# Cyber Security Policy

| | |
|---|---|
| Headteacher | Anita Spires |
| Chair of Governors | Katherine Russell |
| Reviewed | February 2026 |
| Date Last Ratified by LGB | March 2026 |
| Renewal date | March 2027 |

## Contents

## 1. Introduction

Beechwood School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy outlines our approach to cyber security, defines roles and responsibilities, and ensures compliance with relevant UK legislation including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education (KCSIE).

A cybersecurity incident can have a major impact on any organisation. For a school, consequences can include loss of access to learning systems, disruption to safeguarding processes, reputational damage, or data protection breaches leading to enforcement action. This policy sets out the controls in place to prevent, detect, and respond to cyber threats.

## 2. Scope

This policy applies to all staff, students, governors, contractors, volunteers, third parties, and anyone else granted permanent or temporary access to Beechwood School's systems, data, or hardware.

It covers both physical and digital elements of IT service delivery.

## 3. Roles and Responsibilities

**Headteacher / Head of Centre**
- Overall responsibility for cyber security strategy and policy implementation.
- Ensures adequate resources are allocated to reduce cyber risk.

**IT Manager**
- Implement technical controls and system monitoring.
- Manages patching, backups, anti-malware systems, and cloud configuration.
- Responds to incidents and provides technical support.

**Data Protection Officer (DPO)**
- Ensures compliance with data protection law.
- Oversees data breaches and reporting requirements.
- Advises staff on safe data handling.

**Senior Leadership Team / Governors**
- Oversee cyber security arrangements.
- Review risk register updates three times a year.

**All Staff Users**
- Follow this policy and acceptable use requirements.
- Complete annual cyber security training.
- Report incidents or suspected threats immediately.

**Students and Other Users**
- Use systems responsibly and report concerns.

## 4. Technical Security Measures

Beechwood School implements the following technical measures:

- Firewalls and network security controls.
- Anti-virus and anti-malware software.
- Regular software updates and patching.
- Secure data backup following the 3-2-1 methodology.
- Removal of unsupported/unrequired software.
- MFA is enabled for all critical systems and remote access where practicable.
- Prompt removal of accounts for staff or students leaving the school.
- An up-to date register is kept of all computers and devices

## 5. User Account Management

Users are responsible for protecting their account credentials. If they believe their account may have been compromised, they must change their password and inform the IT department

**Changes/additions:**

- Password guidance must follow complex password requirements of capital and lowercase letters, numbers and symbols.
- Password governance follows National Cyber Security Centre guidance
- Exams office staff are informed that password length is a more valuable defense 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, users are instructed to use a strong unique password and that the same password is not used across any other account(s)
- Role-based access controls (RBAC) will be implemented and reviewed regularly.
- Personal accounts must not be used for school business.
- Accounts for leavers must be disabled immediately.
- Accounts activity may be monitored or audited for security reasons.

## 6. Staff Training and Awareness

Beechwood School recognises that high-quality training is essential. Therefore:

- All staff must complete annual cyber security training, with refresher modules where appropriate.
- Phishing and social engineering awareness training will be included.
- Training records will be maintained and made available for inspection.
- Technical staff will receive additional specialised training.
- A no-blame culture will be maintained for staff reporting incidents in good faith.

## 7. Complying with JCQ regulations

The head of centre/senior leadership team at Beechwood School 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:

- Developing and maintaining this cyber security policy
- Ensuring that all members of centre staff who access awarding bodies' online systems undertake annual, certificated cyber security training which includes:
- the importance of creating strong, unique passwords
- 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 suspicious activity, events and incidents
- Downloading and retaining certificates of completed staff cyber training on file
- Implementing and enforcing robust security measures, including:
    - 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
- regularly reviewing and updating security settings to align with current best practices
- 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 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), and that where necessary, they have access 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

## 8. Incident Response Plan

Beechwood School will maintain and test a Major Incident Response Plan covering:

- Procedures for reporting suspected incidents to the Head Teacher and IT department
- Identification of key decision-makers
- System impact assessment and restoration priorities.
- Backup restoration sequence.
- Alternative methods of communication if systems are unavailable.
- Details of emergency budgets and authorisation routes.
- Contact details for key agencies (e.g., DMS, Talking Business).
- Post-incident review to identify lessons learned and update this policy.
- Referral to awarding organisations where required.

## 9. Compliance and Auditing

To ensure continued compliance:

- This policy will be reviewed annually by the Senior Leadership Team.
- Internal audits of cyber security controls will take place at least annually.
- External audits will be conducted periodically where appropriate.
- Outcomes will be reported to Governors

## 10. Policy Review and Approval

The policy will be reviewed annually or sooner if required by changes in technology, threats, or legislation.