The Crypt School Cyber Security Policy

Lead Person: **IT Manager**
Support Persons: **SLT, Exams Officer, Compliance Officer**

1. Introduction

The Crypt 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 The Crypt School's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Headmaster and Head of Centre	*Overall responsibility for policy implementation and cyber security strategy.*
IT Manager/Team	*Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Compliance Officer	*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.*

4. Technical Security Measures

The Crypt 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 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 (Every HR).
    - National CyberSecurity Centre training for school staff:
        - 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.

7. Physical and environmental security

Physical security of the environment

Spaces in which vital (ICT) facilities are housed are defined and specified as such and subject to extra security.

All locations are provided with a lightning conductor installation.

Control of physical access

- Maintenance staff who carry out work on ICT installations are constantly accompanied by an expert internal staff member.
- Rooms, cupboards and shutters must all be lockable.
- Each location must have at least one secure room for storage or installation of sensitive or critical components.
- Entrances and exits of locations are subject to a form of supervision.

Security for computer rooms

- Access to secure spaces is reserved for those with appropriate authorization; in the event of emergencies the security service and technical service also have access.
- Secure spaces are provided with fire detection and extinguishing equipment.
- ICT staff must be aware of where fire-fighting equipment is kept.
- Keys to drawers and cupboards must be carefully administered.

Delivery of goods

- Goods intended for ICT services are delivered under supervision and stored securely.
- Goods intended for ICT services are signed for receipt on delivery.

Clear Desk Policy

- Sensitive information may not be open to casual consultation in operational spaces.
- Sensitive information may not be left unmanaged in operational spaces.

Removal of school property

- School equipment may be taken elsewhere only with formal permission from the responsible party.

Security of equipment

Positioning and security

- Equipment may not compromise the accessibility of emergency exits.
- There is a defined procedure for acquisition of equipment and software.

Use outside the institution

- External use of institution equipment requires authorization in accordance with regulations.
- External use of institution equipment is subject, as a minimum requirement, to the internal security requirements.

- On its return, externally used institution equipment must be in the state in which it was issued.

Discarded resources

- Information carriers which accompany equipment due to be discarded are destroyed or cleaned at bit level.

8. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to IT Support immediately. The School will then follow the Cyber Incident Response Plan (copies held by IT and Finance).

9. Compliance and Auditing

- Annual review and update of this policy: IT Manager, Compliance Officer and Exams Officer
- Regular internal audits: by the School Data Protection and Cybersecurity Group and otherwise as determined by the Trustee Audit & Risk Committee

10. Policy Review

- This policy will be reviewed annually by the IT Manager and updated as necessary to reflect changes in technology, threats, and best practices.
- This policy will be ratified by: The Headmaster.

Version 1 Date: October 2025

Approved by the Headmaster: October 2025

Review Cycle: Annual

Date of next review: September 2026