CYBER SECURITY POLICY

Date of approval by the Trust Board	**15 October 2025**
Review cycle	**2 years**

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Alternative Learning Trusts' guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of policy

This policy applies to all Alternative Learning Trust staff, contractors, volunteers (including Members, Trustees and Governors) and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk management

Alternative Learning Trust will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Trustees through the Audit, Risk and Finance Committee once each term.

Example below:

					Current risk level		
Risk ID	Date Raised	Date Reviewed	Raised by	Risk description	Probability	Impact	Value
R001	Example	Example	Bob	Ransomware attack	Low	Very High	20
R002	Example	Example	Diane	Someone is caught by phishing email	Medium	High	19
R003	Example	Example	Mark	Password is compromised	Medium	High	19
R004	Example	Example	Gareth	No backups in place	Low	High	16
R005	Example	Example	John	No encryption	High	Very High	24
R006	Example	Example	Leslie	USBs used for file storage lost	High	High	21
R007	Example	Example	Bob	Laptop stolen leads to data breach	Medium	Medium	15

Physical security

Alternative Learning Trust will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset management

To ensure that security controls to protect the data and systems are applied effectively, Alternative Learning Trust will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform their schools ICT provider as soon as possible. Personal

accounts should not be used for work purposes. Alternative Learning Trust will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Alternative Learning Trust issued devices and data, users are required to:

- Lock devices that are left unattended.
- Update devices when prompted.
- Report lost or stolen equipment as soon as possible to the schools Headteacher and to Alternative Learning Trust's ICT Manager – Lisa Heyna.
- Change all account passwords at once when a device is lost or stolen (and report immediately to the schools ICT provider and Headteacher.
- Report a suspected threat or security weakness in Alternative Learning Trust's or your school's systems to Lisa Heyna or David Ward.

Devices will be configured with the following security controls as a minimum:

- Password protection.
- Full disk encryption.
- Client firewalls.
- Anti-virus/malware software e.g. Sophos.
- Automatic security updates.
- Removal of unrequired and unsupported software.
- Autorun disabled.
- Minimal administrative accounts.

Data security

Alternative Learning Trust will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Alternative Learning Trust defines confidential data as:

- Personally identifiable information as defined by the ICO (Information Commissioner's Office).
- Special Category personal data as defined by the ICO.
- Unpublished financial information.

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology.

- 3 versions of data.
- 2 different types of media.
- 1 copy offsite/offline.

LGfL (London Grid for Learning) provide Gridstore for example.

Sharing files

Alternative Learning Trust recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites.
- Wherever possible, keeping Alternative Learning Trust files on school systems.
- Not sending school files to personal accounts.
- Verifying the recipient of data prior to sending.
- Using file encryption where possible, sending passwords/keys via alternative communication channels.
- Alerting IT Support/DPO to any breaches, malicious activity, or suspected scams.

Training

Alternative Learning Trust recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular cybersecurity training into INSET days, provide more specialist training to staff responsible for maintaining IT systems and promote a "no blame" culture towards individuals who may fall victim to sophisticated scams.

System security

IT Support will build security principles into the design of IT services for a school within Alternative Learning Trust.

- Security patching – network hardware, operating systems and software.
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them.
- Actively manage anti-virus systems.
- Actively manage and test backups.
- Regularly review and update security controls that are available with existing systems.
- Segregate wireless networks used for visitors' and staff personal devices from school systems.
- Review the security risk of new systems or projects.

Major incident response plan

Alternative Learning Trust will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers.
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again).
- Emergency plans for the school to function without access to systems or data.
- Alternative methods of communication, including copies of contact details.
- Emergency budgets and who can access them/how.
- Key agencies for support (e.g. IT support company).

Maintaining security

Alternative Learning Trust understands that the financial cost of recovering from a major cybersecurity incident can far outweigh the ongoing investment in maintaining secure IT systems Alternative Learning Trust will budget appropriately to keep cyber related risk to a minimum.

	CEO or Deputy CEO	[ ]
	Chair of Trust or Trustee with ICT oversight	[ ]
	Network manager other technical support	[ ]
	Date this policy was reviewed and by whom	[ ]
	Date of next review and by whom	[ ]

Person responsible for updating this policy

Deputy CEO/Director of School Improvement