Academies Trust

# Information Security Policy

Policy details

- Date created: December 2024
- Date approved: 01/10/2026
- Date implemented: 01/10/2026
- Last review date: September 2026
- Next review date: September 2027
- Policy owner: Chief Operations Officer

Released: July 2024 v1.0

This document will be reviewed annually and sooner when significant changes are made to the law.

# Contents


1. Introduction 3
2. Scope and Responsibilities 3
3. IT Acceptable Use Standards 4
**4. Governance, Roles and Responsibilities 4**
    4.1 Trust Board and governance 4
    4.2 Executive and senior leadership 4
    4.3 Head of IT 5
    4.4 Cyber & Information Security Manager 5
    4.5 IT staff 5
    4.6 Academy and Heads of Service 5
    4.7 Data Protection and Safeguarding 5
    4.8 All users 5
5. Principles of Use 6
6. Network Access and Data Security 7
    6.1 Users' Authorisation 7
    6.2 Starters, Movers and Leavers (Account Creation, Approval and Removal process) 8
    6.3 External Support Access 8
    6.4 Confidentiality 9
    6.5 Security of Portable Devices 9
    6.6 Physical Security 9
    6.7 Administrative Access 9
**7. Device and Endpoint Security 10**
**8. Vulnerability, Security Update and Patch Management 10**
**9. Filtering and Monitoring 11**
**10. Artificial Intelligence 11**
11. Disposal of Computing Resources 12
12. Backup Procedures 12
13. Disaster Recovery Procedures 13
14. Breaches of Policy 13

## 1. Introduction

- The Trust's information technology infrastructure, digital services and information are essential to the effective delivery of education, safeguarding, administration and wider Trust operations. The increasing use of cloud services, connected devices and digital information also creates risks to confidentiality, integrity, availability, privacy, safeguarding and operational continuity.

  Co-op Academies Trust is committed to protecting its information, systems and services from accidental or deliberate loss, misuse, unauthorised access, disclosure, alteration, disruption or destruction. Information security is an organisational responsibility and is not solely the responsibility of the IT team.

  This policy establishes the Trust's overarching information security requirements and supports compliance with applicable legislation, statutory guidance, the Department for Education (DfE) Digital and Technology Standards for Schools and Colleges, Keeping Children Safe in Education (KCSIE), National Cyber Security Centre (NCSC) guidance and the Trust's wider governance arrangements.
- The Trust adopts a risk-based and defence-in-depth approach to security. Security controls will be proportionate to the sensitivity and criticality of the information or service being protected and to the risks faced by the Trust.
- This policy should be read in conjunction with the Trust's Colleague Code of Conduct, the Data Protection Policies, the Acceptable Use Policy, and Bring Your Own Device (BYOD) Policy (N.B The BYOD policy is in draft and due to be finalised and published in 2027)

## 2. Scope and Responsibilities

This policy applies to:

- Trustees and Members
- Community Council Members
- All Trust employees
- Any contractors who have access to the Trust's systems
- Any volunteers who have access to the Trust's systems

All users are responsible for reading, understanding and complying with this procedure if they have access to the Co-op Academies Trust IT networks, accounts, systems and services. Whilst this policy applies to all users, the Trust understands that pupils will need additional support to understand the Acceptable Use Policy and Agreement and will need to be taught how to use IT systems safely and securely.

## 3. IT Acceptable Use Standards

All users must:

1. Protect Trust IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
2. Protect individuals from harmful or inappropriate material accessible via the Internet or electronic media.
3. Protect the confidentiality of individuals and of Trust matters and safeguard users by complying with relevant legislation, including:
    - Data Protection Act 2018 and UK General Data Protection Regulation
    - Privacy and Electronic Communications Regulations
    - Copyright, Designs and Patent Act 1988
    - Computer Misuse Act 1990
    - Counter-Terrorism and Security Act 2015 (encompassing the "Prevent Duty")
    - The Regulation of Investigatory Powers Act (RIPA) 2000
    - Waste Electrical and Electronic Equipment Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.
    - The Department for Education Digital and Technology Standards for Schools and Colleges
    - Keeping Children Safe in Education (KCSIE)

Users should understand and adhere to their signed Acceptable Use Agreement.

## 4. Governance, Roles and Responsibilities

### 4.1 Trust Board and governance

The Trust Board is ultimately accountable for ensuring that the Trust meets its legal and regulatory obligations and maintains appropriate oversight of information and cyber security. Relevant committees will receive appropriate assurance on significant risks, incidents and improvement activity.

### 4.2 Executive and senior leadership

The Executive and Senior Leadership Teams are responsible for supporting effective information security governance, ensuring appropriate resources and organisational arrangements are in place, and ensuring significant risks are appropriately escalated and managed.

### 4.3 Head of IT

The Head of IT is responsible for the strategic leadership of technical information and cyber security across the Trust, including the design and oversight of appropriate security controls, resilience, technical standards, assurance and improvement activity.

### 4.4 Cyber & Information Security Manager

The Cyber & Information Security Manager is responsible for coordinating the Trust's operational cyber security programme, including:

- cyber risk management and assurance;
- vulnerability management and security monitoring;
- incident response and cyber resilience;
- security policies, standards and technical assurance;
- supporting compliance with DfE, NCSC and other applicable requirements;
- security awareness activity and advice;
- coordination of security testing and remediation tracking.

### 4.5 IT staff

IT staff are responsible for implementing and maintaining security controls within their areas of responsibility, following approved standards and procedures, reporting security weaknesses and incidents, and supporting academies and central teams to use technology securely.

### 4.6 Academy and Heads of Service

Headteachers, academy leaders, line managers and heads of service are responsible for ensuring that access is appropriate to users' duties, that staff follow Trust requirements, and that information security, safeguarding and business continuity requirements are embedded in local working practices.

### 4.7 Data Protection and Safeguarding

The Data Protection Officer and relevant data protection colleagues provide advice and oversight in relation to data protection obligations. Designated Safeguarding Leads and the central Safeguarding Team are responsible for safeguarding decisions and work with IT colleagues on filtering, monitoring and cyber incidents where there may be a safeguarding impact.

### 4.8 All users

Every user is responsible for protecting Trust information and systems, following security and acceptable use requirements, completing required training, protecting authentication credentials and reporting suspected incidents or weaknesses promptly.

## 5. Principles of Use

For the purpose of this policy, the use of the internet will include associated internet-enabled technologies such as, cloud based systems (such as Google Workspace, Arbor and CPOMS), emails, video calls, video messaging, instant messaging, webinar applications and conferencing applications.

Internet and email use is integral to the effective delivery of services provided by the Trust. Nothing in this policy should be read as restricting the proper use of email, internet or associated technologies for academy or Trust purposes.

Limited personal use of the Trust's Internet is permitted subject to these principles and guidance notes.

- Personal use of the Internet is only permitted in your own time (e.g. before or after work and during your lunchtime) and limited to browser-based activities.
    - Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the Trust's email, Internet and associated systems may result in disciplinary action.
- Users are not permitted to use the Co-op Academy Trust's email system for personal communication.
- If you feel you may have accidentally breached this policy, you should contact your line manager immediately, or, in their absence, a more senior manager who will address the situation.
- The Trust reserves the right to maintain, monitor and review usage logs of the Academy / Trust IT services including the internet and associated internet-enabled technologies including emails, video calls, video messaging, instant messaging, webinar applications or conferencing applications and AI Prompts for both staff and students. Auditing and monitoring of the use of Academy / Trust IT services may form part of disciplinary procedures.
- The Trust has in place a process to block categories of internet sites and individual sites if it is deemed appropriate. Users must not attempt to bypass security measures or processes.
- Any personal information sent via email, the Internet and associated internet-enabled services is covered by Data Protection legislation. All staff are required to handle personal information in accordance with the Data Protection Act 2018 and the UK GDPR.

- Emails, including conversations recorded using facilities such as video calls, instant messaging or conferencing applications, are covered by the Freedom of Information (FOI) Act and may be disclosed as part of an FOI request for information, or as part of any legal proceedings. Always exercise the same caution on email content, video calls, instant messaging or conferencing applications as you would in more formal correspondence.
- Whilst Trust security provides additional protection and real-time scanning, our security measures cannot guarantee that external communications do not contain malicious content or links. All staff, and any other individuals with access to the IT network (with the exception of pupils and students), must take basic cyber security training annually in line with DfE Cyber Security Standards and RPA Insurance requirements.
- Consent from all parties must be obtained before recording conversations when using facilities such as video calls, instant messaging or conferencing applications.
- The Trust reserves the right to withdraw Internet access or email use or any access to the Academy / Trust's computer or communications network, if the User is found to be in breach of this policy.
- Desktop and document sharing capabilities via facilities such as video calls or conferencing applications, must only be used with colleagues of the Trust for collaboration purposes. If you allow changes to be made to these documents during a desktop sharing session as the 'sharer' of the document, it is your responsibility to ensure that the documentation is used correctly and saved appropriately.
- Any Trust approved systems are to be used and associated with Trust based email and logins, personal email addresses are prohibited.
- Personal cloud storage services are not to be used to store work related data and should not be accessed on academy devices.

## 6. Network Access and Data Security

### 6.1 Users' Authorisation

Those accessing information systems, data or services will be authorised to do so by an appropriate authority, usually their line manager.

Changes to access must be requested and authorised. Users who believe they have access to systems they no longer need, must report this to their line manager.

Users must only access information held on the Trust's computer systems if authorised to do so and the information is needed to carry out their work.

Line managers will only request the minimum access required for the user to carry out their work.

A record of user access to systems will be maintained and periodically reviewed.

### 6.2 Starters, Movers and Leavers (Account Creation, Approval and Removal process)

Line managers must ensure that access to IT Systems is only available to employees during their period of employment and withdrawn as soon as employment is terminated.

The same principles apply to pupils joining and leaving the academies.

A new starter, mover and leaver process must be in place in the Trust and each Academy which may include external suppliers, a record of this should detail:

1. The names of the systems Users have been given access to
2. The date the access was enabled
3. The level of access (role)
4. The name of the authoriser

This process should also include changed access due to promotion, secondment, or demotion.

When a contract of employment ends, the member of staff must return all equipment, including peripherals, in full working condition.

It is the responsibility of the user to backup any data or documents they may require, prior to returning the device. Any data pertaining directly to the Trust, academies or members of the academies' communities must not be retained by the former employee.

Retaining any personal data without the authorisation of the Trust is an offence under the Data Protection Act 2018.

The user account and all personal work stored on the laptop will be securely deleted upon return.

### 6.3 External Support Access

Staff providing temporary guest logins for external support services providers must ensure that system access does not extend beyond the requirements for the provision of services.

Those requesting/providing temporary access must also ensure that system access is withdrawn as soon as the affiliate's relationship with the Trust / Academy ceases.

### 6.4 Confidentiality

Under no circumstances should personal or other confidential information held on the Academy / Trust network or IT equipment be disclosed to unauthorised persons. If you accidentally access information which you are not entitled to view, report this immediately to the data protection officer (if a central colleague) or the relevant academy's data protection ambassador.

Staff must ensure that confidential or sensitive data is not accessible to unauthorised persons, by logging off or locking the computer when it is left unattended.

In classrooms, screens must be set to extend to the Interactive whiteboard rather than duplicate and when using screen sharing facilities, users should fully close or minimise screens with any sensitive data / emails.

### 6.5 Security of Portable Devices

All data should be stored only within Google Workspace or the relevant cloud platform e.g. Arbor or CPOMS. No data should be stored on a local device, network storage or removable storage device.

Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the Trust.

All Trust devices used to store personal information will be fully encrypted.

### 6.6 Physical Security

Building access and physical controls protect areas where sensitive or confidential information is processed. Server access and access to network equipment, telecoms and network access points is restricted to those staff with authorisation.
A register of personnel that has access to the identified secure areas should be kept at the academy and updated regularly

### 6.7 Administrative Access

Privileged access presents additional risk and must be tightly controlled.
Administrative accounts must:

- be separate from standard user accounts wherever technically possible;
- use strong authentication and MFA;
- only be used when elevated privileges are required;
- not be used for routine activities such as email or general web browsing;
- be uniquely attributable to an individual wherever technically possible;

- be provided only to authorised personnel with a legitimate business requirement;
- be reviewed regularly and removed promptly when no longer required;
- comply with current Trust authentication and privileged-access standards.

Shared administrative credentials should be avoided. Where unavoidable for technical reasons, their use must be controlled, documented and subject to appropriate credential-management arrangements.

## 7. Device and Endpoint Security

Devices used to access Trust information must be appropriately secured and managed according to the risk presented.

- Trust-managed devices must use approved configurations and management controls.
- Supported operating systems, applications and firmware must be maintained.
- Appropriate endpoint protection, anti-malware and other security controls must be deployed where applicable.
- Trust devices storing personal or confidential information must use appropriate encryption.
- Devices must automatically lock after an appropriate period of inactivity and users must lock devices when unattended.
- Unauthorised software and attempts to disable security or management controls are prohibited.
- Remote management and remote wipe capabilities should be enabled where appropriate.
- Lost or stolen devices must be reported immediately.

The use of personal devices for Trust information is only permitted in accordance with the Trust's Bring Your Own Device requirements (TBC) and any technical controls specified by IT.

## 8. Vulnerability, Security Update and Patch Management

The Trust will maintain arrangements to identify, assess and remediate vulnerabilities across devices, applications, cloud services, infrastructure and other technology.

- Security updates and vulnerability fixes must be applied within timescales proportionate to severity, exposure and risk.
- Automatic updating should be used where appropriate and compatible with operational requirements.
- Unsupported or end-of-life technology must not remain in operational use unless a documented risk assessment, mitigation plan and appropriate approval are in place.
- Regular vulnerability assessment and appropriate security testing will be undertaken.

- Identified vulnerabilities will be risk-rated, assigned to an owner and tracked through remediation or formal risk acceptance.

## 9. Filtering and Monitoring

The Trust will maintain appropriate filtering and monitoring arrangements in accordance with KCSIE, the DfE Filtering and Monitoring Standard and the Trust's safeguarding responsibilities.

- Roles and responsibilities for filtering and monitoring must be clearly assigned between Trust leadership, academy leadership, safeguarding and IT.
- Filtering must block illegal, harmful and inappropriate content without unreasonably restricting legitimate teaching and learning.
- Monitoring arrangements must support the Trust's safeguarding needs and enable concerns to be identified and escalated appropriately.
- Filtering and monitoring provision must be reviewed at least annually.
- Appropriate technical checks must be undertaken and recorded, covering relevant sites, devices, networks and user groups.
- Changes to filtering or monitoring controls must follow appropriate authorisation and safeguarding processes.
- Users must not attempt to bypass filtering or monitoring controls.

The effectiveness and appropriateness of filtering and monitoring will be considered in light of emerging technologies and risks, including generative AI.

## 10. Artificial Intelligence

The Trust recognises the potential benefits of artificial intelligence, including generative AI, while also recognising risks relating to information security, data protection, safeguarding, accuracy, intellectual property and confidentiality.

- Only Trust-approved AI services may be used for Trust business where approval is required by Trust guidance.
- Personal, confidential, commercially sensitive, safeguarding or otherwise restricted Trust information must not be entered into public or unapproved AI services.
- Users remain responsible for reviewing, validating and appropriately using AI-generated outputs.
- AI services involving personal data must be assessed in accordance with data protection requirements, including a DPIA where required.
- AI must not be used to circumvent Trust security, safeguarding, procurement or information-governance controls.

More detailed requirements are set out in the Trust’s AI policy.

## 11. Disposal of Computing Resources

Computing resources will be disposed of in line with WEEE (Waste Electrical and Electronic Equipment) regulations, The Hazardous Waste Act, The Environmental Protection Act 1990, The Environment Act 1995 and The Data Protection Act 2018

1. All equipment which contains sensitive files will have their hard disk drives wiped and all sensitive or confidential data and licensed software will be irretrievably deleted during the disposal process.
2. Damaged devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded.
3. If a third party contractor is used, suppliers will be suitably accredited and disposal certification will be obtained.
4. Finally, the Academy / Trust's inventory will be updated.

## 12. Backup Procedures

The Trust ensures that systematic backup of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

| Process | On-site / off-site | Frequency (daily/weekly/monthly) |
|---|---|---|
| All On-Prem Servers | Off-site | Daily |
| Google Workspace | Off-site | Daily |

There should be at least three copies of important data, on at least two separate devices one of which must be off site.  Backup copies will be securely stored against theft, corruption or physical damage, so that in the event of a major incident a backup copy is available.

The retention period for the trust backup solution is 12 months built from daily backups for both On-prem servers and the Google Workspace tenancy.
Backup sets are stored in the cloud with the trust backup provider. All backup sets are replicated with the supplier to provide redundancy and are encrypted using AES-256.

## 13. Disaster Recovery Procedures

In the case of a disaster, staff should refer to the Disaster Recovery Procedure and Plan which includes cyber incidents and the Cyber Response Plan which plan should include the following as per the DfE Cyber Security Standards:

- staff responsibilities
- out of hours contacts and procedures
- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources

Hard copies of key information should be kept in case of total system failure, and the plans should be regularly tested and reviewed.

The Trust should ensure all items are appropriately insured.

## 14. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Trust assets, or an event which is in breach of the security procedures and policies.

All employees, supply staff, Trustees, Community Council Members, contractors, and volunteers have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Trust's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Academy / Trust.

The Trust will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

Suspected misuse of the Trust's computer systems by a member of staff will be considered by the Senior Leaders.  In the case of an individual then the matter may be dealt with under the disciplinary process.