HAMBLIN EDUCATION TRUST

Cyber Security Policy

Objective

The purpose of this Cyber Security Policy is to safeguard the digital assets[1] of the Hamblin Education Trust[2] against all potential threats - internal or external, and deliberate or accidental. It is designed to ensure the continuity of educational and operational services, protect sensitive data, and to minimise reputational and financial risk.

Policy Statement

The Cyber Security Policy is approved by the Chief Operations Officer (CFOO) and applies to all employees, contractors, and third-party users of Trust systems. The Trust aims to maintain compliance with the NCSC Cyber Essentials standard as a baseline. Under the policy, the Trust will undertake to: • Protect information from loss of confidentiality[3], integrity[4], and availability[5].

- Comply with all applicable laws and regulations[6], including updates to data protection and cybercrime legislation.
- Maintain and regularly test IT services[7], including disaster recovery and business continuity plans.
- Provide mandatory cyber security training to all staff, with annual refreshers and role specific modules.
- Ensure all data breaches (actual or suspected) are reported immediately to, and investigated by, the Head of IT Operations, with clear incident response procedures, and reported to the DPO where necessary.
- Train all employees in the safe and responsible use of IT systems and data handling with a record of training completion to be maintained.
- Secure remote access to Trust systems, including the use of VPNs, multi-factor authentication (MFA), and encrypted connections.
- Ensure Trust-owned IT equipment used off-site is protected by endpoint security tools and used in accordance with acceptable use policies.
- Maintain a clear and enforceable social media policy[8], communicated to all staff and reviewed annually.
- Screen job applicants for roles involving access to sensitive data or systems, including enhanced DBS checks where appropriate.

Supporting Procedures and Guidance

Detailed procedures will support this policy, including but not limited to:

- Incident response and escalation.
- Data backup and recovery.
- Access control and user permissions.
- Anti-virus and anti-malware protocols.
- Password management and encryption standards.
- Acceptable use of IT systems.
- Device management and BYOD standards.
- Risk assessment of third-party systems and cloud services for compliance and security assurance.

Roles and Responsibilities

- The Chief Operations Officer (CFOO) will be responsible for ensuring all employees understand and comply with this policy, and for overseeing training and awareness initiatives.
- The Head of IT Operations will be responsible for managing information security, advising on policy implementation, ensuring technical controls are in place and effective, and investigating security incidents.
- All members of the Trust must adhere to the Cyber Security Policy and report any concerns or breaches immediately.

Review

This policy will be reviewed annually or sooner if significant changes occur in legislation, technology, or the threat landscape. Updates will be approved by the CFOO and communicated to all staff.

Notes

1. Digital assets include data stored electronically (onsite and in the cloud), printed materials, verbal communications, and any other form of information.
2. Hamblin Education Trust includes the central Trust and all member schools.
3. Confidentiality - ensuring access to information is restricted to authorised individuals.
4. Integrity - ensuring information is accurate, complete, and protected from unauthorised modification.
5. Availability - ensuring authorised users can access information and systems when needed.
6. Relevant legislation includes (but is not limited to): UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988, and education-specific safeguarding regulations.
7. IT services include infrastructure, software, cloud services, and user support systems.
8. Social media includes platforms such as Facebook, X (formerly Twitter), Instagram, TikTok, WhatsApp, and others.

Date of Last Review: March 2026
Next Review Due: March 2027