Alderbrook School | Alderbrook Sixth Form

Cyber Security Policy

Author	John Howlett
Date	Updated June 2026
Version	1
Approved Date	June 2026
Review Date	December 2026

Introduction

1 Alderbrook School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our 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.

Scope

2 This policy applies to all staff, students, Trustees, and any third parties who have access to Alderbrook School 's IT systems and data.

Roles and Responsibilities

Role	**Responsibilities**
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
Network Manager	John Howlett Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	Martin McLoughlin Ensure compliance with data protection law, advise on data handling, and oversee data breaches.
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Trustees	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

Technical Security Measures

3 Alderbrook School implements the following security measures, scaled to our size and needs:

- 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
- Prompt removal of access for leavers.

User Account Management

- Password governance must follow NCSC/NIST Guidance.
- Access control and permissions are based on job roles and reviewed regularly.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.

Staff Training and Awareness

4 All staff must complete annual cyber security training and annual refresher training.

- Phishing awareness and social engineering defence training.
    - NCSC Cyber Security Training (Schools)

5 Records of cyber training must be retained for all staff and be available for inspection.

Incident Response Plan

6 All staff members must report any suspected security incidents or concerns to IT Support immediately.

a. Steps for identifying and reporting incidents: Any suspicious emails or digital activity must be reported to IT Support via phone, email or face-to-face immediately.
b. Incident response team: Network Manager, Network Administrator, IT Technicians and relevant third-party contacts as detailed in the IT Disaster Recovery Plan
c. Communication plan for stakeholders – SLT > Trustee Board (as needed) > Wider Staff > ICO/ NCSC/ Police Report Fraud
d. Trusts must not pay any cyber ransom demands. DfE supports the National Crime Agency's recommendation not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and is likely to result in repeat incidents.
e. Include referral to awarding organisation(s) (if applicable)
f. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

Compliance and Auditing

7 Annual review and update of this policy by the school Network Manager

8 Regular internal audits conducted termly and reported to Risk and Audit Committee

9 External audits: Daily reporting for Backups, Email Security, Safeguarding and Forensic Monitoring

Policy Review

10 This policy will be reviewed annually by the Headteacher and updated as necessary to reflect changes in technology, threats, and best practices.

11 This policy will be ratified by: Risk and Audit Committee and Trust Board