IFIELD SCHOOL

Exams
Cyber Security Policy

Review Date: November 2026

Purpose of the Policy

This policy sets out Ifield School's approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

This policy applies to all staff involved in the management, administration and conducting of examinations and assessments. It will be reviewed annually to ensure that updates are made as required to remain abreast of new technologies, threat developments and best practices.

Roles and Responsibilities

Role	Responsibilities
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
IT Manager	Implements technical controls, monitors systems, responds to incidents and manage access and updates.
Data Protection Officer	Ensures compliance with data protection law, advises on data handling, and oversee data breaches.
Exams Officer	Ensures all staff with access to awarding body online systems access online training.
All staff with access to awarding body systems	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.

Complying with JCQ regulations

The Head of Centre and Exams Officer 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) by:

1) Developing and maintaining this Cyber Security Policy

2) ***Ensuring that all members of centre staff who access awarding bodies' online systems undertake annual, certificated cyber security training*** which includes:
   a) the importance of creating strong, unique passwords
   b) keeping all account details strictly confidential
   c) the critical role of Multi-Factor Authentication (MFA) in protecting against unauthorised access
   d) how to set up and use MFA for both centre and awarding bodies' systems
   e) an awareness of all types of social engineering/phishing attempts
   f) the importance of staff quickly reporting suspicious activity, events and incidents

3) ***Downloading and retaining certificates of completed staff cyber training on file***

4) ***Implementing and enforcing robust security measures, including:***
   a) mandatory Multi-Factor Authentication (MFA) 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
   b) regularly reviewing and updating security settings to align with current best practices

5) ***Enabling additional security settings wherever possible***

6) ***Updating any passwords that may have been exposed***

7) ***Setting up secure account recovery options***

8) ***Reviewing and managing connected applications***

9) ***Monitoring accounts and regularly reviewing account access, including removing access when no longer required.***

10) ***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), and that where necessary, they have access to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements***

11) ***Reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body***

All staff have due regard for data protection and understand the impact of data security when using technology. General Data Protection Regulation (GDPR) training is part the new staff induction programme and all staff receive regular updates as required. This includes cyber security and identifying phishing attempts.

The school has the following security measures in place to support this policy:

- Firewalls and network security controls
- Anti-virus and anti-malware software on all devices
- Regular software updates and patch management
- Secure data backup and tested recovery procedures
- Encryption for sensitive and personal data
- Multi-factor authentication (MFA) for critical systems and remote access
- Secure configuration and monitoring of cloud services (e.g. Office 365)

Other policies to be read in conjunction with this policy:

- Exams Policy
- Exams Contingency Policy
- Exams Internal Moderation Policy
- Exams Malpractice Policy
- Exams Complaints Policy
- Exams Conflicts of Interest Policy
- Exams Whistleblowing Policy
- Exams Word Processor Policy

Single Equalities Scheme Impact Assessment (Equalities Act 2010)

This policy has been developed to ensure that there is no negative or adverse impact on any individual or group in terms of disability, race, belief, gender, sexual orientation or age. All opportunities for potential positive impact on individuals, groups and the community are embedded within the ethos, vision and values of the school.

Ifield School is committed to achieving Best Value in all decisions made. We use the principles of Best Value as they apply to securing continuous improvement in this school.

Signed by Headteacher: ……

Signed by Chair of Governors: ……