Merchant Taylors' School

PUBLIC EXAMINATIONS – CYBER SECURITY POLICY

Centre 17632

Purpose and scope of the policy

At Merchant Taylors' School the confidentiality, integrity, and availability of our information assets, IT systems, and the personal data of students, staff, and stakeholders are of paramount importance. The Senior Leadership Team recognises the need for staff involved in the management, administration and conduct of examinations to play a critical role in maintaining and improving cyber security at Merchant Taylors' School.

This policy applies to all Centre staff who have access to awarding bodies' online systems.

This policy defines the responsibilities of relevant parties and supports compliance with JCQ and awarding body regulations, applicable data protection legislation, and relevant statutory guidance, including *Keeping Children Safe in Education*.

This policy details the measures taken at Merchant Taylors' School to mitigate the risk of cyber threats in the following sections:

1. Roles and responsibilities
2. Complying with JCQ and awarding body regulations
3. Cyber security best practice

In addition to adhering to industry best practices, the following areas are addressed in this policy to ensure that all relevant Centre staff involved in the administration, management and conduct of examinations and assessments protect their individual digital assets:

- Cyber Security Awareness and Training
- Device Security and Asset Register
- The use of an approved password manager to generate and securely store 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

Roles and responsibilities

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 examination and assessment systems are protected through appropriate technical and organisational security measures implemented by the Centre
- To ensure that all devices are secured with up-to-date anti-malware and software updates
- To ensure that all relevant Centre staff, supported/led by the IT team, adhere to best practice 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

- Responsible for implementing and maintaining technical controls, monitoring systems, managing access (including confirming MFA is enabled where supported) and responding to incidents
- Help verify the security of relevant Centre staff accounts

Data Protection Officer

- To advise on data protection compliance and personal data breaches

All relevant Centre staff

- To follow this policy, complete annual cyber security training, report incidents or concerns promptly through the centre's established reporting procedures.
    - Minor incident with limited impact; report to IT staff
    - Moderate incident with significant disruption; report to Recovery Team (IT Engineers)
    - Major incident with severe impact; report to CIRT (Senior Master and IT Manager)

Exams Team

- To ensure that they follow best practice in relation to the management of individual accounts and personal data
- Responsible for examination-specific account security and cyber security training records
- Maintain up to date records of all Centre staff with access to awarding bodies' online systems and which systems they use. Access will be reviewed regularly.
- Comply with JCQ and awarding body regulations

Complying with JCQ and awarding body regulations

The Head of Centre and Senior Leadership Team at Merchant Taylors' School must ensure that there are procedures in place to maintain the security of user accounts in line with JCQ regulations by:

- Developing and maintaining this comprehensive cyber security policy
- Ensuring that all Centre staff who access awarding bodies' online systems must complete annual cyber security training, in accordance with JCQ requirements, which must include:
    - the importance of using of an approved password manager to generate and securely store 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 confirming completion of staff cyber security training for inspection – this task will be undertaken by the Exams Team.
- Implementing and enforcing robust security measures, including:
    - mandatory Multi-Factor Authentication (MFA) where available, MFA must be used 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 (Where MFA is not available on the centre's systems, an equivalent multi layered security approach must be in place. For example, strong login controls, access and monitoring controls and secure storage so that exam-related data is protected in line with cyber security best practice.)
    - regularly reviewing and updating security settings to align with current best practices
- 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 or when Cyber Security training not completed
- Ensuring authorised members of staff securely access awarding bodies' online systems in line with all relevant awarding body regulations
- Reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body

Cyber security best practice

The Head of Centre together with the IT Department at Merchant Taylors' School 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 backups, with assessment administration systems included in disaster recovery and business continuity plans, and recovery procedures tested at least annually
    - Encryption for sensitive and personal data
    - Multi-factor authentication (MFA) for all accounts and systems containing exam-related information, including remote access, wherever available.
    - Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
    - Prompt removal of access for leavers
    - Web filtering and monitoring controls to block access to malicious websites and identify suspicious activity.
    - Ensuring that third-party suppliers and cloud service providers are appropriately assessed for cybersecurity risks and that suitable data processing agreements are in place where required.

- 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
- All relevant Centre staff are educated on how to identify phishing attempts, use secure devices and how to protect systems and data
- Best practice, advice and guidance is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.

By adopting industry standard cyber security best practices, the Head of Centre is significantly reducing the risk of cyber-attacks and protecting valuable data and assets within the centre.

Where a cyber incident has the potential to affect the delivery of examinations, assessment evidence, candidate data, access to awarding body systems or candidate results, the Head of Centre together with the Head of Examinations will contact the relevant awarding body/bodies immediately for advice and support.

Head of Examinations
October 2026
To be reviewed October 2027