Cyber Security Policy

Rationale

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.

This Cybersecurity Policy outlines Willow Learning Trust's (WLT) 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 Glenthorne, Abbey and Aragon 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 for the school.

Risk Management

WLT will include cybersecurity risks on its organisational risk register, reporting on the progress and management of these risks to Trustees once a year.

Physical Security

WLT 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, WLT 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 an e-mail scam, they must change their password and inform WLT IT Support as soon as possible. Personal accounts should not be used for work purposes. WLT implements multi-factor authentication for all users logging in externally. Those users with access to sensitive or confidential data will be asked to use multi-factor authentication every time.

Please note that accounts cannot be accessed from abroad, this is to reduce the risk of a cyber-security threat.

Devices

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

- Screen lock devices that are left unattended using Windows key+L
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to WLT Support
- Change all account passwords at once when a device is lost or stolen (and report immediately to WLT IT Support)
- Report a suspected threat or security weakness in GHS, Abbey or Aragon's systems to the Trust Network Manager immediately

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
- Alerts sent to IT Helpdesk and raised as a ticket
- Minimal administrative accounts

Data Security

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

WLT 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 1st Veeam server, (GHS - copied to 2nd Veeam server), then critical/all primary servers copied to Cloud. Portal air gapped storage device used for 6 monthly backup archives. Stored in secure GHS Server room and encrypted with BitLocker.
- 2 different types of media – Local HD and Cloud for critical servers
- 1 copy offsite/offline Abbey/Aragon servers copied to Cloud. Critical GHS servers copied to Cloud.
- Office 365 Tenancy backed up by Veeam/CT to Cloud.

Sharing Files

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

- Consider if an email could be a credential phishing/scam 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
- Keep Trust files on school systems
- Not to send school files to personal accounts
- Verify 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
- Be Wary of Attachments and Links on emails: Avoid clicking on links or downloading attachments from unknown or unexpected emails.

Training

WLT recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate annual 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. Staff will be provided with a cyber-security leaflet and copy of the cyber-security policy.

System Security

WLT IT Support will build security principles into the design of IT services for the 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

Major Incident Response Plan

The Trust Network Manager will develop, maintain, and regularly review our Disaster Recovery plan. This plan includes:

- Categories and severities of a "disaster"
- Risk assessments
- Key system impact assessments and restoration priorities (i.e. which servers needs to be restored first for the school to become operational again) (Business Impact Analysis and Recovery Time Objectives)
- Emergency plans for the school to function without access to systems or data
- Roles and responsibilities
- Emergency budgets and how they can be accessed
- Key agencies for support (e.g. suppliers and support)

Maintaining Security

WLT understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. WLT will budget appropriately to provide training and support to defend against cyber-attacks.

This policy was agreed in July 2024

Next review: July 2026

Appendix. A

Cyber Security Leaflet

Rationale

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 handout provides essential guidelines to protect our systems, services and data and safeguard your information in the event of a cyberattack.

1. **Password Security**
   - **Create Strong Passwords:** Use a mix of upper- and lower-case letters, numbers and symbols. Aim for at least 9 characters.
   - **Avoid reusing the same password:** Never use the same password across multiple web sites!
   - **Keep Passwords Secret: Never write down or share your password**

2. **Data Security**
   - **Use the Microsoft Cloud:** Always use OneDrive or SharePoint to store confidential data. Ensure you use the appropriate areas of SharePoint.
   - **Caution when Sharing: Be careful when sharing folders and their contents.**
   - **SharePoint: Know which areas of SharePoint you should use for confidentiality.**
   - **USB Sticks: The use of USB sticks is not permitted by the Trust.**

3. **Multi-Factor Authentication (MFA)**
   - **MFA:** WLT use MFA for accessing systems from home as well as in school for certain staff. This adds an extra layer of security by requiring a second form of verification (e.g. a code sent to your phone)
   - **It's a good idea to use this for your personal accounts as well!**

4. **Devices**
   - **Keep Software Up to Date:** Keep all your devices up to date. WLT roll out patches, if your PC wants you to reboot, please do this as soon as possible.
   - **Lock your PC: Use Windows key + L when it's unattended**
   - **Sharing Logins:** Never log a PC in for someone else
   - **NB:** WLT user accounts cannot be accessed from abroad to reduce the risk of a cyber-security threat.

5. **Email Security**
   - **Be Wary of Attachments and Links:** Avoid clicking on links or downloading attachments from unknown or unexpected emails.
   - **Scam e-mails:** Be on the lookout for suspicious e-mails that are trying to get you to log into fake websites, otherwise known as "phishing". Verify the sender's email address and look for spelling errors or unusual requests.
   - **If something doesn't look right, report it to the IT service desk https://helpdesk.thewlt.org.uk/**

6. **Monitoring**
   - **Device Monitoring:** All staff and pupil school devices are monitored with "Smoothwall and/or LGfL" for filtering/key input monitoring.

7. **Incident Response**
   - **Report it:** Report any suspicious activity to WLT IT team immediately. All reports are dealt with in confidence.