LLOYD WILLIAMSON
FOUNDATION

The Lloyd Williamson Schools Foundation

CYBER SECURITY POLICY

Policy Statement

LWSF is committed to ensuring the safety and security of its digital environment, protecting the personal data of pupils, staff, and stakeholders, and complying with statutory guidance, including the Data Protection Act 2018, UK General Data Protection Regulation (GDPR), and Keeping Children Safe in Education (KCSIE) 2024. This policy outlines the measures we take to mitigate cyber risks, safeguard sensitive information, and maintain the integrity of our IT systems.

1. Objectives

- To protect sensitive data from unauthorised access, loss, or damage.
- To educate staff, pupils, and stakeholders about cyber security risks.
- To comply with the latest statutory guidance, including the Department for Education (DfE) and KCSIE 2024.
- To minimise disruption to teaching and administrative operations caused by cyber incidents.

2. Scope

This policy applies to all members of the school community, including:

- Teaching and non-teaching staff
- Trustees
- Pupils
- Volunteers
- Contractors
- Third-party service providers

It covers all IT systems, devices, software, and networks used within the school environment or for school-related activities.

3. Key Principles

Safeguarding and Child Protection

In line with KCSIE 2024, the school will ensure online safety is a core component of its safeguarding practices.

The Designated Safeguarding Lead (DSL) and deputies will work alongside the IT Lead (Shaun Watson) to oversee the monitoring of online activity to identify potential risks to pupils, such as grooming, cyberbullying, or exposure to harmful content.

Data Protection

The school will comply with GDPR and the Data Protection Act 2018 to protect personal data. Staff are required to follow the school's Data Protection Policy when handling sensitive information.

Only authorised personnel will have access to sensitive data.

Risk Management and Incident Response

The school will regularly assess and update its cyber security measures to reflect emerging threats. All staff and pupils must report suspected cyber incidents (e.g., phishing attempts, ransomware attacks) to the IT Lead or DSL/s immediately.

In the event of a cyber incident, the school will follow its Incident Response Plan (Appendix 1) to contain and mitigate risks.

4. IT Systems Security

Access Controls

Staff and pupils will be assigned unique user accounts with role-based permissions.

Strong passwords must be used and changed at least every 90 days.

Multi-factor authentication (MFA) will be implemented for access to sensitive systems.

Device Security

All school-owned devices must have up-to-date antivirus software and operating systems. The School uses a monitoring and filtering programme: Famisafe.

Personal devices must be used in line with the School's BYOD Policy. Devices must be encrypted if they store sensitive information.

Network Security

The school's Wi-Fi network will be segmented and secured with strong encryption (e.g., WPA3). Firewalls and intrusion detection systems will monitor network traffic.

5. Online Safety for Pupils

Pupils will receive age-appropriate education on online safety, digital resilience, and recognising cyber risks, in line with KCSIE 2024.

Filters and monitoring systems will block inappropriate content and flag potential safeguarding concerns.

Pupils will be encouraged to report online concerns to their teachers or the DSL.

6. Training and Awareness

All staff will receive annual training on cyber security, data protection, and online safety as part of their safeguarding responsibilities (EDUCARE).

Regular updates on emerging cyber threats will be provided to staff and pupils.

Trustees will receive training to ensure their oversight of the school's cyber security practices.

7. Third-Party Suppliers and Contractors

Contracts with IT service providers will include clauses to ensure compliance with GDPR and the school's cyber security standards.

8. Monitoring and Review

The IT Lead will conduct regular audits of the school's cyber security infrastructure.

This policy will be reviewed annually or sooner in response to significant incidents, changes in statutory guidance, or advancements in technology.

9. Roles and Responsibilities

The Designated Safeguarding Lead (DSL):

The DSL and deputy DSLs will oversee online safety as part of the school's safeguarding responsibilities. They will collaborate with the IT Lead to address cyber security incidents that involve safeguarding concerns.

The IT Lead will:

- Implement and monitor appropriate technical cyber security controls.
- Investigate and respond to cyber security incidents.
- Ensure compliance with statutory requirements.

All Staff will:

- Follow this policy and attend mandatory training.
- Report any suspected data breaches or cyber security incidents.

Trustees will:

- Provide oversight of the school's cyber security framework.
- Ensure appropriate funding and resources are allocated to maintain cyber resilience.

10. Related Policies

This policy should be read alongside the following documents:

- Safeguarding and Child Protection Policy
- Data Protection Policy
- Use of Computers and Internet Access Policy
- Staff Code of Conduct

Review

Next review date: August 2025.

Appendix 1: Incident Response Plan (IRP) 2024–2025

Purpose

The purpose of this Incident Response Plan (IRP) is to outline a structured and effective response to cyber security incidents, safeguarding the school's IT infrastructure, protecting sensitive data, and minimising disruption to teaching and administrative operations.

This plan supports compliance with statutory guidance, including the Data Protection Act 2018, GDPR, and Keeping Children Safe in Education (KCSIE) 2024.

Scope

This IRP applies to all members of the school community, including staff, trustees, pupils, and third-party service providers. It covers all IT systems, data, and devices owned, operated, or accessed by the school / staff.

Incident Definition

A cyber security incident is any event that compromises the confidentiality, integrity, or availability of the school's IT systems, data, or services. Examples include:

- Unauthorised access to systems or data
- Data breaches (e.g., loss of sensitive information)
- Malware or ransomware attacks
- Phishing or social engineering attempts
- Denial-of-service (DoS) attacks
- Inappropriate use of school IT systems

Incident Response Team (IRT)

The following roles are part of the Incident Response Team, with clearly defined responsibilities during an incident:

1. **Incident Response Coordinator (IT Lead):**
    - Leads the response and coordinates the team.
    - Ensures the implementation of technical measures to contain and mitigate the threat.
2. **Designated Safeguarding Lead (DSL):**
    - Handles incidents involving safeguarding risks to pupils.
    - Liaises with external safeguarding bodies as necessary.
3. **Headteacher:**
    - Oversees the overall response and provides strategic direction.
    - Communicates with parents, and external stakeholders.
4. **Data Protection Lead (DPO):**
    - Ensures compliance with data protection regulations.
    - Manages reporting of data breaches to the Information Commissioner's Office (ICO).
5. **Trustees:**
    - Provide oversight and ensure appropriate resources are allocated for response and recovery.

Incident Response Phases

Preparation

The school will:

- Regularly update and test its IT systems, security protocols, and this IRP.
- Provide annual training to staff on recognising and responding to cyber security incidents (Educare).
- Maintain an updated inventory of IT assets and a list of third-party service providers.

Detection and Identification - Responsible: IT Lead, DSL/s (for safeguarding concerns)

Actions:

- Monitor systems using firewalls, antivirus software, and intrusion detection tools to identify suspicious activity.
- Encourage staff and pupils to report unusual activity immediately.
- Confirm the type, scope, and severity of the incident.

Key Questions:

- What type of incident has occurred?
- What systems, data, or users are affected?
- Is the incident ongoing or contained?

Containment - Responsible: IT Lead / 3rd Party Support as necessary

Short-term Actions:

- Disconnect affected systems or devices from the network to prevent further spread.
- Block malicious IP addresses or URLs.
- Implement temporary access controls (e.g., disabling compromised accounts).

Long-term Actions:

- Apply patches or updates to resolve vulnerabilities.
- Ensure back-ups are secure and intact.

Eradication - Responsible: IT Manager.

Actions:

- Remove malware, malicious accounts, or unauthorised access from the system.
- Conduct a thorough review to ensure all traces of the threat have been eliminated.
- Update antivirus and other security tools to prevent recurrence.

Recovery - Responsible: IT Lead

Actions:

- Restore systems, services, and data from secure back-ups.
- Verify the integrity of restored systems.
- Monitor systems for signs of recurring issues.

Key Questions:

- Have all systems been restored to full functionality?
- Have users been informed about any changes to procedures or access?

Reporting - Responsible: DP Lead, Headteacher.

Actions:

- If a personal data breach occurs, report to the ICO within 72 hours, as required by GDPR.
- Notify affected individuals if their data is compromised.

- Prepare an incident report for trustees, summarising the cause, impact, and lessons learned.

Key Questions:

- Does the incident require reporting to external authorities?
- What information must be shared with stakeholders?

Lessons Learned - Responsible: Incident Response Coordinator (IT Lead), Trustees.

Actions:

- Conduct a post-incident review to evaluate the response and identify improvements.
- Update this IRP, policies, and staff training accordingly.

Incident Reporting Workflow

1. **Initial Report:**
    - Incident is reported to the IT Lead or DSL immediately.
    - Initial assessment is conducted to determine severity.
2. **Escalation:**
    - High-risk incidents (e.g., data breaches, safeguarding concerns) are escalated to the Headteacher and DP Lead.
3. **Response Activation:**
    - IT Lead implements this IRP.
4. **Communication:**
    - Regular updates are provided to stakeholders during and after the response.

Communication Protocols

Internal:

- Staff will be informed via email or phone regarding incidents affecting their roles.
- Pupils will be informed through appropriate channels determined by headteacher / IT Lead.

External:

- Parents will be notified of incidents involving pupil safety or significant service disruptions.
- External authorities (e.g., ICO, DfE) will be contacted as required.

January 2025

Lucy Meyer

Co-Principal