Willow Bank School

Learn Grow Achieve Together

Cyber Security Policy

Approved by:	Headteacher/Governors	**Date:** September 2025	
Last reviewed on:	September 2025		
Next review due by:	September 2027		

Contents

Definition of Cyber Security: Application of technologies, processes and controls to protect systems, networks and data from cyber-attacks.

1. Introduction

The protection of information and communication technologies (ICT) within our school environment is essential. This Cyber Security Policy establishes a framework to secure digital resources, protect personal data, and ensure a safe online environment for students, staff, and stakeholders.

Willow Bank school is committed to safeguarding its information assets, IT systems, and personal data from cyber threats, in line with UK legislation including the Data Protection Act 2018, UK GDPR, and *Keeping Children Safe in Education* guidance. This policy outlines our approach to cyber security, defines roles and responsibilities, and ensures legal compliance.

2. Scope

This policy applies to all students, staff, governors and external partners, who have access to school ICT resources.

3. Objectives

- To protect the confidentiality, integrity, and availability of digital information.
- To safeguard the personal data of students, staff, and stakeholders.
- To ensure compliance with relevant legal and regulatory requirements.
- To foster a culture of cyber security awareness and responsibility.
- To respond effectively to cyber security incidents and breaches.

4. Roles and Responsibilities

Role	Responsibilities
Head of Centre	Nicola Laughton Headteacher has overall responsibility for policy implementation and cyber security strategy.
IT Manager/Team	St Helens Council Schools IT Team maintain and secure the schools IT infrastructure, implement technical measures and controls to protect against cyber threats, monitor systems, respond to and mitigate the effects of incidents, manage access and updates.
Data Protection Officer	HY Education Tel: 0161 543 8884 email: DPO@wearehy.com Monitor compliance with data protection laws and our data protection Polices; advise on, and monitoring, data protection impact assessments; raise awareness of data protection issues, cooperating and being the first point of contact with the Information Commissioner's Office, members of staff, parents and pupils.

Role	Responsibilities
All Staff	Adhere to the cyber security policy and procedures, participate in annual training and awareness programmes, report any suspicious activity and/or incidents promptly, safeguard their login and passwords.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly, follow the schools' cyber security guidelines and rules, respect the privacy and security of others and report any concerns.
School Administration Staff	Ensure the development and implementation of the cyber security policy, ensure adequate resources are allocated for cyber security measures, oversee the training and awareness programmes, review and update the policy periodically, Helen Lyons, Exams Officer, will oversee Exam Board compliance in relation to issuing/removing staff accounts, access rights and multi factor authentication Apps.

5. Technical Security Measures

Willow Bank School implements the following security measures through St Helens School IT Team, scaled to our size and needs:

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

6. Acceptable Use

- Using school IT resources for educational purposes only.
- Not accessing, sharing, or downloading inappropriate content.
- Respecting intellectual property rights and avoiding plagiarism.
- Not engaging in cyberbullying, harassment, etc.
- Protecting personal information and not sharing login details

7. Data Protection and User Account Management

Willow Bank School is committed to protecting the personal data it processes, measures include

- Where necessary, encrypting sensitive data to prevent unauthorised access.
- Password governance must follow NCSC Guidance: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

- Regularly updating software and systems to address vulnerabilities.
- Implementing and regularly reviewing, access controls to restrict data access based on roles.
- Monitoring account activity and conducting data audits to ensure compliance with data protection laws
- Accounts are promptly disabled when users leave.

8. Staff Training and Awareness

- All staff must complete cyber security training and annual refresher training.
- Phishing awareness and social engineering defence training.
- Awareness campaigns on the importance of cyber security will be promoted.
- Resources and materials on best practices will be made available.
- Records of cyber training must be retained for all staff and be available for inspection.

9. Incident Response

In the event of a cyber security incident:

- The IT department will initiate an immediate investigation.
- Containment measures will be implemented to prevent further damage.
- Affected individuals will be informed promptly.
- A report detailing the incident and response actions will be documented.
- Preventative measures will be revised to avoid future occurrences.

10. Compliance and Review

Compliance with this policy is mandatory. The policy be reviewed every two years or as required to:

- Ensure it covers evolving cyber security threats and best practices.
- Incorporate feedback from stakeholders.
- Adapt to changes in legal and regulatory requirements.

11. Conclusion

Cyber security is a shared responsibility. By following this policy, we can protect Willow Bank school's digital resources, safeguard personal data, and maintain a secure environment that supports learning and development while building a culture of vigilance, accountability, and safe digital practices.