Cybersecurity Policy

Author	Alison Anderson
Policy Title	Cyber Security Policy
Approval Date	July 2025
Approved By	LGB
Adopted Date	November 2025

Statement of Intent:

ACT Multi Academy Trust (ACT) is committed to maintaining the confidentiality, integrity, and availability of its information and ensuring that the details of the finances, operations and individuals within the Trust are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The Trust recognises that breaches in security can occur. In schools, most breaches are caused by human error, therefore all staff should know how to minimise the risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyberattacks the Trust will make sure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impact of any security breach, to alert the relevant authorities and to take steps to prevent a repeat occurrence.

Table of Contents

1. Purpose

This policy outlines the approach of ACT Multi Academy Trust (MAT) to managing cyber security risks. It ensures the protection of digital systems, data, and users across all schools within the Trust.

The policy supports compliance with UK GDPR, the Data Protection Act 2018, and the Department for Education (DfE) Cyber and Information Security Manual.

2. Scope

This policy applies to all staff, governors, trustees, contractors, volunteers, and pupils using MAT-owned or personal devices for school-related activities. It covers all digital systems, networks, and data owned or managed by the Trust.

3. Legal & Regulatory Framework

This policy is informed by the following legal and regulatory documents:

- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018

- The Children's Code (Age Appropriate Design Code)

- DfE Cyber and Information Security Manual

- Academies Trust Handbook (2024–2025)

- Computer Misuse Act 1990

4. Roles & Responsibilities

The following roles are responsible for implementing and maintaining cyber security across the Trust:

- Trust Board: Strategic oversight and risk governance.
- CEO / Executive Head: Ensures policy implementation and compliance.
- Data Protection Officer (DPO): Oversees data protection and breach response.
- IT Manager / Network Admin: Implements technical controls, monitors systems, and responds to incidents.
- School Leaders: Enforce policy at school level and ensure staff compliance.
- All Staff: Follow safe practices, complete training, and report incidents.
- Pupils & Parents: Use systems responsibly and report concerns.

The ACT Trust Board will be responsible for:

- Ensuring the Schools/Trust has appropriate cyber-security measures in place.
- Ensuring the Schools/Trust has an appropriate approach to managing data breaches in place.
- Support relevant staff in the delivery of the Policy.

The CEO/Headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.

- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Schools' Online Safety Policy and Procedures.
- Organising training for staff members in conjunction with the online safety officer.

The DPO will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading the Trust response to incidents of data security breaches, including leading the cyber recovery team.
- Assessing the risks to the school in the event of a cyber-security breach.
- Ensuring a log of cyber-security incidents in maintained.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations need to be notified following a data security breach, and ensuring they are notified.
- Working with IT Support after a data breach to determine where weaknesses lie and improve security measures.
- Keep up to date with data security, network security and preventing breaches.
- Monitor and review the effectiveness of this policy and communicating any changes to relevant staff.

The Director of Safeguarding / DSL will be responsible for:

Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made. All members of staff will be responsible for:

- Understanding their responsibilities regarding this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

5. Policy Areas

This section outlines the technical and procedural controls in place to protect the Trust's digital infrastructure.

5.1 Access Control

- All users are assigned unique credentials. Passwords must meet NCSC complexity standards and be changed regularly.

- Multi-factor authentication (MFA) is required for administrative systems.

- Example: Staff accessing the MIS system must use MFA and have role-based access permissions.

5.2 Device & Network Security

An inventory will be kept of all ICT hardware and software currently in use across the Trust, including mobile phones and other personal devices provided by the school/Trust.

The inventory will be stored in the central office of each academy and will be audited on a termly basis to ensure it is up to date. Any changes to the ICT hardware will be documented using the inventory and checked before use and the central document will be updated inline.
Systems should be audited on a termly basis by IT Support to ensure the software is up to date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security and will be recorded in the inventory. Any software that is out of date or reaches its 'end of life' will be removed from systems e.g., when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore. All hardware, software and operating systems will require passwords from individual users. Passwords will be changed regularly to prevent access to facilities which could compromise network security. In line with Trust regulations 2 step authentication will be used when accessing software when not in the ACT tenancy. ACT will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's)- Cyber Essentials. These are:

- **Firewalls:** Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure Configuration:** The default configuration on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The Trust will remove or disable any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access Control:** The more people have access to data the larger the chance of a security breach. The Trust will ensure that access is given on a 'need to know' basis to help protect data. All accounts will be protected with strong passwords and two-factor authentication (where needed).
- **Malware Protection:** The Trust will protect itself from malware by installing antivirus and antimalware software and using techniques to protect any malware issue.
- All devices must have endpoint protection and automatic updates enabled.
- Networks are segmented to separate administrative, curriculum, and guest traffic.
- Example: Guest Wi-Fi is isolated from internal systems to prevent unauthorized access.

5.3 Data Protection & Privacy

- Data is encrypted at rest and in transit. Data minimisation principles are applied.

- Data Protection Impact Assessments (DPIAs) are conducted for new systems.

- Example: Before deploying a new parent communication app, a DPIA is completed and reviewed by the DPO.

5.4 Children's Data & EdTech

- EdTech providers must comply with the Children's Code and UK GDPR.

- Parental consent is obtained where required.

- Example: An online learning platform is assessed for age-appropriate design and profiling risks.

5.5 Email & Communication Security

- Email filtering and anti-phishing tools are implemented.

- Sensitive data is only sent via encrypted channels.

- Example: Staff are trained to identify phishing emails and report them to IT.

5.6 User Awareness & Training

- All staff complete annual cyber security and data protection training.

- Pupils receive age-appropriate digital safety education.

- Example: Year 6 pupils participate in Safer Internet Day workshops.

5.7 Incident Response & Breach Management

Types of Security Breaches and Causes

1. Unauthorised use without damage to data - involves unauthorised persons accessing data on the school system, e.g., hackers who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the school, e.g., schools where pupils access systems that staff have left open and/or logged into, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.
2. Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it onto another person who is not authorised to view it, e.g., a staff member with authorised access who passes the data to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.
3. Damage to physical systems – Involves damage to hardware in the school/Trust IT system, which may result in data being inaccessible to either or both but can be accessed by unauthorised persons.
4. Unauthorised damage to data – Involves an individual person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.
5. Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence.

- Accidental breaches can occur because of human error or insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches can occur because of a hacker wishing to cause damage to the school through accessing and altering, sharing, or removing data. Breaches caused by negligence can occur because of a staff member knowingly disregarding School/Trust Policies and procedures or allowing pupils to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school/Trust software more vulnerable to a virus.
- Incorrect firewall settings being applied, e.g., unrestricted access to the school network, can allow unauthorised individuals to access the school system.
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten.

All incidents are reported to the IT Manager and DPO immediately.

The Incident Response Plan includes containment, eradication, recovery, and notification.

- Example: A ransomware attack is isolated, backups are restored, and the ICO is notified within 72 hours.

5.8 Third-Party & Cloud Services

- Due diligence is conducted on all suppliers. Data Processing Agreements (DPAs) are required.

- Cloud services must meet ISO 27001 or equivalent standards.

- Example: A cloud-based HR system is reviewed for compliance and security certifications.

5.9 Remote Learning & Working

- VPN access is provided for remote staff. Devices must meet Trust security standards.

- Only approved platforms (e.g., Microsoft 365, Google Workspace) are used.

- Example: Staff working from home use Trust-issued laptops with VPN and endpoint protection.

6. Incident Reporting Best Practices

- All staff must report cyber incidents immediately to the IT Manager and DPO.

- Use the Incident Log Template to record details such as date, systems affected, and actions taken.

- Notify the ICO within 72 hours if personal data is involved.

- Example: A phishing email that results in credential theft is logged, contained, and reported.

7. Monitoring & Compliance

The Trust conducts regular audits, penetration testing, and reviews of access logs. Non-compliance may result in disciplinary action.

8. Policy Review

This policy is reviewed annually or following significant incidents, regulatory changes, or the introduction of new technologies.

Appendix A: Incident Log Template

Date & Time of Incident	Reported By	Description of Incident	Systems Affected	Severity Level	Actions Taken	Resolution Date	Follow-up Notes

Appendix B: Staff Onboarding Cyber Security Checklist

[ ] Received and read Cyber Security Policy

[ ] Completed cyber security induction training

[ ] Set up secure password and MFA

[ ] Received Trust-issued device (if applicable)

[ ] Trained on acceptable use of email and internet

[ ] Aware of incident reporting procedures

[ ] Signed staff declaration form

Enhancements from the Academy Trust Handbook 2024

Internal Scrutiny

- The Audit and Risk Committee must oversee cyber security controls as part of internal scrutiny.
- Regular reviews of cyber risk management, incident response plans, and compliance with DfE's Risk Protection Arrangement (RPA) are required.
- Cyber security audits should be documented and findings reported to the Trust Board.

Risk Management

- Cyber risk must be included in the Trust's risk register and reviewed termly.
- Trusts must assess the likelihood and impact of cyber threats and implement proportionate controls.
- Cyber insurance coverage should be reviewed annually to ensure adequacy.

Incident Response

- Trusts must maintain a cyber incident response plan aligned with DfE guidance.
- All incidents must be logged, investigated, and reported to the ESFA if they involve significant disruption or data loss.
- Post-incident reviews must be conducted to identify lessons learned and improve resilience.

Governance Responsibilities

- Trust Boards are accountable for ensuring effective cyber security governance.
- The Accounting Officer must ensure that cyber security is embedded in operational and strategic planning.
- Trusts must provide cyber security training to trustees and senior leaders annually.

Appendix C: DfE-Recommended Platforms and Tools

Examples of DfE-Recommended Platforms and Tools:

1. Productivity & Collaboration:
   - Microsoft 365 for Education (Teams, OneDrive, SharePoint, Outlook)
   - Google Workspace for Education (Google Classroom, Meet, Drive, Gmail)

2. Security & Endpoint Protection:
   - Microsoft Defender for Endpoint
   - Sophos Intercept X
   - Cisco Umbrella

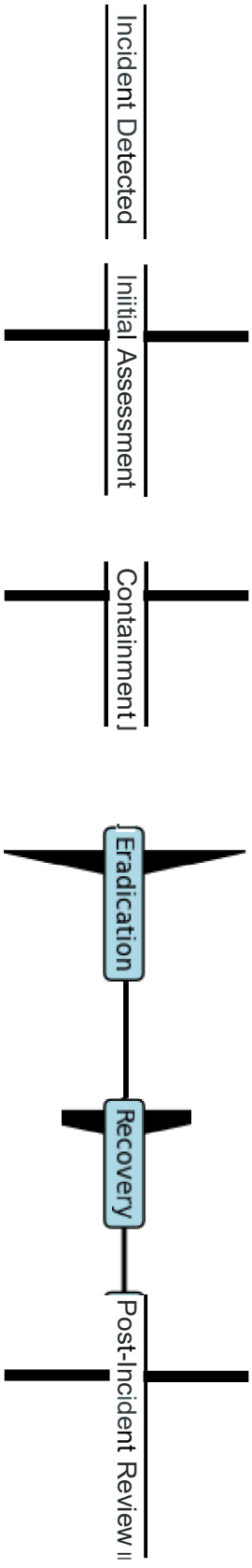
3. Backup & Recovery:
   - Redstor
   - Datto

4. Filtering & Monitoring:
   - Smoothwall
   - Securly

5. Remote Access & VPN:
   - Fortinet
   - Cisco AnyConnect

Appendix D: Incident Response Flowchart

This flowchart outlines the steps from detection of a cyber incident through containment, recovery, and post-incident review.



Appendix E: Access Control Hierarchy

This diagram illustrates the hierarchy of access permissions from Trust Board to Students

Access Control Hierarchy:

- Trust Board: Full access to strategic systems and reports
- CEO & DPO: Access to sensitive data and compliance systems
- Headteachers: Access to school-level systems and staff data
- IT Support: Access to infrastructure and user management
- Staff: Access to curriculum and communication tools
- Students: Access to learning platforms

Appendix F: Password Policy Matrix

This table summarizes password requirements and change frequency for different user groups.

Password Policy Matrix

User Group	Password Length	Change Frequency	2FA Required
Trust Board	12+ characters	Every 90 days	Yes
Staff	10+ characters	Every 90 days	Yes (off-site)
Students	8+ characters	Every term	No
IT Admins	16+ characters	Every 60 days	Yes

Appendix G: Audit Schedule Table

This table provides a quick reference for audit types, their frequency, and responsible parties.

Audit Schedule

Audit Type	Frequency	Responsible Party
Network Security Audit	Termly	IT Support
Software Inventory Check	Termly	IT Support
Policy Compliance Review	Annually	DPO
Incident Log Review	Quarterly	DPO

Appendix H: Cyber Awareness Infographic

This infographic highlights key cyber hygiene practices for staff training and awareness.