Cyber security – JCQ requirements

Following the publication of JCQ regulations for the 2025/26 academic year, there have been numerous requests from exams officers and senior leaders for additional information relating to cyber security, and in particular the training which must be taken by members of centre staff who have access to awarding bodies' online systems.

Training

Section 3.21a of the *General Regulations for Approved Centres* confirms that it is now a requirement for centre staff who access awarding bodies' online systems to undertake annual cyber security training.

Therefore, exams officers, SENCos, teaching staff, senior leaders, and any other centre staff who have access to secure sites such as OCR interchange, AQA Centre Services and Edexcel Online must complete training on the areas detailed in section 3.21a.

Although JCQ has signposted to the resources and training found on the National Cyber Security Centre website, centre staff can undertake any training as long as it covers the following six areas:

- The importance of creating strong, unique passwords for all accounts
- 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 any suspicious activity, events, incidents and encouraging a safe and supportive reporting culture.

Evidence - Certification

JCQ also require centres to retain evidence to prove that this training has been completed in the form of a certificate which must be downloaded and held on file for inspection.

Online training and assessments

The Exams Office has devised a certificated online training and assessment module which covers the areas required by JCQ. This is available for all centre staff and is available in the Hub as part of your centre membership.

The Exams Office cyber security training and assessment module is the only online certificated training which has been designed to specifically meet JCQ regulations.

Additional cyber security requirements

In addition to certificated training, centres are also required to complete the following eight actions in relation to cyber security.

- To develop and maintain a comprehensive cyber security policy
- To implement and enforce robust security measures, including:

- mandatory Multi factor authentication 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
- and regularly reviewing and updating security settings to align with current best practices

- To update any passwords that may have been exposed
- To set up secure account recovery options
- Review and manage connected applications which allow a connection with other devices to share data
- To monitor accounts and regularly review account access, which includes removing access when no longer required
- To ensure that 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*
- To report any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body.