Cyber Security Policy (Exams)

Document Owner:	Exams Officer
Published:	October 2025
Approved by:	Assistant Headteacher (Raising Standards)
Review Date:	Annual review
Version:	1

Shaw Education Trust

Contents

At Woodhey High School our vision is:

To be a centre of excellence, where students, staff and the community are proud to work together to broaden our horizons, exceed our aspirations and where everyone achieves their full potential.

#TeamWoodhey

At Woodhey High School, we have two key values that drive our actions, our choices, and our decisions.

These are:

Respect

We treat everyone as we wish to be treated ourselves; we are all part of the same team

Excellence

We strive to be the best we can be at all times; nothing but the best is good enough for us

---

Underpinning our values are two clear expectations.

These are:

Respect every member of staff and student in our community, following all instructions without answering back

Being excellent by being prepared for, and completing all work to the best of our ability without distracting others

We are a team made up of our staff, our students, our parents and carers, and our wider community. Our vision, values and expectations apply to all of our community.

Teamwork is the secret that makes common people achieve uncommon results (Ifeanyi Enoch Onuoha)

#TeamWoodhey

Cyber Security Policy (Exams) 2025-26

Key staff involved in the policy

Role	Name(s)
Head of Centre	Dean Watson
Data and Exams Officer	Alison Abbott
Exams Officer	Alison Abbott
Senior Leader(s)	Gary Holden
IT Technician	David Burdaky Chris Greenwood
Strategic Operations Manager	Carol Hill
Data Protection Officer (Shaw Education Trust)	Peter Potts

Purpose of the Policy

At Woodhey High School, the confidentiality, integrity and availability of our information assets, IT systems, and the personal data of students, staff and stakeholders are of a paramount importance.

This policy establishes our comprehensive cyber security framework, delineates the duties and accountabilities of all relevant parties, 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.

This Cyber Security Policy details the measures taken at Woodhey High School to mitigate the risk of cyber threats under the following sections:

- Roles and Responsibilities
- Complying with JCQ Regulations
- Cyber security best practice
- Account management best practice
- 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 Woodhey. 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 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 to Woodhey High 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.

Review

Our Exams Officer 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 the Assistant Headteacher (Raising Standards).

Roles and Responsibilities

Academy Councillors

- To oversee and review cyber security arrangements and policy compliance

Head of Centre and the 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 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 data
        - 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 Technicians

- 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 and Invigilators

- 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 and users

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

Complying with JCQ Regulations

The Head of Centre and the Senior Leadership Team at Woodhey High 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 2025/2026 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

Cyber Security Best Practice

Woodhey High School ensure the following aspects of Cyber Security Best Practice are implemented:

- 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

All staff involved in the management, administration and conducting of examinations and assessments stay informed about the latest security threats and trends in account security.

The Head of Centre and the Senior Leadership Team at Woodhey High 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

Staff within the exams team are educated on how to identify phishing attempts, use secure devices and how to protect systems and data by regular online training. The staff within this team are also expected to:

- Understand the importance of creating strong, unique passwords
- Keep all account details secret
- Enable additional security settings wherever possible
- Update any passwords which may have been exposed
- Set up/an awareness of secure account recovery options
- Review and manage connected applications
- Have an awareness of all types of social engineering/phishing attempts
- Review and monitor account access on a regular basis by completing online training.

Best practice, advice and guidance from The Exams Office and the National Cyber Security Centre 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 Woodhey High School which includes:

- 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

The Exams Office training and guidance is followed at Woodhey High 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 and the 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 or the Exams Officer will contact the relevant awarding body/bodies immediately for advice and support.

Account Management Best Practice

Creating strong, unique 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)
- Exams Office staff are informed that passwords should include a range of different characters, including:
    - Capital letter(s)
    - Number(s)
    - Special character(s)

Keeping all account details secret:

- Exams Office staff are instructed never to share login or password details or additional factor or 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 wherever possible

- All staff will follow awarding body two-step verification (2SV), two-factor verification (2FA) or multi-factor authentication (MFA) wherever available or 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 or factors are protected

Updating any passwords that may have been exposed:

- If it is believed that a password may have been exposed or become known to others, staff will inform their Senior Leadership Team link 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 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 recover options

- Staff are instructed to follow centre account recovery options, which includes MFA

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 particularly cautions when interesting with content and services (e.g. quizzes, prize draws and surveys, etc.)
- Staff will only grant permissions to required applications or the necessary access to allow them to function
- Staff will only download and install applications with consent from the Shaw Education Trust
- 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 or signed out of after use

Staying alert for all types of social engineering and phishing attempts

- Staf 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 must 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, checking 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 or approve logins. Requests to share codes or approve logins 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
- Staff will report any phishing attempts which reference awarding bodies or their systems to the awarding body concerned immediately

Monitoring accounts and reviewing account access

- 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 it is believed that user account security may have been compromised
- Access control and permissions are based on job roles and reviewed regularly
- Levels of access for 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

Training

The Head of Centre and the 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. All staff at Woodhey High School, including exams staff, completed Cyber Security Training via Flick Learning. This is completed on an annual basis, and evidence is gathered via the Flick Learning system. Exams staff will also complete any relevant Cyber Security Training issued or recommended either by JCQ or awarding bodies.