appropriate, incidents may be escalated to senior leadership, external agencies, or relevant authorities.

Data Protection and Cyber Incidents

Where an incident involves personal data or cyber security risk, it will be managed in line with the School's data protection obligations.

This may include:

- Assessment of the risk to individuals.
- Implementation of measures to contain and mitigate the impact.
- Notification to relevant authorities where required.
- Communication with affected individuals where appropriate.

Recording and Review

All incidents must be recorded accurately and securely. The School will review incidents and trends to:

- Inform safeguarding practice.
- Improve systems and controls.
- Identify emerging risks.
- Support staff training and pupil education.

Conduct and Sanctions

Misuse of School systems or breaches of this policy may result in disciplinary action in accordance with the School's behaviour and staff conduct policies.

Where incidents involve potential criminal activity, the School will involve external agencies as appropriate.

13. Education, Training and Awareness

The School recognises that effective online safety depends on education, awareness and a culture of vigilance. Online safety, digital safeguarding and responsible technology use are embedded across the School community.

Staff Training

All staff receive appropriate training to ensure they understand their responsibilities in relation to online safety, safeguarding, data protection and the use of technology.

This includes:

- Safeguarding and online safety training as part of staff induction.
- Regular updates and refresher training in line with statutory guidance (including KCSIE).
- Guidance on the safe and appropriate use of technology, including artificial intelligence.
- Awareness of current risks, trends and emerging issues.

Staff must understand how to recognise, respond to and report online safety concerns in accordance with School procedures.

Pupil Education

Online safety is embedded within the curriculum and wider School life to ensure that pupils develop the knowledge and skills required to use technology safely and responsibly.

This includes:

- Teaching pupils about safe and responsible use of the internet, social media and digital technologies.
- Developing understanding of risks such as bullying, exploitation, misinformation and inappropriate content.
- Promoting critical thinking and digital literacy, including the safe and ethical use of artificial intelligence.
- Reinforcing expectations around acceptable use, behaviour and academic integrity.

Online safety education is responsive to emerging risks and informed by trends identified through monitoring and safeguarding processes.

Parent and Carer Awareness

The School works in partnership with parents and carers to promote online safety.

The School will:

- Provide information and guidance to support safe technology use at home.
- Communicate emerging risks and relevant updates where appropriate.
- Encourage parents and carers to report concerns to the School promptly.

Ongoing Awareness and Culture

The School promotes a culture in which online safety is understood as a shared responsibility.

This includes:

- Regular communication and reminders to staff and pupils.
- Responding to current issues, incidents or trends as they arise.
- Reinforcing expectations through assemblies, pastoral systems and communications.
- Ensuring that online safety remains a visible and integral part of School life.

Review and Development

The School will review its education and training provision regularly to ensure that it remains effective, relevant and aligned with current guidance and emerging risks.

14. Review, Audit and Governance

The School is committed to ensuring that its online safety, digital safeguarding and technology use arrangements remain effective, proportionate and aligned with statutory guidance and best practice.

Policy Review

This policy will be reviewed at least annually, or more frequently where:

- There are significant changes in technology or safeguarding risk.
- Statutory guidance is updated (including KCSIE).
- Incidents or monitoring indicate a need for change.

Updates will be approved by the appropriate leadership body.

Monitoring and Assurance

The School maintains ongoing oversight of filtering, monitoring and safeguarding arrangements.

This includes:

- Regular review of filtering and monitoring systems to ensure they are effective and appropriate.
- Analysis of safeguarding incidents and trends.
- Assurance that systems are operating in line with statutory requirements.
- Review of user behaviour and emerging risks.

The Designated Safeguarding Lead (DSL), Senior Master and IT team work together to ensure that monitoring arrangements are effective and proportionate.

Governance and Oversight

The Governing Body / Proprietor provides strategic oversight of online safety and digital safeguarding.

This includes:

- Receiving regular assurance on the effectiveness of filtering and monitoring systems.
- Reviewing safeguarding risks, trends and serious incidents where appropriate.
- Ensuring that policies, procedures and training remain compliant with statutory guidance.
- Supporting a culture of safe and responsible technology use across the School.

Audit and Evaluation

The School will periodically review and evaluate its online safety and cyber security arrangements to ensure continuous improvement.

This may include:

- Internal reviews of systems, processes and incidents.
- External security assessments or penetration testing.
- Review of training provision and curriculum effectiveness.
- Evaluation of new and emerging technologies, including artificial intelligence.

Continuous Improvement

Findings from monitoring, incidents, audits and reviews will be used to:

- Strengthen safeguarding practice.
- Improve technical controls and procedures.
- Inform staff training and pupil education.
- Update policies and guidance where required.