



Countesthorpe
Academy

Cyber Security Policy 2025-26

Policy Reviewed and Adopted: October 2025

Date of Next Review: October 2026

Person Responsible for the Policy: Headteacher (Mrs Aitcheson)

Key staff involved in the policy

Role	Name(s)
Exams officer	Mrs J Thompson
SLT member(s)	Mrs C Aitcheson Mr T Gartside Mr D Thurston
IT manager	Mr S Knott

Cyber Security Policy

1. Introduction

Countesthorpe Academy 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 Countesthorpe Academy'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>Stephen Knott - Implement technical controls, monitor systems, respond to incidents, manage access and updates.</i>
Data Protection Officer	<i>Tim Gartside - 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

Countesthorpe Academy 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.
- Records of cyber training must be retained for all staff and be available for inspection. These records are updated on Every HR platform

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to IT Lead in school / Headteacher immediately.

Phase 1: IDENTIFY & REPORT (First 30 Minutes)

- A Staff Member or System Alert IDENTIFIES a potential incident.
- (e.g., Ransomware message, unusual pop-ups, can't access files, phishing email has been clicked)
- Action: Do not switch off the computer unless instructed. Disconnect it from the network (unplug the ethernet cable or turn off Wi-Fi).
- IMMEDIATE REPORT to the Headteacher (Incident Lead) , DSL, IT Lead in school.
- Action: Staff member provides a clear account of what they saw and did.

Phase 2: ASSESS & CONTAIN (First 1-2 Hours)

- Headteacher convenes the core response team (Headteacher, DSL, IT lead in school).
- Responsibility: Headteacher.
- Action: Provide all known details. Follow their immediate instructions.
- IT Support investigates and advises on CONTAINMENT.
- Responsibility: IT Support.
- Action: May advise isolating the school network from the internet, shutting down servers, or taking specific systems offline.
- DSL assesses the safeguarding risk.
- Responsibility: DSL.
- Action: Is there a risk of harm to children? Has personal data been accessed, especially for vulnerable pupils?

Phase 3: RESOLVE & RECOVER (Hours to Days)

- IT Support works to ERADICATE the threat.
- Responsibility: IT Support.
- Action: Remove malware, block malicious connections, patch vulnerabilities.
- IT Support begins RECOVERY.
- Responsibility: IT Support.
- Action: Restore systems and data from clean, recent backups. Verify data integrity.
- School team tests key systems before bringing them fully back online.
- Responsibility: IT support /Data and Admin Team.

Phase 4: COMMUNICATE & REPORT (As Required, some within 72 hours)

- Headteacher decides if a personal data breach has occurred.
- Responsibility: Headteacher (with advice from DSL and IT Support).
- IF a significant personal data breach has occurred:
- Report to the DPO who will liaise with solicitors who may refer to Information Commissioner's Office (ICO) within 72 hours.
- Responsibility: Headteacher/DPO
- Report the crime.
- Report to Action Fraud.
- Responsibility: Headteacher.
- Notify other key bodies which might include Exam Boards.
- Inform the Department for Education (DfE).
- Inform Local Authority
- Responsibility: Headteacher.
- Manage Communications.
- Communicate with staff about the status and what they can/cannot do.
- Communicate with parents/carers if their data is affected or if school operations are impacted. All communications must be approved by the Headteacher.
- Responsibility: Headteacher.

Phase 5: REVIEW & LEARN (1-2 Weeks Post-Incident)

- Incident Lead convenes a full review meeting.
- Responsibility: Headteacher.
- Attendees: DSL, DPO, IT Support, Chair of LGB.
- Review the response: What went well? What could be improved?
- Identify lessons learned: What vulnerabilities were exploited?
- Action Plan: Update policies, implement new security measures, and plan staff training.

8. Compliance and Auditing

- Annual review and update of this policy
- Regular internal audits: [Specify frequency and scope]
- External audits: [If applicable, specify frequency and type]

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.