Academies Trust

Education Data Hub

Information Security Policy

Policy details

- Date created: December 2024
- Date approved: 02/10/2025
- Date implemented: 02/10/2025
- Next review date: September 2025
- 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

- The Trust's IT (Information Technology) infrastructure and digital resources are essential to the effective delivery of education and other activities, but they also present risks to data protection, online safety and safeguarding. We are committed to using IT facilities in a way that meets legal requirements and upholds confidentiality and people's privacy rights.
- This policy supports business continuity, data protection and cyber security, and explains how we use technology in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), the Departments for Educational Digital and Technology standards in schools and colleges and other relevant legislation.
- 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 2025)

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 IT network, 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. Roles and Responsibilities

Everyone who works for Co-op Academies Trust has a responsibility to ensure that data is collected, accessed, stored and handled appropriately and lawfully.

The Trust Board is ultimately responsible for ensuring the Trust meets its legal obligations. Operational compliance with the terms of this policy is overseen by the Trust's Senior Leadership Team and by specialist staff in the central team and within each academy.

Breaches of this policy should be reported to a line manager, senior leader, or in an Academy, the headteacher in the first instance.

IT staff are responsible for:

- Maintaining an understanding of this policy in the academy/ies they support
- Implementing and supporting implementation of this policy
- Ensuring that pupils and staff follow the Acceptable Use Policy and that any breaches are reported.
- Working with the Designated Safeguarding Lead (DSL) in each academy and the central Safeguarding Team, and other colleagues who are responsible for

the filtering and monitoring systems and processes, and ensuring any breaches or incidents are reported and logged appropriately.
- Ensuring IT security and cyber incidents are reported and logged appropriately.
- Working with the Digital Lead in order to ensure that students are kept safe from potentially harmful and inappropriate content and contact.

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 email use 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.
- Only use Trust approved systems

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

The Trust does not allow the use of USBs / removable storage devices.

Sensitive or confidential information should be accessed via the network and should not be permanently stored on portable devices e.g. memory sticks / laptops / tablets.

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.

6.7 Administrative Access

- Administrative accounts and credentials must use strong authentication / complex passwords. Current guidance on the authentication and security measures that should be put into place for network devices, filtering and monitoring services and administrative accounts can be found in the DfE Digital Standards.
- Administrative accounts should have passwords of at least 12 characters including special characters and use MFA where available.
- Administrative accounts must not be used for general activities, especially those of high-risk, such as browsing the internet or emailing.
- Administrative access is only provided to designated staff and a review of administrators for each system will be carried out termly, including administrative accounts that have not been used for a prolonged period of time, in line with the DfE Cyber Security Standards.

7. 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.

8. Backup Procedures

If software/hardware problems arise, a device may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all Users to ensure that files are saved to network drives or cloud-based networks.

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	On and Off-site	Daily
Google Workspace	Off-site	Daily

There should be at least three backup 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-premises servers and the Google Workspace tenancy. Backup sets are primarily stored in the Cloud with the Trust backup provider with a replication of the backup; all backup sets are encrypted using AES-256.

9. 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.

10. 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.