The Willow LEARNING TRUST

DATA SECURITY POLICY

Statement of intent

The Willow Learning Trust (WLT) is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the WLT are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The aim of this policy is to inform staff, pupils, parents and visitors to the WLT schools of the security arrangements and controls in place and encourage them to help ensure that these are implemented effectively to protect individuals' privacy. This policy and the associated procedures apply to all individuals entering WLT school premises.

1. Legal framework

This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- The Computer Misuse Act 1990
- The General Data Protection Regulation (2018)

This policy has due regard to the WLT's policies and procedures including, but not limited to, the following:

- Data Protection Policy
- Code of Conduct and ICT Acceptable Use
- Data Retention Policy

2. Responsibilities

The WLT as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements. All staff members are responsible for ensuring that any records for which they are responsible are accurate, maintained and stored securely and disposed of correctly, in line with the provisions of this policy.

- The CEO holds overall responsibility for this policy and for ensuring it is implemented correctly.
- The data protection officer (DPO) is responsible for promoting compliance with this policy, ensuring all staff are aware of the importance of storing records securely and disposing of records correctly in accordance with retention periods.
- The Trust Network Manager (TNM) is responsible for the overall monitoring and management of data security.
- The Executive Headteacher (primaries) and Headteachers of WLT schools are responsible for ensuring the policy is implemented correctly in their schools.

3. Information audit

The WLT conducts information audits to update an Information Asset Register. This is in order to evaluate the information the WLT is holding, receiving and using, and to ensure that this is correctly managed in accordance with the General Data Protection Regulation (GDPR). This includes the following information:

- Paper documents and records;

- Electronic documents, databases and records;
- Sound recordings;
- Video and photographic records;
- Hybrid files, containing both paper and electronic information.

The DPO is responsible for completing the information audit. The information audit will include the following:

- The WLT's data needs;
- The information needed to meet those needs;
- The format in which data is stored;
- How long data needs to be kept for;
- Vital records status and any protective marking;
- The person responsible for maintaining the original document.

The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

4. Storing and protecting information

The TNM will:

- Conduct a back-up of information on a daily basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data. Backed-up information will be stored in separate locations on the WLT school premises'.
- Be responsible for continuity and recovery measures to ensure the security of protected data.
- Notify of any damage or theft of data which will be managed in accordance with the WLT's Data Protection Policy.

All staff will ensure that confidential paper records are:

- Kept in a locked filing cabinet, drawer, office or safe, with restricted access.
- Not left unattended or in clear view when held in a location with general access.

Digital data:

- Is coded and encrypted on a network drive that is regularly backed-up off-site.
- Sensitive, confidential records such as child protection files are stored using specific safeguarding software.
- Staff are strongly advised not to use memory sticks are not to hold personal information unless they are encrypted.
- All electronic devices require user credentials to access in order to protect the information on the device in case of theft.
- Where possible, the WLT enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.
- Circular emails to personal email addresses are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

All staff members and governors are made aware of their professional responsibilities by abiding with the WLT Code of Conduct. The WLT takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Where personal information that could be considered private or confidential is taken off the premises, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices and paperwork under lock and key or using encrypted portable media to store data. The person taking the information from the WLT premises accepts full responsibility for the security of the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the WLT containing sensitive information are supervised at all times.

The physical security of the WLT schools' buildings and storage systems, and access to them, is reviewed termly by the site managers in conjunction with the headteachers. If an increased risk in vandalism, burglary or theft is identified, this will be reported so that extra measures to secure data storage can be put in place.

5. Secure configuration

An inventory will be kept of all IT hardware and software currently in use across the WLT. This will be stored digitally by the TNM and will be audited on a regular basis to ensure it is up-to-date. Any changes to the IT hardware or software will be documented using the inventory.

All systems will be audited to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory. The Trust will work towards removing any software that is out-of-date or reached its 'end of life', i.e. when suppliers end their support for outdated products such that any security issues will not be rectified. Any unsupported software or hardware still in use will be reviewed to ensure the risk to data security is kept at a minimum.

6. Network security

The WLT will employ firewalls in order to prevent unauthorised access to the systems.

Firewalls for the schools within the WLT will be deployed as a:

- Localised deployment: the broadband service connects to a firewall that is located on an appliance or system on each school premises, as either discrete technology or a component of another system.

Although each school's firewall is managed on the premises, it is the responsibility of the TNM to effectively manage the firewall and ensure that:

- The firewall is checked regularly for any changes and/or updates, and that these are recorded using the inventory.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is checked weekly to ensure that a high level of security is maintained and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the CEO.

7. Malware prevention

The WLT understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls. The TNM will:

- Ensure all WLT devices have secure malware protection and undergo regular malware scans.

- Ensure malware protection is updated on a weekly basis to ensure it is up-to-date and can react to changing threats.
- Ensure malware protection is also updated in the event of any attacks to hardware and software.
- Ensure that websites are filtered on a weekly basis for inappropriate and malicious content and block access to websites with known malware immediately.
- Review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.
- Ensure the WLT mail security technology will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

8. User privileges

The WLT understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The TNM will:

- Ensure that user accounts are set up to allow users access to the facilities required, whilst minimising the potential for deliberate or accidental attacks on the network.
- Record any member of staff or pupil that has accessed inappropriate or malicious content in accordance with the monitoring process outlined in the Code of Conduct.
- Create and manage a multi-user account for visitors such as volunteers. Access will be filtered and usernames/passwords will be changed on a termly basis.
- Ensure all inactive users or users who have left the WLT are deleted and do not have access to the system.
- Review the system on a termly basis to ensure the system is working at the required level.

The WLT believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users. Staff are aware it is a disciplinary offence to disclose passwords or security information as per the Code of Conduct. All users will be required to change their passwords every 90 days and are advised to ensure that passwords are strong. Workstations must be locked when unattended to prevent unauthorised access. Access to the 'master user' password used by the TNM is only available to relevant authorised ICT staff.

Secondary Pupils are responsible for remembering their passwords; however, the TNM will be able to reset them if necessary.

Primary Pupils will have either individual logins or class logins will be used.

9. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The WLT informs all pupils and staff that their usage will be monitored, in accordance with the WLT's Code of Conduct.

Any alerts will be documented using an incident log by the DSL. All incidents will be responded to in accordance with our Code of Conduct. All data gathered by monitoring usage will be kept by the TNM. This data may be used as a method of evidence for supporting a not yet discovered breach of network security. In addition, the data may be used to ensure the WLT is protected and all software is up-to-date.

10. Removable media controls and home working

The WLT understands that pupils and staff may need to access the WLT network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

- The TNM will encrypt all WLT-owned devices such as laptops and tablets, to ensure that they protected.
- Pupils and staff are not permitted to use their personal devices where the school can provide alternatives, such as work laptops and tablets, unless instructed otherwise by the Headteacher.
- If pupils and staff are instructed to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security.
- When using laptops, tablets and other portable devices, the relevant Headteacher will determine the limitations for access to the network.
- The WLT uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.
- All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.
- Wi-Fi networks will be password protected and will only be given out as required. A separate Wi-Fi network will be established for visitors at the WLT to limit their access to printers, shared storage areas and any other applications which are not necessary.

11. Backing-up data

The TNM will:

- Perform and log a back-up of all electronic data held by the WLT schools on a daily basis.
- Perform an incremental back-up on a monthly basis of any data that has changed since the previous back-up.
- Where possible, run back-ups overnight to be completed before the beginning of the next school day.

12. User training and awareness

The TNM and Executive Headteacher will arrange training:

- For pupils and staff on an annual basis to ensure they are aware of how to use the network appropriately in accordance with the Code of Conduct.
- For staff as part of their induction programme.
- For all staff members following an attack or significant update.
- To ensure that all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.
- To ensure that all users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks.

13. Policy review

This policy is reviewed every two years by the TNM, DPO and the Executive Headteacher.

The next scheduled review date for this policy is **May 2023**.