

Examinations Policy

Appendix 11

Senior School

2026 / 2027



Ibstock Place

CO-EDUCATIONAL DAY SCHOOL

Examinations Policy Appendix 11: Cyber Security

Contents

1. Cyber Security

In accordance with JCQ General Regulations, Section 3.38:

The Head of Centre is to ensure that there are procedures in place to maintain the security of Awarding Body user accounts by:

- a) Ensuring that all members of staff who access awarding bodies' online systems undertake annual cyber security training. Suitable training resources for this purpose can be found on the website of the National Cyber Security Centre: Cyber security training for school staff – NCSC.GOV.UK
- b) The training is to include:
 - The importance of creating strong, unique passwords for all accounts
 - Keeping all account details strictly confidential. Note: Members of staff are not to share access to their personal accounts. If a staff member requires access to an awarding body's resources, they are to apply through the Examinations Officer for their own user account
 - 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 following resources may prove useful: <https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>
 - The importance of staff quickly reporting any suspicious activity, events, incidents and encouraging a safe and supportive reporting culture.

A record of completed cyber security training is to be held on file for inspection. This record may take the form of a certificate, a paper checklist, a spreadsheet-based checklist, or a Learning Management System (LMS) report.
- c) A comprehensive cyber security policy for the centre is to be maintained.
Note: The National Cyber Security Centre (NCSC) provides resources to assist centres in creating such policies
- d) Ensuring and enforcing the implementation of robust security measures, including:
 - Where available, MFA is used 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.

- Where MFA is not available on the centre's systems, an equivalent multi-layered security approach is to be in place. For example, strong log-in controls, access and monitoring controls and secure storage so that exam-related data is protected in line with cyber security best practice
 - By regularly reviewing and updating security settings to align with current best practices
- e) By updating any passwords that may have been exposed/compromised
- f) By setting up secure account recovery options
- g) By reviewing and managing connected applications
- h) By regularly monitoring and reviewing all account access. The Examinations Officer is to remove all access when it is no longer required, and delete accounts belonging to members of staff who leave or have left the school
- i) By ensuring 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: <https://www.jcq.org.uk/exams-office/general-regulations>.
Authorised staff are to have access, where necessary, to a device which complies with awarding bodies' MFA requirements

By reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body