Luccombe Hub This document forms part of the policy handbook and is intended for use at Luccombe Hub	
Title:	**Cyber Security Policy**
Subject Area:	Safeguarding – Whole Centre
Applies:	Immediately
Issue/Review Date:	21 Oct 2025
Next Review:	NLT 20 Oct 2028
Sponsor:	Henri Monier-Williams
Contact:	Marcus Monier-Williams
Email:	marcus@Luccombehub.com

Contents

Contents 1

WHY DOES THE LUCCOMBE HUB NEED A CYBER SECURITY POLICY? 3

Objectives 4

Roles and Responsibilities 4

ACCEPTABLE USE – STAFF 5

- **Staff Laptops** 5
- **Use of Equipment at Home** 5
- **Internet Connections** 5
- **Password Management** 5
- **System Maintenance** 6
- **Data Protection and Usage** 6
- **Reporting Issues** 6

ACCEPTABLE USE – LEARNERS 6

- **Use of Logins and Accounts** 6
- **Use of Equipment** 6
- **Respect and Kindness Online** 6
- **Mobile Phones** 7
- **Use of Social Media** 7
- **Monitoring and Safety** 7
- **Staying Safe Online** 7

Access Control 7
Account Provisioning 7
Role-Based Access 7
Account Management and Offboarding 8
Network and System Security 8
Web Filtering and Firewall Protection 8
Malware Protection and Endpoint Security 8
System Updates and Patch Management 8
INCIDENT RESPONSE PLAN 8
Identify and Report the Incident 9
Contain and Mitigate 9
Investigate and Document 9
Notify Stakeholders (as Required by Law) 9
Review and Update Procedures 9
Staff Awareness and Training 9
Training 10
Reporting Suspicious Activity 10
Continuous Improvement 10
Annex 1 - The Luccombe Hub - Online Safety agreement 12

WHY DOES THE LUCCOMBE HUB NEED A CYBER SECURITY POLICY?

Protects Sensitive Information

This policy defines how sensitive data (staff and learner information, financial records, or intellectual property etc) must be handled and protected. It will help prevent data breaches, leaks, and unauthorised access.

Sets Clear Security Expectations

It establishes rules and responsibilities for all staff, contractors, and vendors. Everyone knows what's acceptable (e.g., password policies, data sharing, use of personal devices).

Helps Prevent Cyber Attacks and Details How We Respond

With clear procedures for incident detection, response, and recovery, The Luccombe Hub can:

- React quickly to minimise damage.
- Maintain operations.
- Learn from incidents and strengthen our defences.

This policy also supports Legal and Regulatory Compliance

Like any other organisation The Luccombe Hub must follow strict laws and guidelines (GDPR, KCSiE 2025, Working Together to Safeguard Children, ISA Inspectorate). A cybersecurity policy ensures compliance and avoids fines or legal penalties.

Builds a Culture of Security Awareness

Policies promote awareness and accountability. This helps employees to understand the risks and ensure that we only use best practices. Human error is a major cause of breaches.

Reduces Financial and Reputational Risk

Cyber incidents are costly — not just in money but in trust. Parents and local authorities trust with their data, and we have a responsibility to look after the data. Whilst it is impossible to predict or in some cases prevent a cyber attack, we can work towards lessening the likelihood of an attack and defining how we will respond should a cyber-attack happen

Provides a Framework for Continuous Improvement

Cyber threats evolve constantly, working with our partner Assist Networks – we look to establish a secure environment which is regularly reviewed and adapts to new risks and technologies.

Scope

This policy applies to:

- All staff, contractors, students, visitors and third-party providers (including Assist Networks) who access the school's digital systems.
- All school-owned or connected systems, including Microsoft Entra, Bitdefender, and Smoothwall platforms.
- Devices – laptops, phones, iPads and all other IT equipment used for school business, this also includes all cloud-based applications.

Objectives

The primary objectives of this Cybersecurity Policy are to ensure that the school's digital systems, data, and users are protected in accordance with educational safeguarding standards and legal requirements. Specifically at The Luccombe Hub, we aim to:

- Prevent Unauthorised Access and Data Breaches.
- Safeguard sensitive pupil, staff, and school data against unauthorized access, loss, or misuse.
- Utilise Microsoft Entra for secure identity management and multi-factor authentication (MFA).
- Maintain endpoint and network protection using Bitdefender and Smoothwall.
- Ensure Business Continuity and Operational Resilience.
- Maintain reliable and secure access to critical systems for teaching, learning, and administration.
- Implement backup and recovery measures to minimise disruption during technical failures or cyber incidents.
- In collaboration with Assist Networks to provide rapid incident response and technical support.
- Comply with Legal, Regulatory, and Safeguarding Requirements - meet the requirements of the UK GDPR, Data Protection Act 2018, KCSiE 2025 and Department for Education (DfE) digital and safeguarding standards.
- Protect pupils' online safety through robust filtering and monitoring controls (Smoothwall).
- Maintain records and evidence of compliance for audit and inspection purposes.
- Promote a Culture of Cyber Awareness and Responsibility - Ensure that all staff, pupils, and third-party providers understand their role in maintaining cybersecurity.
- Provide ongoing training and awareness sessions on safe digital practices, phishing prevention, and data handling.
- We aim to continuously improve Cybersecurity Maturity by regularly assessing risks and updating security controls in line with evolving threats.

Roles and Responsibilities

- Principal - Overall accountability for cybersecurity and safeguarding compliance.
- DSL/DDSL/SLT - Ensures cyber practices align with safeguarding policies.

- IT Manager – Monitoring of IT provision, resources and overall health. First port of call for all IT issue. In the absence of the IT Manager, Marcus Monier-Williams should be contacted in the first instance.
- Assist Networks – Provides 2nd Line Support – Monitoring of Bitdefender, Network support
- Staff - Follow cybersecurity and data protection practices, report incidents promptly.
- Learners - Use school systems responsibly and safely.

ACCEPTABLE USE – STAFF

This section outlines the responsibilities of all staff members when using school-provided devices and systems, whether on-site or at home. Compliance with these rules ensures the protection of sensitive information and the reliability of school IT systems.

Staff Laptops

Staff are issued laptops according to operational need. While we aim to ensure that all full-time members of staff have sole use of a company laptop, this may not always be possible, particularly for part-time roles.

All staff must ensure that company laptops are used by staff only and are not accessed by learners. Dedicated learner laptops are available for learner use.

Use of Equipment at Home

Staff may take school-issued laptops or tablets home solely for work-related purposes.

Devices must not be used for personal activities such as streaming, gaming, or accessing personal accounts.

Staff must ensure devices are stored securely when not in use and protected from access by others (including family members).

Internet Connections

When working remotely, staff must use a secure, password-protected home Wi-Fi network with WPA2 or WPA3 encryption.

Staff must not connect to free or public Wi-Fi networks (e.g. coffee shops, airports, or other unsecured hotspots). Staff should use their data allowance for connections outside of their home or The Luccombe Hub locations. Staff have a monthly data allowance of 4GB which is pooled.

Password Management

All user accounts must have a strong password that:

- Contains at least 9 characters, including upper and lower case letters, at least one number, and at least one special character (e.g., !, @, #, $).
- Passwords must be changed regularly (at least every 90 days) and must not be reused across different systems.
- Passwords must never be shared with anyone, including colleagues or IT support.

System Maintenance

Staff must reboot their school devices at least once per week to ensure security updates and patches are properly applied.

Devices should remain connected to the internet regularly so that updates and antivirus definitions (via Bitdefender) can install automatically.

Data Protection and Usage

All data accessed or stored on school devices must relate to school business only.

Staff must use their Luccombe login credentials for all system access to ensure proper identity verification and security logging.

Confidential data must not be downloaded, copied, or transferred to personal storage or cloud services.

Reporting Issues

Any suspected security incident, unusual device behaviour, or potential breach must be reported immediately to the IT Manager or a member of SLT.

Incident Response

In the event of a cybersecurity incident (e.g. malware infection, phishing attempt, data breach) staff must: Report immediately to the IT Manager or any member of the SLT.

ACCEPTABLE USE – LEARNERS

This section sets out how learners at The Luccombe Hub are expected to use school technology and digital systems safely and responsibly. These rules are designed to protect everyone and ensure that technology supports learning in a safe environment.

Use of Logins and Accounts

Learners must always use their own login details when accessing any school computer, tablet, or online system. Sharing passwords or logging in as another person is strictly prohibited.

Use of Equipment

Learners must only use Luccombe Hub owned devices and equipment. Personal laptops, tablets, or other devices must be handed in on arrival to school. Personal devices must not be connected to the school network.

Respect and Kindness Online

Learners must be kind and respectful to other learners and other people when using school systems or communicating with others. Cyberbullying, harassment, or unkind messages—whether in class or online—will not be tolerated.

Staff are to report any potential safeguarding issues, using My Concern, or if unsure to the DSL/DDSL on duty. All learners must sign the IT Code of Conduct (signed on joining).

Mobile Phones

All learners must hand in their mobile phone to staff when they arrive at school and collect it before going home.

Use of Social Media

Learners must not access or use social media on any Luccombe Hub IT equipment or network.

This includes websites or apps such as Facebook, Instagram, TikTok, Snapchat, or similar platforms.

Monitoring and Safety

All activity on school computers, tablets, and networks is monitored using Smoothwall.

Any attempt to access inappropriate or unsafe websites are reported to the DSL/DDSL in real time via email.

Any suspicious activity will be reported to the Designated Safeguarding Lead (DSL) and may be investigated further.

Staying Safe Online

Learners should report anything online that makes them feel uncomfortable, worried, or unsafe to a member to the member of staff working with them or the DSL/DDSL immediately.

The Luccombe Hub promotes a positive and safe environment. This includes the responsible safe use of technology and forms part of its safeguarding commitment.

Access Control

To maintain secure access to school systems and protect sensitive data, The Luccombe Hub enforces strict access management procedures:

Account Provisioning

Staff user accounts are created only when confirmation of a new starters has been received, this is after the contract of employment has been signed and all other pre-employment checks are complete, i.e DBS, referencing etc.

All user accounts are provisioned by the IT Manager and managed through Microsoft Entra (formerly Azure Active Directory).

Microsoft Entra does allow the securing of accounts using multi-factor authentication (MFA) to protect against unauthorised access. At The Luccombe Hub we have not enforced this as yet, however we do plan to rollout the facility with a completion towards the end of 2026

Role-Based Access

Access permissions are assigned based on the principle of least privilege, ensuring users only have access to the systems and data necessary for their role. This level of access that is required for each job role is decided by the Senior Leadership Team

Administrative access over Microsoft Entra is restricted to authorised individuals. Except for the IT Manager, administrative access is granted through an additional set of credentials.

Account Management and Offboarding

Leavers' accounts immediately have the password changed, and all Microsoft licencing removed. The account will be disabled within 24 hours of departure to prevent unauthorised access. Accounts will remain disabled for 2 months following which the account will be deleted

At The Luccombe Hub we do not assign temporary or guest accounts, if there is a situation whereby this is the only option, the account and its necessity will be reviewed a minimum of weekly.

Network and System Security

The Luccombe Hub maintains a secure and monitored network environment to protect learners, staff, and data from digital threats. All systems are managed in partnership with Assist Networks to ensure technical and safeguarding compliance.

Web Filtering and Firewall Protection

The school's network is protected by Smoothwall web filtering. This ensures compliance with KCSiE 2025 as well as ISI regulations. This system not only blocks inappropriate or harmful online content, but emails all DSL/DDSL's in real time stating, who has searched inappropriate material, the device used, the time and date as well as subject matter. This instant reporting really assists in safeguarding pupils. With this information we can support the learner to promote safe internet.

Malware Protection and Endpoint Security

All school devices are protected by Bitdefender Endpoint Security, which provides real-time antivirus, anti-malware, and threat detection. Bitdefender automatically scans for potential threats, isolates suspicious files, and alerts IT support (Assist Networks) for investigation.

System Updates and Patch Management

Patching is important. Microsoft and some other vendors release security updates weekly. Not all patches are relevant, but some contain updates the remove a vulnerability. We use system 1 to alert us to missing patches and vulnerabilities. Both the IT manager and Assist Networks have access to the system 1 portal. Devices must be connected to the internet to receive automatic updates. Any device found to be out of date or unprotected may be restricted from accessing the school network until compliance is restored.

INCIDENT RESPONSE PLAN

The Luccombe Hub follows a structured process to identify, contain, and resolve any cybersecurity incidents that could impact data, systems, or users. This ensures that incidents are handled effectively, reported appropriately, and used as learning opportunities for continuous improvement.

Identify and Report the Incident

Any member of staff who suspects or detects unusual system activity, data loss, phishing, malware, or unauthorized access must report it immediately to IT Manager and/or a member of the SLT.

Learners should inform a member of staff straight away if they notice anything unusual or concerning on school devices.

Contain and Mitigate

The IT Manager along with Assist Networks will act promptly to isolate affected systems, devices, or accounts to prevent further spread or damage.

Temporary measures may include disabling network access, resetting passwords, or switching to backup systems.

Investigate and Document

A detailed investigation will be carried out to determine the nature, cause, and impact of the incident.

Findings, evidence, and actions taken will be documented in the school's incident log, maintained by the DSL and IT support team.

Notify Stakeholders (as Required by Law)

If the incident involves a data breach, the Data Protection Officer (DPO) will assess whether it must be reported to the Information Commissioner's Office (ICO) within 72 hours, in line with UK GDPR requirements.

Affected individuals and relevant authorities will be informed where appropriate.

The Principal and Head of Education will coordinate any required external communications. No member of staff should talk to the press or any other person. If approached the only response should be either 'no comment' or no response at all.

Review and Update Procedures

After every incident, a post-incident review will be conducted to identify lessons learned and improve procedures.

Security policies, technical controls, and staff training will be updated accordingly to prevent recurrence.

Staff Awareness and Training

The Luccombe Hub is committed to maintaining a strong culture of cybersecurity awareness and responsibility among all staff. Ongoing education ensures that staff can identify potential threats, respond appropriately, and uphold the school's safeguarding and data protection standards.

Training

All staff must complete Online Safety training annually. Staff must achieve a high percentage pass mark to pass the course(s). Staff who do not complete the course must revisit the entire course. Different questions are used at each attempt.

Courses are delivered by our training partners 'Smart Log' and include:

- What is online safety
- Online Abuse
- Risks to Children
- Risks to Children – Roles and Responsibilities
- Cyber Bullying
- Grooming
- Sexual Exploitation
- What are the signs of online abuse
- What to do if you discover a victim of online abuse
- Online Safety
- Harmful Content
- Online Radicalisation and Extremism
- Violent Content
- Cyber Security
- Malware
- Ransomware
- Phishing
- Cyber Security
- Identity Theft
- Copyright
- Artificial Intelligence
- Reporting & Advice

Reporting Suspicious Activity

Staff must immediately report any suspicious or unexpected emails to the IT Manager and SLT.

In addition, staff must notify the IT Manager and Assist Networks if they believe a system, device, or account may have been compromised.

Prompt reporting allows the IT team to investigate and mitigate risks effectively.

Continuous Improvement

The Luccombe Hub, in collaboration with Assist Networks, will review training materials regularly to ensure they reflect current threats and best practices.

Refresher sessions may be required following a security incident or policy update.

Annex 1 - The Luccombe Hub - Online Safety agreement

The Luccombe Hub Centre understands the importance of children being able to use the internet for education and personal development. This may include social media platforms such as You Tube, games and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

This agreement is part of our E-Safety Policy and Safeguarding policy. If you would like to know more about this, please speak to Henri Monier Williams who can be contacted by emailing office@luccombehub.com

More information about online safety is available from learning.nspcc.org.uk/safeguarding child protection/online-safety-for-organisations-and-groups

Learners: please read the following agreement and discuss it with your parents/carers and facilitator.

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the group leader. If you have any questions or concerns, please speak to Henri Monier-Williams — Centre Lead.

Name of Learner	

Young person's agreement

- I will only use my own Luccombe Hub logon details.
- I will keep my passwords securely — If I forget my passwords I can ask for a password reset
- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal.
- If I accidentally come across any such material I will report it immediately to the facilitator.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or facilitator and am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to Henri Monier-Williams, Lydia Bryant or my facilitator.

I understand that my internet use at The Luccombe Hub will be monitored and logged and can be made available to the Centre lead, Henri Monier-Williams. I understand that these rules are designed to keep me safe and that if I choose not to follow them, The Luccombe Hub Centre may contact my parents/carers and pass any relevant information onto multi agency teams where applicable.

Please sign below, to confirm that you and the learner have discussed Online Safety and that the learner agrees to follow the rules set out above				
Parent/Carer Name		Learner Name		
Parent/Carer Signature			Date	
Learner Signature			Date	