Thomas More Catholic Academy

FAITH | EXCELLENCE | RESPECT

CYBER SECURITY POLICY (Centre-wide & Exams)

2025/26

Key staff involved in the policy

Role	Name(s)
Head of centre	Mr M Rayner
Senior leader(s)	Mr M Rayner, Mr P Shufflebotham, Mrs E Pycroft, Mrs E Todd, Mrs T Leese, Mrs K Nuttall, Mrs A Bradbury Miss S Beasley (Associate Assistant Headteacher)
Exams officer	Mrs M Thompson
IT Technician(s)	Mr A Bailey, Mr L Blackshaw, Mr R Thompson
Invigilators	
Other exams team staff	Mrs C Wheeler (SENCo), Mrs G Mutton (Assistant SENCo)

Purpose of the policy

At St Thomas More Catholic Academy, the confidentiality, integrity, and availability of our information assets, IT systems and the personal data of students, staff and stakeholders are of paramount importance.

This policy establishes our comprehensive cyber security framework, delineates the duties and accountabilities of all relevant parties, and ensures strict adherence to JCQ regulations, the Data Protection Act 2018, the UK General Data Protection Regulation, and the statutory guidance detailed in *Keeping Children Safe in Education.*

The Cyber Security policy details the measures taken at St Thomas More Catholic Academy to mitigate the risk of cyber threats under the following sections:

1. Roles and responsibilities
2. Complying with JCQ regulations
3. Cyber security best practice
4. Account management best practice
5. Training

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 St Thomas More Catholic Academy 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

Scope

This policy applies to all staff who have access t St Thomas More Catholic Academy'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.

Review

A designated member of the Senior Leadership Team will carry out annual 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 Mr A Bailey – please feedback any new cyber security related requirements to Mr A Bailey

1. Roles and responsibilities

Governors

- To oversee and review cyber security arrangements and policy compliance

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) (selective (dependent on access)
        - 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

- To implement technical controls, monitor systems, respond to incidents, manage access and updates

Data Protection Officer

- To ensure compliance with data protection law, advise on data handling, and oversee data breaches

All staff

- To follow this policy, complete annual training, report incidents or concerns promptly within the centre

Exams officer

- 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
    - 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 follow this policy, complete annual training, report incidents or concerns promptly within the centre

2. Complying with JCQ regulations

The head of centre/senior leadership team at St Thomas More Catholic Academy 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

3. Cyber security best practice

The head of centre/senior leadership team at St Thomas More Catholic Academy ensure that:

- Security measures are in place including:
    - Firewalls and network security controls
    - Anti-virus and anti-malware software on all devices
    - Regular software updates and patch management
    - Secure data backup and tested recovery procedures
    - Encryption for sensitive and personal data
    - Multi-factor authentication (MFA) for critical systems and remote access
    - Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
    - Prompt removal of access for leavers

- They and all staff involved in the management, administration and conducting of examinations/assessments stay informed about the latest security threats and trends in account security.
- Staff within the exams team are educated on how to identify phishing attempts, use secure devices and how to protect systems and data by undertaking online training during INSET on 2 September 2025.

Best practice, advice and guidance from: A Bailey (internal); S Jenkins, ICTN (external) is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.

National Cyber Security Centre (NCSC) training and guidance is followed at St Thomas More Catholic Academy which includes:

- Establishing a robust password policy
- Enabling multi-factor authentication (MFA) – staff set up via Awarding Body. Authenticator App on mobile phone for Pearson and Cambridge OCR. AQA – at log-in staff to request code to be sent to mobile phone via text or for call to be made, WJEC Eduqas, NCFE – verification code sent to email address prior to final login.
- 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

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.

4. Account management best practice

Creating strong unique passwords

Exams office staff are informed that password length is a more valuable defence than complexity and instructed to use a password creation approach such as three random words to generate suitably secure passwords

- Password governance follows National Cyber Security Centre guidance (enforced by IT Support)
- Exams office staff will be informed that password length is a more valuable defence than complexity and instructed to use a password creation approach such as three random words to generate suitably secure passwords
- Exams office staff will not use easily guessable information such as birthdays, singular names or common words for a password
- For every account, users are instructed to use a strong unique password and that the same password is not used across any other account(s) – enforced by IT Support (See appendix)

Keeping all account details secret

- Exams office staff are instructed never to share login/password details or additional factor/authentication codes with anyone else
- Staff who require access to a system will request their own user account and never share an account assigned for their use with anyone else. Staff are reminded that anything done with an account assigned to someone will be attributed to that person in the first instance

Enabling additional security settings wherever possible

- All staff will follow awarding body two-step verification (2SV)/two-factor verification (2FA) or multi-factor authentication (MFA) wherever available/requested. Staff are made aware of the purpose of 2SV/2FA /MFA, which includes:
  - adding a layer of account security
  - helps to protect users if the extra steps/factors are protected

Updating any passwords that may have been exposed

- If it is believed that a password may have been exposed/become known to others, staff will inform their senior leader/line manager immediately
- Any exposed passwords will be changed as soon as possible and the new passwords should not be shared with anyone
- Staff are instructed to use strong unique passwords (e.g. three random words) when changing passwords and that old passwords should not be reused nor should cycling through a small set of passwords across multiple accounts be used

Setting up secure account recovery options

- Staff are instructed to follow centre account recovery options which include:
  - centre account recovery options, may include alternate email accounts or phone numbers protected by 2SV/2FA/MFA security measures

Reviewing and managing connected applications

- Staff within the exams team will regularly review and remove access for third-party applications or services that no longer require access to accounts
- Staff will be informed that access should only be provided to trusted services
- Staff will be asked to be particularly cautious when interacting with content and services (e.g. quizzes, prize draws, surveys etc.)
- Staff will only grant permissions to applications and grant the necessary access required for them to function
- Staff will only download and install applications with established reputations from trusted sources (installations restricted – tech support staff ony)
- Staff will not save passwords to local web browsers unless a secure password manager extension is used in a browser that requires unlocking (e.g. with another password) before the saved account details can be retrieved, however care will be taken to ensure that this is locked/signed out of after use
- When using a shared browser, staff will clear browser history and caches after use

Staying alert for all types of social engineering/phishing attempts

- Staff must take care if unsolicited or unexpected emails, instant messages, or phone calls are received asking for account credentials or personal or confidential information. Passwords and 2FA/MFA authentication codes should not be given out to anyone
- Staff are instructed that they should have a wariness of anyone or anything that seems to want to gain their trust, rush them into doing something or that just seems off, they should hang up/not reply and not click on links or take any action and check with a trusted party via a secure channel (i.e. call awarding body customer services via a known support number)
- Staff will never approve or authenticate a login request that they did not initiate
- Staff will not share codes/approve logins should not be approved and requests to do so should be treated with a high degree of suspicion
- Staff will not click on suspicious links, download attachments or scan QR codes from unknown sources
- The centre will provide exams team staff with a secure QR code scanner with a good reputation to help gauge whether a QR code is suspicious or malicious
- Staff will verify the authenticity of any communication by contacting the organisation directly through official known channels
- Staff will report any phishing attempts which reference awarding bodies/their systems to the awarding body concerned immediately

Monitoring accounts and reviewing account access

- Centre staff accounts will be routinely reviewed for any suspicious, unusual or unauthorised activity
- If any suspicious, unusual or potentially unauthorised activity on awarding body systems is observed this will be immediately reported to the relevant awarding body, particularly if is believed that user account security may have been compromised
- User access for staff who have left the centre is reviewed promptly
- Levels of access for all exams team staff are reviewed regularly to ensure accounts have the minimum level of access required for their current role
- Accounts are promptly disabled when users leave
- Account activity is monitored and audited
- Requested security changes made within one working day of reporting to Tech Support Team

5. Training

The head of centre/senior leadership team ensure that there are procedures in place to maintain the security of user accounts by ensuring that all staff who have responsibility for the administration or delivery of examinations complete annual cyber security training and annual refresher training, with practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.

Records of cyber training are retained for all staff and are available for inspection

Overtype here any information relating to the type and frequency of training provided for staff and appropriate evidence.

- Online as part of annual INSET
- Evidence (certification via online training)
- Frequency (annual)

APPENDIX

Password Enforcement Policy (STM Staff)

Passwords expire and require changing after 180 days.

Passwords must contain a minimum of 8 characters, differ from the last 4 chosen passwords used historically and contain characters from three of the following categories:.

1. Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters).
2. Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters).
3. Base 10 digits (0 through 9).
4. Non-alphanumeric characters (special characters): '-!"#$%&()*,./:;?@[]^_`{|}~+<=>

Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Neither of these checks is case-sensitive.

The samAccountName is checked in its entirety only to determine whether it's part of the password. If the samAccountName is fewer than three characters long, this check is skipped. The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password. Tokens that are shorter than three characters are ignored, and substrings of the tokens aren't checked.

Complexity requirements are enforced when passwords are changed or created.

The rules that are included in the Windows Server password complexity requirements are part of Passfilt.dll, and they can't be directly modified.