CYBER SECURITY POLICY (Exams)

Key staff involved in the policy

Role	Name(s)
Head of Centre	**Mr S Corless**
Senior Leader(s)	**Mrs S Morris**
Exams Officer	**Ms M Mattis**
Exams Lead	**Mrs M Shemming**

Purpose of the policy

This policy details the measures taken at St Alban's Catholic High 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 St Alban's Catholic High 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)
        - 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

- 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
- 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 St Alban's Catholic High School to 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 St Alban's Catholic High 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 annual INSET face to face training.

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 St Alban's Catholic 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.

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*
- *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/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 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 are instructed to follow centre account recovery options which 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 should 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*
- *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 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*
- *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.*

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.

All staff receive face to face training as part of annual INSET. This is delivered by our IT company.