

Cyber Security Policy

Key staff involved in contingency planning

Head of Centre	Richard Wilson
Exams officer line manager	Raza Shah Assistant Vice Principal
Exams officer	Alyson Wharton
SENDCo	Heather Holiday
Review Date:	November 2026

1. Introduction

Dixons AllertonAcademy 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.

2. Scope

This policy applies to [all staff, students, governors, and any third parties] who have access to Dixons Trinity Chapeltown's IT systems and data.

3. Roles and Responsibilities

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

4. Technical Security Measures

Dixons Allerton Academy through Dixons 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 (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance must follow NCSC Guidance:
 - <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>
 - <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>
- Access control and permissions are based on job roles and reviewed regularly.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.

6. Staff Training and Awareness

- All staff must complete annual cyber security training and annual refresher training.
 - Phishing awareness and social engineering defence training.
 - [Specify any additional training requirements -
 - https://www.ncsc.gov.uk/section/education-skills/cyber-security-Centres#section_17.
- Records of cyber training must be retained for all staff and be available for inspection.
- ***Staff with access to awarding bodies secure sites will be required to complete additional training via the exams office.***

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to SLT immediately.
- DAT IT must also be informed via topdesk
- Report all suspected security incidents to relevant exam boards and JCQ
- Actions will then be shared by leadership within the Trust
- Exam specific actions to be shared by Exams Officer and Line Manager (P. Grove, T. Lascelles)

8. Compliance and Auditing

- Annual review and update of this policy – P. Grove & F. Hitch
- Regular internal audits at least annually

9. Policy Review

- This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.
- This policy will be ratified by the Principal

