HARROGATE GRAMMAR SCHOOL

EXCELLENCE FOR ALL

EXAM CYBER SECURITY POLICY

2025-26

Member of Staff Responsible	**Alison Meacher**
Approved on:	**14 May 2026**
Review date:	**March 2027**
Signed off by:	**Kirstie Moat**

Contents

Version history

Commented [KM1]: @Alison Meacher does this one need the branded HGS header?

Version number	Narrative	By	Date
Version 0.1	Template created	David Burns	19/02/26

Purpose

This policy establishes the measures taken at Harrogate Grammar School to mitigate the risk of cyber threats and attacks to the administration and running of internal and external exams 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

Roles and responsibilities

Head of Centre/Senior Leadership Team

- Will ensure that members of the exams team follow Trust policies and adhere to best practice(s) in relation to:
    - ensuring that all members of centre staff who access awarding bodies' online systems undertake annual cyber security training
    - the management of individual/personal data/accounts
    - centre wide cyber security including:
        - Developing and maintaining a comprehensive cyber security policy for the centre
        - Enforcing MFA for all accounts and systems containing exam-related information
        - Reviewing and managing connected applications
        - Monitoring accounts and regularly reviewing account access, including removing access when no longer required
        - Setting up secure account recovery options
        - Conducting regular data backups
        - Educating employees, including invigilators, 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 Manager/Exams Assistant

- Will ensure that they follow best practice in relation to the management of individual/personal data/accounts
- Will be aware of and follow best practice in relation to cyber security as defined by JCQ regulations/guidance including:
    - the importance of creating strong unique passwords and keeping all account details secret
    - awareness of all types of social engineering/phishing attempts
- Will ensure invigilators undertake training on cyber security

Complying with JCQ regulations

The Head of Centre, Senior Leadership Team and Exams Officers will 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).

This will include:

- 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
- updating any passwords that may have been exposed
- configuring 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
- ensuring 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
- 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

Cyber security best practice

The Head of Centre, Senior Leadership Team and Exams Officers will:

- ensure that all staff involved in the management, administration and conducting of examinations/assessments stay informed about the latest security threats and trends in account security
- ensure that staff within the exams team are educated on how to identify phishing attempts, use secure devices and how to protect systems and data
- ensure that best practice, advice, and guidance from IT Services is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.
- ensure that all staff, including invigilators, complete the required cyber security training

The IT Services Team will ensure that National Cyber Security Centre (NCSC) training and guidance is followed for Trust wide systems, 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

If a cyber-attack which impacts any learner data, assessment records or learner work is experienced, the Head of Centre, Senior Leadership Team and/or Exams Officers will immediately inform the IT Services Team and then contact the relevant awarding body/bodies for advice and support.

Account management best practice

The Head of Centre will ensure that best practice is followed for all accounts used with exam systems and information. These practices include:

- Creating strong unique passwords
    - Exams office staff are to be 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, staff 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

- 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
- 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
    - 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 will 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