CYBER SECURITY POLICY (Exams)

2025/26

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Mr A Hammersley (Head teacher) Signed	
Date of next review	April 2027

Role	Name
Head of centre	**Mr A Hammersley**
Senior leader(s)	**Mr P Cairns, Mrs L Wood, Mr S Porter, Mr J Haworth, Mrs J Cairns, Mrs V Dovey**
Exams officer	**Mrs A Kearton**
Invigilators	
Other exams team staff	

Purpose of the policy

This policy details the measures taken at Academy@Worden 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 Academy@Worden.

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:

- 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

1. Roles and responsibilities

Head of centre/Senior leadership team

- 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
        - Immediately contacting the relevant awarding body/bodies for advice and support in the event of a cyber-attack which impacts any learner data, assessment records or learner work

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. Evidence will include a certificated assessment.
- To undertake training on:
    - the importance of creating strong unique passwords and keeping all account details secret
    - awareness of all types of social engineering/phishing attempts

2. Complying with JCQ regulations

The head of centre/senior leadership team at Academy@Worden 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:

- providing training for authorised staff on the importance of creating strong unique passwords and keeping all account details secret
- providing training for staff on awareness of all types of social engineering/phishing attempts
- 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

  Authorised staff will have access, where necessary, 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 ensure that they and all staff involved in the management, administration and conducting of examinations/assessments at Academy@Worden 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 online training.

Best practice, advice and guidance from Schools | National Cyber Security Centre - NCSC.GOV.UK 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 Academy@Worden 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

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

- 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)
- Set strong passwords which will not be shared with other colleagues or students and will change every 3 months (a strong password is one which uses a combination of letters, numbers and other permitted signs)

Keeping all account details secret

- Only use, move and share personal data relating to any member of the school community securely using approved methods such as encryption
- Only use school email account for any school matters, access to personal email in school is strictly prohibited (Unless permission is given by the Head Teacher)
- Not share any confidential information over the phone or email unless to a confirmed approved source e.g. Police and sent securely using encryption

Enabling additional security settings wherever possible

- Only allow the intended named user account to have access to the management information system (SIMS), and will close it once finished using it
- Only access files / folders and data as necessary and in line with purpose of employment
- Not use or bring in any removable storage devices such as USB drives, external hard drives, personal SD cards and insert them into any school device
- Not store any confidential school data (including addresses, phone numbers, photos or assessment data) on home computer, memory stick or hard drive

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 except their senior leader/line manager
- 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 email accounts are protected by MFA
- Any documents or files saved onto the school infrastructure are protected by a local back up server

Reviewing and managing connected applications

- Staff / The School 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 only grant permissions to applications and grant the necessary access required for them to function
- 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

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 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 5
- 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

- Not open attachments or emails unless they have come from someone you already know and trust.

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
- Documents, resources, lesson plans and any files stored on the network are property of The School and will not be removed without permission
- Files may be examined and deleted if they not appropriate, pose a security threat to the system or if misuse is suspected
- The school network and activities are constantly monitored and senior staff / ICT support staff may carry out checks of usage at any time.

5. Training

The head of centre/senior leadership team ensure that there are procedures in place to maintain the security of user accounts by:

- providing training for authorised staff on the importance of creating strong unique passwords and keeping all account details secret
- providing training for staff on awareness of all types of social engineering/phishing attempts