

Exams Cyber Security Policy

Last reviewed: March 2026

Next review due: Spring 2029

www.dorothy-stringer.co.uk

Contents

1. Purpose of the Policy	page 3
2. Roles and responsibilities	page 4
3. Complying with JCQ regulations	page 5
4. Cyber security best practice	page 6
5. Account Management	page 7
6. Training	page 7

1. Purpose of the Policy

This Cyber Security Policy outlines the measures taken at Dorothy Stringer School to protect the confidentiality, integrity and availability of information related to examinations. It ensures compliance with JCQ General Regulations 2025–26, statutory data protection law, and recognised cyber-security best practice.

The policy supports the safeguarding of:

- awarding body systems
- candidate data
- assessment materials
- staff accounts used for exam administration

This policy applies to all staff who have access to Dorothy Stringer School's IT systems and data, with particular focus placed upon those members of staff who are involved in the management, administration and conducting of examinations and assessments.

The senior leadership team recognises the need for staff involved in the management, administration and conducting of examinations to play a critical role in maintaining and improving cyber security at Dorothy Stringer School. This includes ensuring that all members of centre staff who access awarding bodies' online systems undertake annual cyber security training.

In addition to adhering to industry best practices, the following areas are addressed in this policy to ensure that members of the exams team protect their individual digital assets:

- Cyber Security Awareness and Training
- Device Security and Asset Register
- Creating strong, unique passwords
- Keeping all account details secret
- Enabling additional security settings wherever possible
- Updating any passwords that may have been exposed
- Setting up secure account recovery options
- Reviewing and managing connected applications
- Staying alert for all types of social engineering/phishing attempts
- Monitoring accounts and reviewing account access regularly

Review

A designated member of the Senior Leadership Team will carry out regular evaluation of this policy, incorporating updates as required to remain abreast of new technologies, threat developments, and industry best practices.

Upon completion of the review and any revisions, the policy will receive formal approval from the Head of Centre.

2. Roles and responsibilities

Governors

- Oversee cyber-security arrangements, review policy compliance and ensure strategic support for cyber-resilience.

Head of centre/Senior leadership team

- To provide overall responsibility for policy implementation and cyber security strategy
- To ensure that an up-to-date device security and asset register is maintained which details all computers, devices, and user accounts used for examinations and assessment administration. This ensures that all technology used is regularly reviewed, patched, and secured, thus reducing the risk of overlooked vulnerabilities being exploited
- To ensure that all devices are secured with up-to-date anti-malware and software updates
- To ensure that members of the exams team, supported/led by the IT team, adhere to best practice(s) in relation to:
 - the management of individual/personal data/accounts
 - centre wide cyber security including:
 - Establishing a robust password policy
 - Enabling multi-factor authentication (MFA)
 - Keeping software and systems up to date
 - Implementing network security measures
 - Conducting regular data backups
 - Educating employees on security awareness
 - Developing and testing an incident response plan
 - Regularly assessing and auditing security controls
 - Managing and reporting a cyber-attack which impacts any learner data, assessment records or learner work

IT Manager/Team

- Implement, maintain and monitor technical security controls.
- Support the Exams Team with access management, MFA, system configuration and device readiness.
- Respond to cyber incidents and ensure logs are reviewed as part of routine monitoring.

Data Protection Officer

- Advise on compliance with Data Protection Act 2018 and UK GDPR.
- Support breach investigations and reporting.

All staff

- Follow this policy and complete annual cyber-security training.
- Report any suspicious activity immediately.

Exams officer/Exams assistant

- To ensure that they follow best practice in relation to the management of individual/personal data/accounts
- To provide evidence of an awareness of best practice in relation to cyber security as defined by JCQ regulations/guidance, including the completion of certificated, annual, up-to-date cyber security awareness training
- To undertake training on:
 - the importance of creating strong, unique passwords
 - keeping all account details secret
 - enabling additional security settings wherever possible
 - updating any passwords which may have been exposed
 - setting up/an awareness of secure account recovery options
 - reviewing and managing connected applications
 - awareness of all types of social engineering/phishing attempts
 - reviewing and monitoring account access on a regular basis

Students/users

- To use IT systems responsibly and report any concerns.

3. Complying with JCQ regulations

The head of centre/senior leadership team at Dorothy Stringer School ensure that there are procedures in place to maintain the security of user accounts in line with JCQ regulations (sections 3.20 and 3.21 of the *General Regulations for Approved Centres* document) by:

- Developing and maintaining this cyber security policy
- Ensuring that all members of centre staff who access awarding bodies' online systems undertake annual, certificated cyber security training which includes:
 - the importance of creating strong, unique passwords
 - keeping all account details strictly confidential
 - the critical role of Multi-Factor Authentication (MFA) in protecting against unauthorised access
 - how to properly set up and use MFA for both centre and awarding bodies' systems
 - an awareness of all types of social engineering/phishing attempts
 - the importance of staff quickly reporting suspicious activity, events and incidents
- Downloading and retaining certificates of completed staff cyber training on file
- Implementing and enforcing robust security measures, including:

- mandatory Multi-Factor Authentication (MFA) for all accounts and systems containing exam-related information, including those that interface between awarding body and centre systems, to enhance security and protect sensitive data
 - regularly reviewing and updating security settings to align with current best practices
- Enabling additional security settings wherever possible
- Updating any passwords that may have been exposed
- Setting up secure account recovery options
- Reviewing and managing connected applications
- Monitoring accounts and regularly reviewing account access, including removing access when no longer required
- Ensuring authorised members of staff securely access awarding bodies' online systems in line with awarding body regulations regarding cyber security and the JCQ document *Guidance for centres on cyber security* (www.jcq.org.uk/exams-office/general-regulations), and that where necessary, they have access to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements
- Reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body

4. Cyber security best practice

The head of centre/senior leadership team at Dorothy Stringer School ensure that:

- Network security controls and firewalls are configured and monitored.
- Anti-virus and anti-malware software is installed and maintained.
- Software updates and patches are applied promptly.
- Secure data backup and recovery systems are tested and verified.
- Sensitive data is encrypted where appropriate.
- Cloud services (e.g., Microsoft 365) are secured and regularly audited.

Staff receive training (The Exams Office, NCSC or equivalent) covering:

- phishing awareness
- secure handling of digital assessment materials
- account protection and secure authentication
- device security

The Exams Office training and guidance is followed at Dorothy Stringer School which includes:

- Good practice in creating strong and unique passwords
- Account security: Keeping account details secret (including sharing passwords, remembering passwords and monitoring account access)

- Additional security settings (including, multi-factor/two-step/two-factor authentication, the security of confidential examination materials)
- Updating expired or exposed passwords
- Account recovery (including recovery options)
- Reviewing and managing connected applications (including reviewing and removing access, using a third-party or a cloud service, granting permissions, saving passwords, saving details on local web browsers, using a shared browser)
- Social engineering/phishing attempts (including suspicious emails and phone calls, sharing information, QR codes, phishing attempts, recovery plan)
- Monitoring and reviewing access (including suspicious, unusual or unauthorised activity, departing staff, levels of access, reviewing user accounts)

Exam specific guidance is also provided on each of the areas listed above. By adopting industry standard cyber security best practices, the head of centre/senior leadership team are significantly reducing the risk of cyber-attacks and protecting valuable data and assets within the centre.

If a cyber-attack which impacts any learner data, assessment records or learner work is experienced, the senior leadership team/exams officer will contact the relevant awarding body/bodies immediately for advice and support.

5. Account Management

Password and Account Management requirements must follow the school's [Cyber Security Policy](#)

6. Training

To comply with JCQ 3.21, the school ensures that:

- All staff involved in the administration or delivery of examinations complete **annual** cyber-security training. <https://teohub.theexamsoffice.org>
- Training includes practical advice on exam-specific cyber threats such as phishing and targeted credential theft.
- Log of training completion completed and available for inspection.
- Refresher training is delivered annually.