The Sutton Academy

Cyber Security Policy

Status	**Non-Statutory**
Responsible Governors' Committee	**ALT**
Date last approved by GB	**Not Applicable**
Responsible Person	**Mr N Marsh**
To Review Date	**February 2028**
Last Amended Date	**February 2026**

1. Purpose

This policy establishes how The Sutton Academy protects its digital systems, data, and users from cyber threats. It ensures that students, staff, and visitors use technology safely, responsibly, and in line with legal and safeguarding requirements.

2. Scope

- All staff, students, governors, contractors, and visitors
- All devices used on academy premises or to access academy systems (academy-owned or personal)
- All digital platforms, networks, and data managed by The Sutton Academy

3. Roles and Responsibilities

Principal

Overall responsibility for policy implementation and cyber security strategy.

Academy Leadership Team

- Ensure the academy meets legal and regulatory requirements
- Provide resources for secure systems and training
- Approve and review this policy annually

IT Network Manager / Technical Staff

- Maintain secure networks, servers, and devices
- Monitor systems for threats or misuse
- Manage user accounts, permissions, and backups
- Ensure software and security patches are up to date

Staff

- Follow all cyber security procedures
- Report suspicious activity or breaches immediately
- Protect passwords and sensitive information
- Model safe and responsible digital behaviour
- Follow the Staff Acceptable Use Policy (AUP) at all times

Students

- Use academy technology responsibly and respectfully
- Never attempt to access systems, accounts, or data they are not authorised to use
- Report concerns to a teacher or safeguarding lead
- Follow the Student Acceptable Use Policy (AUP) at all times

Parents and Carers

- Support the academy's approach to online safety
- Encourage responsible use of technology at home

4. Access Control

Passwords

- Must be strong, unique, and kept confidential
- Must not be shared with anyone
- Staff must change passwords if they suspect compromise

User Accounts

- Every user receives an individual account
- Access is granted based on role and reviewed regularly
- Accounts are disabled when a user leaves the academy
- Account activity is monitored

5. Device Security

Academy-Owned Devices

- Must be used for educational or work-related purposes
- Must not be altered or used to install unauthorised software
- Must be locked when unattended

Personal Devices (BYOD)

- Only permitted where authorised by the academy
- Must connect only to designated networks
- Must not store sensitive academy data unless approved

6. Network and Data Protection

Network Security

- Firewalls, filtering, and monitoring systems are in place
- Unauthorised access attempts are logged and investigated
- Anti-virus and anti-malware software on all devices
- Multi-factor authentication (MFA) for critical systems
- Users must not bypass filters or use VPNs/proxies

Data Protection

- Personal data is handled according to UK GDPR and the Data Protection Act 2018
- Sensitive data must be encrypted when stored or transmitted

- Data must only be accessed for legitimate educational or operational purposes

Backups

- Critical data is backed up regularly
- Backups are stored securely and tested periodically

7. Email and Communication Safety

- Academy email accounts must be used for academy business
- Users must not open suspicious links or attachments
- Phishing attempts must be reported immediately
- Staff must verify unexpected requests for sensitive information

8. Software and Updates

- Only approved software may be installed on academy devices
- Automatic updates must remain enabled
- Unlicensed or pirated software is strictly prohibited

9. Online Behaviour and Acceptable Use

- Bullying, harassment, or inappropriate content is not tolerated
- Students must follow Acceptable Use Policy
- Staff must follow Acceptable Use Policy
- Staff must maintain professional conduct online
- Social media use must not compromise the academy's reputation

10. Incident Reporting and Response

All cyber security incidents must be reported immediately to the ICT Network Manager or a member of ALT. Incidents include:

- **Suspected hacking or unauthorised access** - any activity suggesting someone has gained access to systems, accounts, or data without permission, including unusual login attempts, unexpected password resets, or unfamiliar devices on the network.
- **Lost or stolen devices** - laptops, tablets, phones, USB drives, or any equipment containing or accessing organisational data. Even if the device is encrypted, the loss must still be reported.
- **Malware infections** - viruses, ransomware, spyware, or any suspicious behaviour such as pop-ups, system slowdowns, unknown applications installing themselves, or files being encrypted or deleted.
- **Data breaches** - any accidental or deliberate loss, disclosure, or alteration of personal, confidential, or sensitive information. This includes emails sent to the wrong recipient, files shared incorrectly, or unauthorised downloads.

- **Phishing attempts** - suspicious emails, messages, or calls attempting to obtain passwords, financial information, or access to systems. Even if no information was provided, the attempt must be reported.

The academy will:

- Investigate promptly
- Contain and mitigate the issue
- Inform affected individuals where required
- Report serious breaches to the ICO if legally necessary

Immediate reporting allows the academy to activate the appropriate containment, investigation, and recovery steps outlined in the Cyber Response Plan. This document provides detailed procedures for isolating affected systems, preserving evidence, communicating with stakeholders, and restoring normal operations.

11. Training and Awareness

- Staff receive regular cyber security training
- Students are taught safe online behaviour
- Awareness campaigns run throughout the year

12. Policy Review

This policy is reviewed annually by the Academy Leadership Team to ensure it remains effective, relevant, and aligned with organisational needs. The review process considers new cyber threats, including changes in attack methods, vulnerabilities, and trends that may affect the organisation’s risk profile.

Changes in legislation are monitored to ensure compliance with data protection laws, regulatory requirements, and sector-specific guidance. Any updates required to meet legal obligations are incorporated promptly.

Technological developments are assessed to ensure the policy reflects current systems, tools, and security capabilities. As new technologies are adopted or existing ones evolve, the policy is updated to provide clear expectations and guidance for their secure use.