The Ladder School
Cyber Security Policy
Version 1.0
1/9/25

Sample Centre Cyber Security Policy

1. Introduction

The Ladder 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 Ladder School's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
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.
Data Protection 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.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

The Ladder School implements the following security measures, scaled to our size and needs: [amend as appropriate]

- 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 are delivered via the School Pro training system
- 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 James Fendek Director of Information via phone 07498210289 or email james.fendek@merciantrust.org.uk immediately.

a. Steps for identifying and reporting incidents:
   i. adhere to staff training on cyber security (e.g. do not click on unknown links; check email address of sender; look for poor spelling / layout, etc.)
   ii. inform the Director of Information Systems
   iii. Director of Information Systems to oversee response to incident in line with IT Provider TIO

b. Incident response team:
   Dan Parkes – CEO
   Andrew Paulson – CFO
   James Fendek – Director of Information Systems
   Jamie Hynes – Trust IT Manager
   Mark Smith – Communications Manager
   TIO Support Team

c. Communication plan for stakeholders – [Director of Information Systems to work with Head of Centre (via SLT lead for exams) and Communications Manager to establish communication with stakeholders - relevant awarding body, National Cyber Security Centre (NCSC), etc.

d. 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 by Director of Information system
- Regular internal audits: Quarterly – TIO Securityhealth check

9. Policy Review

- This policy will be reviewed annually by the Director of Information Systems and updated as necessary to reflect changes in technology, threats, and best practices.
- This policy will be ratified by: Board of Governors, Senior Leadership Team

Version	Date of Review	Reviewed By	Next Review Due	Approved By
[1.0]	1/9/25	James Fendek Director of Information Systems	1/9/26	[Head of Centre/Governing Body Chair]

Signed: _____ H. Stephens _____

[Head of Centre/Governing Body Chair]