LIGHTHOUSE SCHOOLS PARTNERSHIP

CYBER SECURITY POLICY
Non-Statutory

Policy approved by Trust Executive Team	
Signed: Gary Lewis	Date: 13 July 2026
Name: Gary Lewis	Role: Chief Executive

Document History

Version	Author/Owner	Drafted	Comments
1.0	Kirk Perrin	May 2026	New policy created
2.0			
3.0			

Review cycle	Every two years
Review date	July 2028

This policy applies to all schools and employees within the Lighthouse Schools Partnership.

This policy remains valid, and in operation, until a new or updated policy is published.

CYBER SECURITY POLICY

Non-Statutory

1. Introduction

This cyber security policy outlines guidelines and provisions for preserving the security of our data and technology infrastructure for the Lighthouse Schools Partnership (LSP).

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacking attacks and system malfunctions could cause great damage and may jeopardise the Trust's reputation or threaten our finances.

For this reason, we implement a range of security measures. We have also prepared guidance that may help mitigate security risks. We outline both solutions in this policy.

2. Scope of policy

This policy applies to all our staff, governors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

3. Roles and responsibilities

Managing IT and e-safety are important aspects of strategic leadership within the Trust.

The Board of Trustees maintains strategic oversight of cyber risk. Cyber security is a standing item on the Trust's risk register and the Audit and Risk Committee receive an annual report to review and assess the measures in place.

The Chief Financial and Operating Officer has strategic responsibility for cyber security and delegates the tasks necessary to fulfil this responsibility to the Director of Trust Services and the Head of IT.

Headteachers and governors have responsibility to ensure that the policy and practices are embedded and monitored at individual school level.

Data and cyber security is, however, the responsibility of all users. In this policy, we give our staff guidance on how to best avoid security breaches.

4. Policy elements

Confidential data is private and valuable and accessing or removing access to this data for financial gain is often the purpose of a cyber attack. Common examples of valuable data are:

- Data of students/parents/carers/staff
- Financial data
- Personal information
- Medical information

- Employment information

5. Cyber Security Threats

Threats, if left unchecked, could disrupt the day-to-day operations of the Trust, the delivery of education and ultimately has the potential to compromise the Trusts and its school's security.

The types of security threats are constantly developing and becoming more and more sophisticated. Below are some of the common threats but we need to be constantly alert and adapting as new threats arise:

5.1. Cyber criminals and Cybercrime - Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party or using directly for criminal means. Key tools and methods used by cybercriminals include:

5.1.1. Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals

5.1.2. Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid

5.1.3. Phishing – emails purporting to come from an often trusted senders, which in fact are coming from a bad actor, seeking to gain information for financial gain or reputational damage.

5.2. Hacktivism - Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against Trust or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service attacks (DDoS – when a system, service or network is so overwhelmed with requests that it becomes unavailable). Attacks of this nature are a daily occurrence across the wider world.

5.3. Insiders - Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but often this is due to human error and a lack of understanding about the risks involved when handling data.

5.4. Zero-day exploit - A zero-day exploit is a cyber-attack that occurs on the same day an exploit is discovered in software. At that point, it's exploited before a fix becomes available. This makes an attack of this kind very hard to defend against as there is no appropriate mitigation when the attack begins.

5.5. Physical threats - The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

5.6. Terrorists - Some terrorist groups demonstrate intent to conduct cyber-attacks, but currently seem to have limited technical capability. However, with the proliferation of online sharing portals, and the Dark Web, they have the ability

to improve this over time.

5.7. Espionage - Many sophisticated and hostile foreign intelligence agencies target UK government and public sector organisations to steal sensitive information.

6. Mitigations

Within the LSP, we aim to implement the National Cyber Security Centre's advice for keeping our data secure:

6.1. The Trust's insurance, via the Risk Protection Arrangements covers the Trust for cyber security. This is subject to particular arrangements being in place, which are secured via this policy.

6.2. All schools have a Cyber Response plan in place and review them annually.

6.3. Training

6.3.1. All staff, Governors and Trustees complete Cyber Security Training annually,

6.3.2. A phishing training and security awareness service is deployed in one LSP location each year,

6.3.3. Regular advice to staff/leaders based on specific incidents (within or outside the Trust) and information received e.g. from the counter fraud updates service,

6.4. Protect personal and school devices

In general, staff should try to only use school-issued devices to access school emails, accounts or folders. When staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. To achieve this staff must take the following actions when using schools issued devices, or when using their personal devices to access school emails or accounts:

6.4.1. Keep all devices password protected.

6.4.2. Ensure that they have anti-virus software installed on home computers/devices (anti-virus is a part of school built devices).

6.4.3. Ensure they do not leave their devices exposed or unattended.

6.4.4. Ensure that school-wide security updates of browsers and systems have taken place.

6.4.5. Log into school accounts and systems through secure and private networks only.

6.4.6. Avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

6.4.7. Follow all instructions for the use of school-issued equipment such as password management setup

6.4.8. Install antivirus software is installed on personal devices used to access school emails or accounts (Antivirus/anti-malware software is installed on all school-owned laptops/devices).

6.4.9. Staff must follow instructions to protect their devices and refer to central Team IT - if they have any questions.

6.5. Keep emails safe

Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft, we instruct staff to:

6.5.1. Avoid opening attachments and clicking on links when the content is not anticipated or adequately explained (e.g. “watch this video, it’s amazing.”)

6.5.2. Be suspicious of clickbait titles (e.g. offering prizes, advice).

6.5.3. Check email and names of people they received a message from to ensure they are legitimate.

6.5.4. Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

6.5.5. If a member of staff isn’t sure that an email they received is safe, they can refer to the Central IT Team.

6.5.6. See the section in the individual schools Acceptable Use of ICT Policy for further details on email etiquette and email security.

6.6. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, staff are required to:

6.6.1. Choose passwords with at least sixteen characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g.birthdays).

6.6.2. Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.

6.6.3. Exchange user credentials (e.g. userids and passwords) only when absolutely necessary. Where exchanging them in person isn’t possible, staff should use a telephone call, and only if they personally recognise the person they are talking to.

6.6.4. Whilst some providers and organisations with whom we work advise (and expect) passwords to be changed regularly, we advise that passwords only be changed if and when they are compromised.

6.7. Transfer data securely

Transferring data introduces security risks. Staff must:

6.7.1. Avoid transferring sensitive data (e.g. personal information, staff records) to other devices or accounts unless absolutely necessary.

6.7.2. Share confidential data over the school network/system and not over public Wi-Fi or private connection.

6.7.3. Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

6.7.4. Ensure that data is sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility).

6.7.5. Report scams, privacy breaches and hacking attempts in line with the LSP data protection policy.

6.7.6. Our IT Team needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we require our staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our team. Our IT Team will investigate promptly, resolve the issue and send a Trust wide alert when necessary.

6.7.7. Our IT Team is responsible for advising staff on how to detect scam emails. We encourage our staff to reach out to them with any questions or concerns.

6.8. Additional measures

To reduce the likelihood of security breaches, we also instruct staff to:

6.8.1. Turn off screens and lock devices when leaving desks (There are also technical solutions in place to lock workstations after a set time).

6.8.2. Report stolen or damaged equipment as soon as possible to ITSupport@lsp.org.uk.

6.8.3. Change all account passwords at once if a device is stolen or compromised.

6.8.4. Report a perceived threat or possible security weakness in the Trust's systems.

6.8.5. Refrain from downloading suspicious, unauthorised or illegal software on Trust equipment.

6.8.6. Avoid visiting suspicious websites.

6.8.7. We also expect staff to comply with our Data Protection Policies, Records Management Policy and Acceptable Use of ICT policies.

Our Central IT Team will:

6.8.8. Install firewalls, anti malware software and access authentication systems on all Trust devices.

6.8.9. Investigate security breaches thoroughly.

6.8.10. Follow policy provisions as other staff do.

6.9. Working remotely

Anyone working remotely for whatever reason, must follow the instructions in this policy, Data Protection Policies, Records Management Polic and Acceptable Use of ICT policies. When staff are accessing our Trust's systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage staff to seek advice from our IT team.

6.10. Reporting incidents, abuse and inappropriate materials

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Central IT Team. Additionally, all security breaches, must be reported to **DPO@lsp.org.uk.**
The Trust's DPO is outsourced and can be contacted at i-west@bathnes.gov.uk.

In the event of an incident, the Central IT Team would Inform the local police and education team, National Cyber Security Centre (https://report.ncsc.gov.uk/), Action Fraud (https://www.actionfraud.police.uk/) and Department for Education.

6.11. Disciplinary Action

We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action.

For first-time, unintentional or small-scale security breach, we may require staff to undertake additional training on the security or issue a management direction.

Intentional, repeated or large scale breaches (which may cause severe financial or other damage or disruption) will be considered as a disciplinary matter and investigated in accordance with the Trust's disciplinary policy. The same will apply to staff who have disregarded the Trust's security instructions or policies, even if their behaviour hasn't resulted in a security breach.

We will examine each incident on a case-by-case basis.

7. Links to other policies

This policy has important links to the following other policies/plans:

- Data Protection Policies
- Records Management Policy
- Risk Management Policy
- Critical Incident and Business Continuity Plans
- Cyber Response Plans
- Acceptable Use Policies