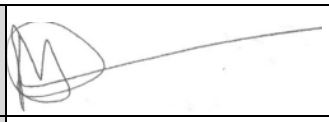
Cyber Security Policy

Centre Number: 11025

Signed	
Position	Micheal Jeffrey Head of School
Date Agreed	September 2025
Next Review	September 2026

Centre Academy London is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

Equality Statement

Centre Academy London is committed to a policy of equality and aims to ensure that no employee, job applicant, pupil or other member of the school community is treated less favourably on grounds of sex, race, colour, ethnic or national origin, marital status, age, sexual orientation, disability, or religious belief. We provide a safe, supportive, and welcoming environment.

1. Introduction

Centre Academy London 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 Centre Academy London's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre Michael Jeffrey	*Overall responsibility for policy implementation and cyber security strategy.*
IT Manager/Team Angel Okundaye	*Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer Angel Okundaye	*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.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Centre Academy London 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.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to Michael Jeffrey and Angel Okundaye immediately.

a. Steps for identifying and reporting incidents:

i. **Recognize an Incident:** Be alert for unusual system activity, lost/stolen devices, suspicious emails or files, unauthorized access, or data breaches.

ii. **Immediate Action:** As soon as a cyber incident is discovered, report it to the designated staff member without delay.

iii. **Record Details:** Write down what happened, when it was detected, who found it, and any actions already taken (such as changing passwords or disconnecting devices).

iv. **Report to Data Protection Officer (DPO):** The incident should be forwarded to the DPO or safeguarding lead for further assessment and handling.

v. **Contain the Incident:** The relevant staff (IT, DPO, Headteacher) act quickly to limit damage (for example, retrieving information, blocking access, or informing affected users).

vi. **Investigation and Follow-up:** The incident is reviewed and investigated to understand its cause and impact. The school decides

whether to notify external authorities, such as the Information Commissioner's Office (ICO), if personal data was affected.

vii. **Learn and Improve:** Document recommendations to prevent future incidents and update procedures or provide staff training as needed.

b. Incident response team: Michael Jeffrey, Angel Okundaye, SMT
c. Communication plan for stakeholders – [e.g. relevant awarding body, National Cyber Security Centre (NCSC), etc.]
d. Include referral to awarding organisation(s) (if applicable)
e. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

8. Compliance and Auditing

- Annual review and update of this policy: SMT
- Regular internal audits: Termly by Angel Okundaye
- External audits: Agile Technologies

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.