

The 3-18 Education Trust

Cyber Security Policy

‘Every individual is in a great school.’

Approved: Spring Term 2026
Review: Spring Term 2027

www.3-18education.co.uk



Our Mission

To celebrate the diverse nature, culture and identity of our individual schools, whilst collaborating and enjoying the benefit of the team.

Our Values

Compassionate

To show care and understanding towards others.

Accomplished

To provide high quality education and training for all.

Resilient

To be solution focused and able to intelligently manage challenges.

The 3-18 Education Trust

101 Longden Road
Shrewsbury
SY3 9PS

Company Number: 08064698

Policy Monitoring and Review

Monitoring

The IT Director, in conjunction with the CEO and DPO, will monitor the outcomes and impact of this policy on an annual basis and whenever significant changes occur in technology, threat landscape or regulatory requirements.

This monitoring includes:

- Once developed, annual review and testing of the incident response plan using NCSC Exercise in a Box
- Annual third-party audit of cyber security controls
- Regular review of filtering, monitoring and access controls
- Review of any cyber security incidents and lessons learned

This policy will be updated as required to reflect changes in legislation, NCSC guidance, DfE standards, Jcq regulations and insurer requirements.

Linked Policies

This policy should be read alongside:

Information Security Policy and Procedure

ICT and Internet Acceptable Use Policy

Data Protection Policy

Data Breach Procedure

Online Safety Policy

Use of Artificial Intelligence Policy

Operation of CCTV Procedure

Protection of Pupils' Biometric Information and Consent to use Biometric Data

Records Management Policy and Retention Schedule

Member of Staff Responsible	IT Director
Relevant Guidance/Advice/Legal Reference	UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, NCSC Cyber Security for Schools, KCSIE 2024, Jcq General Regulations for Approved Centres, DfE Digital and Technology Standards
Policy Adopted By	Board of Trustees
Date of Policy	Spring Term 2026
Review Period	Annually
Date of Next Review	Spring Term 2027

Contents

1. Purpose and Scope.....	5
2. The Trust's Cyber Security Framework.....	5

Protect	5
Detect	6
Respond	6
Recover	6
3. Roles and Responsibilities	6
Board of Trustees and Local Governors	6
Chief Executive Officer and Senior Leaders	7
IT Director and IT Manager	7
Data Protection Officer	7
School Business Managers	7
All Staff	7
Exams Officers and Staff Involved in Examinations	7
4. Account Management	7
5. Training and Awareness	8
Appendix A: JCQ Examination Cyber Security Requirements	9
Appendix B- School Level Responsible Persons	11

1. Purpose and Scope

- 1.1. This policy establishes the cyber security framework for The 3-18 Education Trust (The Trust). It brings together and supplements the Trust's existing policies to provide a single, coherent reference point for cyber security across all Trust schools.
- 1.2. The policy applies to all trustees, local governors, employees, contractors, volunteers and any third parties authorised to use the Trust's IT systems. It has particular relevance for staff involved in the management, administration and conducting of examinations and assessments.
- 1.3. This policy does not replace the Trust's existing policies. Detailed provisions on the topics below are set out in the following documents, which should be read alongside this policy:
 - Information Security Policy and Procedure – physical security, digital access controls, password requirements, encryption, data storage, homeworking, and breach reporting
 - ICT and Internet Acceptable Use Policy – acceptable/unacceptable use, filtering and monitoring, protection from cyber-attacks, data security standards, and the cyber security glossary
 - Data Protection Policy – lawful processing, data subject rights, DPIAs, and security measures for personal data
 - Data Breach Procedure – identification, containment, assessment, ICO notification, and reporting
 - Online Safety Policy – safeguarding, filtering and monitoring standards, cyber-bullying
 - Use of Artificial Intelligence Policy – AI-specific cyber security, JCQ assessment integrity, data protection for AI tools, and AI-enabled threats
- 1.4. Where this policy addresses a topic covered in detail in an existing policy, it provides a summary and cross-reference rather than restating the full provisions. This avoids duplication and ensures that updates need only be made in one place.

2. The Trust's Cyber Security Framework

- 2.1. The Trust's approach to cyber security is based on the National Cyber Security Centre (NCSC) guidance for schools and the DfE's digital and technology standards. It is built on four principles: protect, detect, respond, and recover.

Protect

- 2.2. The Trust implements the following preventative controls. Full details are set out in the Information Security Policy and Procedure and the ICT and Internet Acceptable Use Policy:
 - Firewalls and network security controls across all Trust sites
 - Anti-virus and anti-malware software on all devices, configured for automatic updates
 - Regular software updates and patch management
 - Full disk encryption on all devices used to access Trust systems
 - Multi-factor authentication (MFA) for all staff email accounts and all external access to Trust systems
 - Role-based access controls with regular reviews by the IT Support Team
 - Secure configuration and monitoring of cloud services (Microsoft 365, SharePoint, OneDrive)

- Supply chain security checks, including verification of Cyber Essentials certification where appropriate
- Prompt removal of access for leavers

Detect

2.3. Detection measures include:

- Automated filtering and monitoring systems configured to DfE standards
- Monitoring of AI-related phishing, fraud and unauthorised access attempts (see Use of AI Policy, Section 9)
- Routine review of user accounts for suspicious, unusual or unauthorised activity
- Regular access reviews to verify that each user has only the level of access required for their current role
- Annual third-party audit (such as 360 Degree Safe) to objectively test effectiveness of controls

Respond

2.4. The Trust will develop, review and test an incident response plan with the IT department. This plan will cover how the Trust will communicate if communications go down, who will be contacted and when, and who will notify Action Fraud. Once in place, the plan will be reviewed and tested annually, and after any significant event, using the NCSC's Exercise in a Box.

2.5. Key response principles:

- All suspected or confirmed cyber security incidents must be reported immediately to the IT Manager, IT Director or School Business Manager
- Staff must not attempt to resolve an IT security breach without first consulting the IT Manager, IT Director or School Business Manager (see Information Security Policy)
- Where personal data is compromised, the Data Breach Procedure must be followed, including ICO notification within 72 hours where required
- The Trust will not engage with ransom demands from ransomware attacks

2.6. Where a cyber-attack impacts learner data, assessment records or learner work, the relevant awarding body or bodies must be contacted immediately (see Appendix A)

Recover

2.7. The Trust's recovery arrangements include:

- Daily backup of critical data to Barracuda servers
- Tested recovery procedures to restore systems and data following an incident
- Delegation of MIS security responsibility to the Arbor platform provider
- Post-incident review to identify lessons learned and update controls accordingly

3. Roles and Responsibilities

3.1. Detailed role descriptions for information security are set out in the Information Security Policy and Procedure and the ICT and Internet Acceptable Use Policy. This section summarises the cyber-security-specific responsibilities.

Board of Trustees and Local Governors

- Oversee the Trust's cyber security strategy and ensure it is given appropriate time and resources

- Review cyber security arrangements and policy compliance

Chief Executive Officer and Senior Leaders

- Overall responsibility for policy implementation across the Trust
- Ensure staff complete annual cyber security training, including at induction

IT Director and IT Manager

- Implement and maintain technical controls, monitor systems, manage access and updates
- Develop, review and test the incident response plan
- Conduct regular access reviews and ensure compliance with Cyber Essentials standards

Data Protection Officer

- Ensure compliance with data protection law in the context of cyber incidents
- Advise on data handling and oversee data breach responses

School Business Managers

- Receive and escalate reports of cyber security incidents at school level
- Support implementation of this policy within their school

All Staff

- Follow this policy and all related Trust policies
- Complete annual cyber security training and report incidents promptly
- Never share passwords, authentication codes or login credentials
- Remain vigilant for phishing, social engineering and other threats

Exams Officers and Staff Involved in Examinations

- Follow the JCQ-specific requirements set out in Appendix A of this policy
- Complete annual certificated cyber security training and retain evidence for inspection

4. Account Management

4.1. The Trust's account management requirements are set out in the Information Security Policy and Procedure (Digital Access Security) and the ICT and Internet Acceptable Use Policy (Passwords). This section summarises the key principles; the full provisions in those policies remain authoritative.

- Password governance follows NCSC guidance. Password length is a more valuable defence than complexity. Staff should use approaches such as three random words to generate suitably secure passwords.
- Every account must have a strong, unique password. The same password must not be reused across accounts.
- MFA is required for all staff email accounts and for external access to Trust systems. Student accounts do not require MFA. MFA must also be enabled on awarding body systems where available.
- Passwords and authentication codes must never be shared. Staff requiring access to a system must request their own user account.

- Exposed or compromised passwords must be changed immediately and reported to the relevant line manager and IT team.
- Staff may use the built-in password manager in Microsoft Edge when signed in with their Trust Microsoft account. Passwords must not be saved in browsers where the user is not signed in with an authenticated Trust profile, or on shared or public devices.
- Account access is reviewed regularly to ensure the minimum level of access required. Accounts are disabled promptly when users leave.

5. Training and Awareness

5.1. The Trust provides annual cyber security training for all staff, with training included in the induction programme for new starters joining outside the annual training window. Training covers:

- Recognising phishing, social engineering and other cyber threats
- Checking sender addresses, verifying requests for payments or information changes
- Creating and managing strong passwords
- The purpose and use of multi-factor authentication
- Reporting incidents and suspicious activity promptly
- Safe use of AI tools in line with the Use of AI Policy

5.2. Staff involved in examinations must additionally complete the JCQ-specific training requirements set out in Appendix A.

5.3. Breach of this policy or related Trust policies will be treated as a disciplinary matter, which may result in action under the Trust's Disciplinary Policy and Procedure, up to and including summary dismissal depending on the seriousness of the breach.

Appendix A: JCQ Examination Cyber Security Requirements

This appendix sets out the additional requirements that apply to all Trust schools operating as approved exam centres, in compliance with the JCQ General Regulations for Approved Centres (sections 3.20 and 3.21) and the JCQ Guidance for Centres on Cyber Security. These requirements are supplementary to the Trust-wide provisions in the main body of this policy. All Trust-wide controls, training and incident response arrangements apply fully to examination systems and data.

A1. Scope

This appendix applies to all staff who have access to awarding body online systems and/or who are involved in the management, administration and conducting of examinations and assessments. This includes, but is not limited to, heads of centre, senior leaders responsible for exams, exams officers and exams assistants.

A2. Awarding Body System Access

- Authorised staff must securely access awarding bodies' online systems in line with awarding body regulations and the JCQ Guidance for Centres on Cyber Security (www.jcq.org.uk/exams-office/general-regulations).
- MFA must be enabled on all awarding body accounts and systems containing exam-related information, where available. Staff must have access to a device that complies with awarding bodies' MFA requirements.
- Access to awarding body systems must be reviewed regularly. Access must be removed when no longer required, including promptly upon staff departure.
- Staff must never approve or authenticate a login request that they did not initiate.

A3. Exam-Specific Account Security

In addition to the Trust-wide account management requirements in Section 4 of this policy, exam staff must:

- Use strong, unique passwords for each awarding body account, following the three random words approach recommended by NCSC
- Never share login details, passwords or authentication codes with anyone, including colleagues
- Set up secure account recovery options using alternate email accounts or phone numbers protected by MFA
- Regularly review and remove access for third-party applications or services that no longer require access to exam-related accounts
- Exercise particular caution with content and services such as quizzes, prize draws and surveys that may request access to accounts
- Only grant permissions to trusted applications and only the minimum access necessary
- Clear browser history and caches after using shared browsers
- Be alert to QR codes from unknown sources, which may be used for phishing

A4. Device Security and Asset Register

Each school must maintain a device security and asset register that records all computers, devices and user accounts used for examinations and assessment administration. This register must be reviewed regularly to ensure that all devices are:

- Secured with up-to-date anti-malware and the latest software updates

- Protected by full disk encryption
- Covered by the Trust's backup and recovery arrangements

The asset register must be available for inspection by the head of centre and, where required, by JCQ or awarding body inspectors.

A5. Training and Evidence

All staff who access awarding bodies' online systems must undertake annual, certificated cyber security training. This training must cover:

- The importance of creating strong, unique passwords
- Keeping all account details strictly confidential
- The critical role of MFA in protecting against unauthorised access
- How to properly set up and use MFA for both centre and awarding body systems
- Awareness of all types of social engineering and phishing attempts, including via email, phone and QR codes
- The importance of quickly reporting suspicious activity, events and incidents

Certificates of completed training must be downloaded, retained on file and made available for inspection. Each school should record:

- The type and source of training provided (for example, online training, face-to-face INSET, or training provided by The Exams Office)
- Evidence of completion (for example, certificates from online training)
- The frequency of training (annual, with records of completion dates)

A6. Incident Reporting to Awarding Bodies

In addition to the Trust's standard incident response and data breach procedures:

- Any actual or suspected compromise of an awarding body's online systems must be reported immediately to the relevant awarding body
- Any cyber attack that impacts learner data, assessment records or learner work must be reported immediately to the relevant awarding body or bodies for advice and support
- Any phishing attempts that reference awarding bodies or their systems must be reported to the awarding body concerned immediately

The head of centre and senior leader responsible for exams are accountable for ensuring these reporting requirements are met.

Appendix B- School Level Responsible Persons

Each school within the Trust must complete and maintain this appendix, identifying the individuals responsible for cyber security and JCQ examination compliance at their centre. This information should be reviewed at least annually and updated whenever staffing changes occur.

Role	Name(s)
Head of Centre	
Senior Leader(s) responsible for Exams	
Exams Officer(s)	
School Business Manager	
IT Support Technician (on-site)	
Data Protection Officer	
Governor(s) with oversight of Cyber Security	

Training Record	Details
Type/Source of Cyber Security Training	
Evidence Held (e.g. certificates)	
Frequency	
Date of Last Completion	

Exam Device Asset Register	Details
Location of Asset Register	
Date of Last Review	
Reviewed By	

This appendix is completed and maintained locally by each school. The Trust IT Director retains oversight and may request this information at any time.