

Enterprise Learning Alliance

Cyber Security Policy



Date	Approval Date	Review Date
25 November 2025		24 November 2026

1. Introduction

Enterprise Learning Alliance (ELA) 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 ELA's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	David DuCane - Overall responsibility for policy implementation and cyber security strategy.
IT Manager	John Fermor - Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	Sarah Jeffery - 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.
Management Committee	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

ELA 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.
 - <https://www.ncsc.gov.uk/information/cyber-security-training-schools>
- 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 David DuCane immediately.
 - a. Steps for identifying and reporting incidents: Incident details to be noted and David DuCane advised by phone in the first instance; a written report to be completed by staff member.
 - b. Incident response team: David DuCane Head of Centre, John Fermor Head of IT, Sarah Jeffery Data Manager
 - c. Communication plan for stakeholders - Exam awarding body, National Cyber Security Centre (NCSC), any other stakeholders to be advised if directed by David DuCane and Sarah Jeffery
 - d. Post-incident review process: David DuCane to conduct a review to identify lessons learned and update procedures if necessary.

8. Compliance and Auditing

- Annual review and update of this policy, Angela Shrimpton Exam Officer will review policy annually, draft any amendments needed and send to Senior Leadership Team for checking and approval
- Regular internal audits: David DuCane to complete internal audit as part of Centre Reviews.

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 Senior Leadership Team

Signed: _____

Head of Centre