THE CAMDEN SCHOOL FOR GIRLS

Exams Cyber Security Policy

Lead Staff members:	P Schofield & L Lennon
Review Date:	January 2028

Purpose of the policy

The school recognises that cyber security is essential to the management, administration and conducting of examinations. This policy outlines the measures taken at Camden School for Girls 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

1. Roles and responsibilities

The Head of Centre and Senior Leadership Team

- Will ensure that members of the exams team supported by the IT team, adhere to best practice 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 including invigilators on security awareness
        - 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

The Exams Officer and Deputy Exams Officer

- Will be aware of best practice in relation to cyber security as defined by JCQ regulations/guidance
- Will undertake training on cyber security
- Will ensure training for invigilators covers cyber security:

2. Complying with JCQ regulations

The Head of Centre, Senior Leadership Team and Exam Officers will ensure that there are procedures in place to maintain the security of user accounts in line with the JCQ General Regulations for Approved Centres.

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
- 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 *Guidance for centres on cyber security*
- ensuring authorised staff 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 if a cyber-attack impacts any learner data, assessment records or learner work.

3. Cyber security best practice

The Head of Centre, Senior Leadership Team and Exam Officers will promote cyber security best practice by:

- ensuring 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.
- Ensuring staff within the exams team are educated on how to identify phishing attempts, use secure devices and how to protect systems and data.
- Ensuring best practice, advice and guidance is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.
- Ensuring best practice training takes place on the importance of the following:
    - 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
    - Monitoring accounts and reviewing account access
    - Staying alert for all types of social engineering/phishing attempts