CYBER SECURITY POLICY

OUR TRUST'S PRAYER

Heavenly Father

Let peace, friendship and love grow in our schools

Send the Holy Spirit to give:

Excellence to our learning

Love to our actions and

Joy to our worship

Guide us to help others

So that we may all

Learn, Love and Achieve, Together with Jesus.

Amen

Introduction and Scope of Policy

A cyber security incident can have a major impact on any organisation for extended periods of time. For LDST and its schools ('our Trust'), 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 Cyber Security Policy outlines our Trust's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyber attack.

This policy applies to all staff, contractors, volunteers 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.

1. Risk Management

Our Trust will include cyber security risks on its organisational risk register, regularly reporting on the progress and management of these risks to the Board of Directors and Local Governing Body.

2. Physical Security

Our Trust will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems.

3. Asset Management

To ensure that security controls to protect the data and systems are applied effectively, our 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.

4. 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 Techminder/IT Support as soon as possible. Personal accounts should not be used for work purposes. Our Trust will implement multi-factor authentication where it is practicable to do so.

5. Devices

To ensure the security of all 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 Techminder/IT Support
- Change all account passwords at once when a device is lost or stolen (and report immediately to Techminder/IT Support)
- Report a suspected threat or security weakness in our Trust's systems to
    - Steve Boothroyd (Trust Corporate Services Director)
    - Techminder
    - Executive Headteacher/Headteacher

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

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

6. Data Security

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

Our Trust defines confidential data as:

- Personally identifiable information as defined by the ICO
- 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

7. Sharing Files

Our 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
- Keeping our Trust's files on LDST approved systems
- Not sending our Trust's 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 the Trust Data Protection Officer (Alison Tennant) and Techminder to any breaches, malicious activity or suspected scams

8. Training

Our Trust recognises that it is not possible to maintain a high level of cyber security without appropriate staff training. It will integrate regular cyber security 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.

The following compulsory training courses are available via National College:

Cyber Security for Staff

Data Protection and GDPR for Staff

Cyber Security for Governors

Data Protection and GDPR for Governors

Cyber Security for Leaders

Data Protection and GDPR for Leaders

All staff must also complete the compulsory training available via the National Cyber Security Centre and download the certificate as evidence of training received – this is also a requirement of the RPA insurance.

Our Trust also makes available, via National College, the following training for parents/carers:

Cyber Security for Parents/Carers

The National College LDST subscription provides all staff with access to other related courses and webinars (online safety, filtering & monitoring, phishing, cyber culture…).

9. System Security

Techminder/IT support will build security principles into the design of IT services for our 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

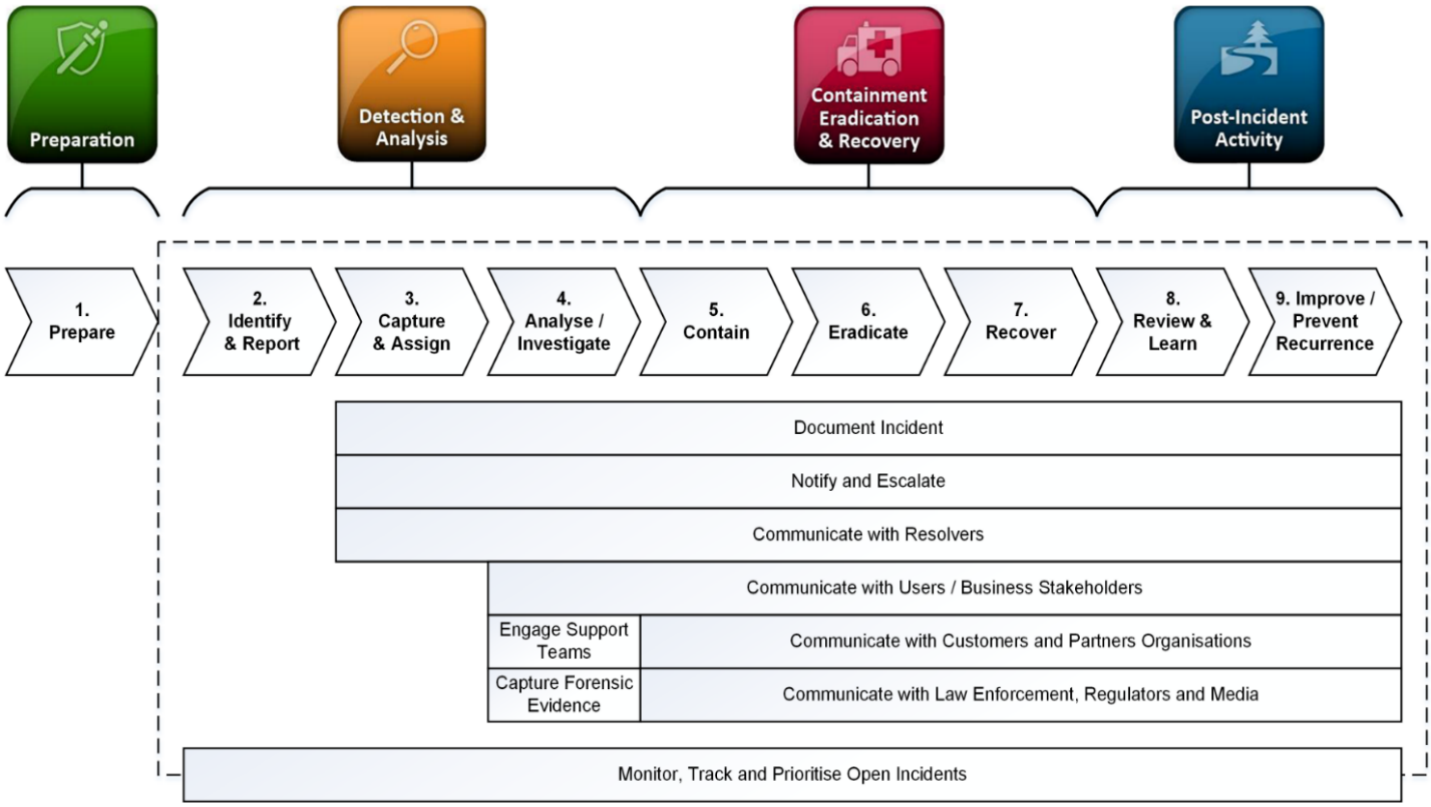
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

10. Cyber Incident Response Plan (CIRP)

Our Trust will develop, maintain, and regularly test a Cyber Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers (Cyber Incident Response Team (CIRT))
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for our Trust/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)

The following illustration sets out an overview of the end-to-end incident handling process.



11. Maintaining Security

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

Review Schedule

Policy Author	Trust DPO
Policy Approver	Trust Corporate Services Director
Current Policy Version	1.0
Policy Effective From	April 2024
Policy Review Date	April 2026

Revision Schedule

Version	**Revisions**	**By whom**
1.0	Original	DPO