JIGSAW LEARNING TRUST

Cyber Security Policy

Introduction

The purpose of this policy is to alert Trustees, governors, all staff, and those responsible for ICT and online safety to the potential risks of cyber-attacks to the school, to set out what protective measures we have in place, and to describe the basic principles and responsibilities of good cybersecurity and digital safeguarding.

Cyber-attacks are deliberate attempts by individuals or organisations to breach, disrupt, or exploit a computer system, network, or data. These attacks may disable, steal, modify, or deny access to systems or data, or use compromised systems for further attacks.

Under Keeping Children Safe in Education (KCSIE) 2025, schools must ensure robust cyber resilience and oversight of filtering and monitoring systems. Online harms, including misinformation and disinformation, are recognised safeguarding concerns. This policy supports the safeguarding, data protection, and online safety frameworks of Jigsaw Learning Trust.

2. Common Types of Cybersecurity Attacks Affecting Schools

The Trust recognises the following as the most common types of cyber threats that can affect schools:

- Phishing – deceptive emails or messages that trick users into revealing sensitive data.
- Ransomware – malicious software that encrypts files and demands payment for their release.
- Password or Brute Force Attacks – attempts to guess or steal passwords for unauthorised access.
- Denial of Service (DDoS) – overwhelming systems with traffic to make them unusable.

- Insider Threats – malicious or accidental misuse of access by authorised individuals.
- Supply Chain Risks – attacks through third-party systems or service providers.
- Misinformation and Disinformation – online content designed to mislead, which KCSIE 2025 recognises as a safeguarding concern.

3. Connected IT Solutions – Schools Technical Support

Jigsaw Learning Trust maintains an annual Service Level Agreement with Connected IT Solutions, which provides technical support and network protection across all Trust schools. Measures in place include:

- Firewalls to monitor incoming and outgoing network traffic.
- Antivirus and anti-malware software updated regularly.
- Secure backups, tested regularly, with offsite copies.
- Multi-factor authentication for key accounts and systems.
- Regular patching and software updates across all devices.
- Network segmentation and monitoring of anomalies.
- Incident response and disaster recovery planning.
- Annual review of filtering and monitoring systems in line with KCSIE 2025.

4. National Cyber Security – Practical Tips and Do's and Don'ts

Cybersecurity is everyone's responsibility. The following do's and don'ts apply to all staff and contractors:

Do

- Use strong, unique passwords and passphrases (three random words).
- Enable multi-factor authentication wherever possible.
- Lock devices when unattended and log out after use.
- Report suspicious emails or incidents immediately to IT or leadership.
- Keep devices updated and only use approved software.

Dont

- Reuse passwords across multiple accounts.
- Click unknown links or attachments.
- Share login details or access tokens.
- Ignore system or antivirus alerts.
- Install unauthorised software or connect unknown devices.

5. Summary

All staff are required to complete annual Cyber Security Training and sign the E-Safety / Acceptable Use Agreement. Incidents or suspected breaches must be reported immediately. A cybersecurity risk assessment is completed annually and reviewed by the Trust Board. The Trust ensures all schools maintain robust systems and align with KCSIE 2025 and national NCSC guidance.

Link to staff training: https://www.ncsc.gov.uk/information/cyber-security-training-schools

A cyber security risk assessment is compiled from the above policy to focus on IT security risk and control measures in place and will be review in individual trust schools on an annual basis.