CHATHAM & CLARENDON GRAMMAR SCHOOL

Cyber Security Policy 2026

Agreed by Governors: May 2026

1. Introduction

Chatham & Clarendon Grammar 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.

2. Scope

This policy applies to all staff, students, governors, and any third parties who have access to Chatham & Clarendon Grammar School's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Headteacher	Overall responsibility for policy implementation and cyber security strategy.
Network IT Manager/Team	Network Manager: Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	DPO: 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.
Governors	Oversee and review cyber security arrangements and policy compliance.

Role	Responsibilities
Students/Users	Use IT systems responsibly and report any concerns.
Third party individuals	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Chatham & Clarendon Grammar 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 (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance meets NCSC Guidance:
- 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 complete annual cyber security training and annual refresher training.
    - Phishing awareness and social engineering defence training.
    - NCSC appropriate training
- Records of cyber training are retained for all staff and are available for inspection.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to the Network IT Manager immediately.
- The Network IT Manager will follow procedures within the Plan to investigate any incidents immediately and report accordingly to the Headteacher, Governors or external agencies as appropriat

8. Compliance and Auditing

- Annual review and update of this policy will be undertaken by the Business Manager

- Regular internal audits to be carried out twice yearly by the IT Team;
- External audits to be carried out through the Scrutiny programme as per the Academies Handbook

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 Board of Governors.

Version	Date of Review	Reviewed By	Next Review Due	Approved By
1	March 27th 2026	C Freeman	March 2027	Board of Governors