Bishop Douglass School

In Pursuit of Excellence

CYBER SECURITY POLICY (Exams)

2025/26

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Bishop Douglass Governors 19.03.26	
Date of next review	09.09.26

Key staff involved in the policy

Role	Name(s)
Head of centre	Michelle Henderson
Senior leader(s)	Simon Bent
Exams officer	Manisha Saleem
Exams assistant	
Invigilators	
Other exams team staff	

***"Let all things be done decently and in order."* – 1 Corinthians 14:40**

Purpose of the policy

This policy details the measures taken at Bishop Douglass School 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 Bishop Douglass School.

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) where available
        - 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/Exams assistant/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 – see Appendix 1
- 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 Bishop Douglass 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:

- 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 Bishop Douglass School 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, INSET.

Best practice, advice and guidance from NCSC 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 Bishop Douglass 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

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 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)

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. 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 and the IT department 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

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 – this is carried out throughout the year
- 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

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 is they 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
- 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

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

The Senior Leader responsible for exams will run face-to-face training with exam staff and other staff on an annual INSET day

Appendix 1

Below are the detailed best practices for cyber security, aligned with JCQ guidelines:

1. **Regular Training**
   Staff should receive ongoing training to stay informed about emerging cyber threats and best practices. Training should cover password security, social engineering attacks, and data protection. Schools should also conduct simulated cyber attack exercises to test staff preparedness.
2. **Phishing Awareness**
   Phishing emails are a common entry point for cyber attacks. Staff and students should be trained to recognize suspicious emails, avoid clicking on unknown links, and report phishing attempts immediately. Implementing email filtering systems can help reduce the risk of phishing attacks.
3. **Secure Devices**
   All school devices should have strong passwords, multi-factor authentication (MFA) where available, and encryption enabled. Devices should be regularly updated with security patches to protect against vulnerabilities. Schools should also implement endpoint security software to detect and prevent cyber threats.
4. **Data Protection**
   Schools must back up critical data regularly and store it securely, both on-site and in cloud-based systems with encryption. Access to sensitive data should be limited to authorized personnel only. Compliance with the UK GDPR is essential to protect student and staff information.
5. **Incident Response Plan**
   A structured response plan should be in place to address cyber security incidents efficiently. The plan should include clear roles and responsibilities, escalation procedures, and recovery strategies. Regular testing of the plan ensures preparedness in the event of a cyber attack.
6. **Access Controls**
   Implement the principle of least privilege, ensuring staff and students only have access to the resources they need. Use role-based access control (RBAC) and audit logs to monitor and track access to sensitive systems. Revoking access when staff or students leave the school is crucial.
7. **Software Updates**
   Operating systems, antivirus software, and school applications should be regularly updated to protect against the latest cyber threats. Schools should enable automatic updates where possible to reduce the risk of exploitation. Outdated software should be decommissioned to minimize vulnerabilities.