NEWMAN CATHOLIC TRUST

HEART SPEAKS TO HEART

Cyber Security and Digital Resilience Policy

2026-27

Review

Review Cycle	Date of Policy	Reviewed by	Review Date
Annual	New Policy	FAR/FBM	02/04/26

Ratification

Role	Name	Signature	Date
Chair of Board	Chris Izuka		02/04/26
CEO	Dr Daniel Doyle		02/04/26

Commitment to Equality:

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed. a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these. policies are reviewed regularly in this regard.

"Rooted in faith, we ignite a love of learning, foster inclusive education and empower every individual to achieve their utmost potential."

At the Newman Catholic Trust, we stand united in our unwavering mission to nurture a transformative educational experience, where every child is seen, valued, and cherished as a unique gift from God. Rooted in faith, we ignite a love for learning that awakens curiosity, sparks imagination, and fuels a lifelong journey of discovery.

Guided by the teachings of Christ and inspired by the profound wisdom of our namesake, Saint John Henry Newman, we strive to foster a community where inclusion is lived, diversity is embraced, and every individual is empowered to fulfil their highest potential. As Newman said, *"To live is to change, and to be perfect is to have changed often."* We believe that education is a sacred journey of continual transformation—intellectually, spiritually, and personally. We believe that true education is not just about knowledge, but about shaping hearts and minds, cultivating resilience, and nurturing the whole person.

Our vision is simple yet profound: To be a beacon of **Hope** and **Excellence**, where pupils are not only academically accomplished but spiritually enriched and personally inspired to make a difference in the world.
In all that we do, we seek to embody our Trust's **HEART Values**, which define who we are and guide how we serve:

- **Hope** – Believing in the boundless potential of every child, and striving to build a future filled with possibility, courage and faith.
- **Excellence** – Pursuing the highest standards in learning, leadership and love, so that every action reflects our calling to greatness.
- **Authenticity** – Living truthfully and faithfully, ensuring our words, actions and decisions are grounded in integrity and the Gospel.
- **Responsibility** – Caring for one another and for creation with compassion, stewardship and a deep sense of duty to the common good.
- **Truth** – Seeking wisdom and understanding through Christ, who is the Way, the Truth and the Life.

Together, **Heart to Heart and Hand in Hand**, we build communities of faith and learning where every child flourishes — intellectually, spiritually and morally — for the greater glory of God.

1. Purpose and Scope

The Cardinal Newman Catholic Educational Trust recognises that the security of digital systems and information is fundamental to its ability to deliver excellent Catholic education and to fulfil its duty of care to pupils, families, staff and the wider Trust community.

This policy establishes the Trust's framework for managing cyber security risks and building digital resilience across all schools and central services. It sets out the principles, responsibilities, controls and expectations that govern the Trust's approach to protecting information, systems and digital infrastructure.

The policy applies to all employees, governors, volunteers, contractors and any third party who accesses Trust systems, data or digital services. It covers all Trust schools, central services and associated governance structures.

This policy should be read alongside the Trust's Data Protection Policy, Acceptable Use Policies, Records Retention Schedule and any school-level IT policies or procedures.

2. Policy Context and Alignment

This policy is informed by and aligned with the following frameworks and standards:

- Department for Education Cyber Security Standards for Schools and Colleges
- National Cyber Security Centre (NCSC) guidance for the education sector
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE) – safeguarding of digital records
- The Trust's HEART values: Hope, Excellence, Authenticity, Responsibility and Truth

The Trust recognises that effective cyber security is not solely a technical matter. It requires strong governance, a culture of awareness and individual accountability at every level of the organisation. This reflects the Trust's commitment to Responsibility and Truth – taking collective ownership for protecting the information and systems entrusted to us.

3. Cyber Security Principles

The Trust's approach to cyber security is built around five core principles which guide decision-making, investment and practice across the organisation.

- **Secure Systems**

Trust systems are designed, configured and maintained to reduce vulnerabilities and prevent unauthorised access. The Trust invests in secure cloud-based infrastructure and works with a specialist IT provider to ensure systems meet recognised security standards.

- **Controlled Access**

Access to systems and information is restricted to authorised users and granted according to role and responsibility. The Trust operates multi-factor authentication, role-based permissions and centralised account management to ensure that access is appropriate and auditable.

- **User Awareness**

All staff and governors are trained and supported to recognise cyber threats and to follow safe digital practices. The Trust provides annual training, regular communications and simulated exercises to build and sustain awareness.

- **Governance and Oversight**

Cyber risks are monitored through the Trust's governance framework and reported to the Board through established committee structures. Risks, incidents and improvements are tracked and reviewed regularly.

- **Resilience and Recovery**

Systems are designed to protect data integrity and availability, and to enable recovery in the event of a cyber incident. The Trust maintains backup arrangements, business continuity awareness and incident response procedures.

• 4. Governance and Accountability

Cyber security is embedded within the Trust's wider governance and risk management framework. Clear lines of accountability ensure that cyber risks are identified, monitored and addressed at every level.

Body / Role	Responsibility
Board of Directors	Overall accountability for ensuring that appropriate cyber security arrangements are in place across the Trust. Receives assurance through the Finance, Audit and Risk Committee.
Finance, Audit and Risk Committee (FAR)	Provides oversight of cyber risk as part of its wider remit for risk management and internal controls. Receives regular reports and updates on cyber security posture, incidents and planned improvements. Recommends this policy for Board approval.
Risk Working Party (RWP)	Reviews operational cyber risks and IT security matters at each meeting. Considers reports from the IT provider, monitors incident trends and emerging threats, and escalates key issues to the FAR Committee. Meeting packs evidence discussion and actions.
Chief Executive Officer	Responsible for ensuring that cyber security controls are implemented across the Trust and that the policy is applied consistently. Acts as the Trust's senior risk owner for cyber security.
Chief Finance Officer	Supports the CEO in overseeing IT and digital infrastructure. Ensures that cyber security requirements are reflected in procurement, contracts and financial controls.
IT Provider (2IT Systems)	Delivers operational IT management, security monitoring and technical support on behalf of the Trust. Provides regular security reports, manages infrastructure configuration and advises on emerging risks. Strategic oversight remains with the Trust.
School Principals	Ensure that this policy is implemented at school level, that staff complete required training and that local cyber risks or incidents are reported promptly to the central team.
Local Governing Committees	Receive school-level cyber security updates when appropriate and provide local governance oversight. Escalate any concerns to the Trust Board through established channels.
All Staff and Users	Responsible for following Trust cyber security guidance, completing required training, protecting login credentials and reporting any suspected incidents or concerns immediately.

5. Technical Infrastructure and Systems

The Trust operates a centrally managed cloud-based infrastructure designed to strengthen security, reduce risk and ensure consistency across all schools.

- **Core Systems**

The Trust's primary digital environment is built on Microsoft 365 and includes the following centrally managed services:

- Microsoft SharePoint and OneDrive for secure document storage, collaboration and file management
- Microsoft Outlook and Exchange Online for email and calendar services
- Microsoft Teams for communication and collaboration
- Arbor Management Information System for pupil data, attendance and school administration

These platforms provide encrypted data storage, version control, audit logging and centralised access management. The Trust continues to migrate legacy and locally hosted systems into this environment to ensure consistent security standards.

- **Infrastructure Security**

Technical security measures are implemented and managed through the Trust's IT provider and include:

- Network security monitoring and firewall management
- Endpoint protection and anti-malware controls
- Email filtering and anti-phishing protection
- Regular patching and system updates
- Conditional Access policies restricting access based on device, location and risk level
- Geographic access restrictions where appropriate to reduce risk from overseas threats
- Cloud-based backup and data recovery arrangements

The IT provider submits regular security update reports to the Trust which are reviewed through the Risk Working Party and reported to the FAR Committee.

6. Access Controls and Authentication

Access to Trust systems is controlled through centralised account management and a layered authentication approach.

- **Account Management**

- Individual user accounts are created centrally for all staff, governors and authorised users
- Role-based permissions restrict access to systems and information appropriate to each user's responsibilities
- Accounts are reviewed when staff change roles and disabled promptly when individuals leave the Trust
- Shared or generic accounts are not permitted for accessing Trust systems containing personal or sensitive data

- **Multi-Factor Authentication**

The Trust has implemented multi-factor authentication (MFA) across Microsoft 365 services to provide an additional layer of security for all user accounts.

When accessing Office 365 or SharePoint, users are required to verify their identity using a secondary method such as a mobile authentication app or verification code. This protects Trust accounts even where a password has been compromised.

All users must complete the MFA verification process when prompted and must not attempt to bypass or disable this security control.

- **Password Security**

All users must follow the Trust's password security expectations:

- Passwords must contain at least 12 characters and include a mixture of upper and lower-case letters, numbers and symbols
- Users should adopt passphrases made up of several unrelated words where possible
- Passwords must be changed on first login and updated periodically as required by system policy
- Passwords must never be shared with colleagues, governors, family members or anyone else
- The Trust will never request passwords by email or other messaging
- Passwords must not be written down or stored in unsecured locations

7. Data Protection and Information Security

Cyber security is closely linked with the Trust's responsibilities under data protection legislation. The protection of personal data – particularly pupil and family data – is central to the Trust's duty of care.

The Trust ensures that:

- Personal and sensitive data is stored within secure, centrally managed systems
- Access to data is restricted to authorised users with a legitimate need
- Audit trails and activity monitoring are maintained within core systems
- Secure sharing mechanisms are used for Trust documentation and collaboration
- Staff do not store Trust data on personal devices, personal email accounts or unapproved cloud platforms
- Removable media are used only where absolutely necessary and with appropriate encryption

Where a cyber incident involves or may involve a personal data breach, it will be managed in accordance with the Trust's Data Protection Policy and reported to the Data Protection Officer. Where the threshold is met, notification to the Information Commissioner's Office will follow within the statutory timeframe.

8. Cyber Security Awareness and Training

Staff awareness is one of the most effective defences against cyber threats. The Trust maintains a comprehensive programme of training and awareness designed to ensure that all staff understand the risks and their individual responsibilities.

- **Annual Training**

All staff are required to complete cyber security awareness training annually. The Trust delivers this through its compliance and training platform (iAMCompliant), which covers topics including:

- Identifying phishing emails and social engineering attempts
- Safe handling of email, attachments and links
- Password security and authentication
- Data protection and secure use of Trust systems
- Reporting cyber incidents and suspicious activity

Completion records are maintained at school level and monitored centrally. Staff who do not complete training within the required timeframe will be followed up through their Principal.

- **National Cyber Security Awareness**

In addition to internal training, the Trust promotes participation in nationally recognised cyber awareness programmes, including the National Cyber Security Centre (NCSC) training modules. These provide an additional layer of knowledge and reinforce sector-wide best practice.

- **Ongoing Communications and Guidance**

Cyber security awareness is reinforced throughout the year through regular communications issued to all staff and governors. These include guidance on current threats, reminders about phishing, password security and safe digital practices, and updates following any relevant incidents or sector alerts.

- **Phishing Simulation**

The Trust undertakes simulated phishing exercises to test staff awareness and measure organisational resilience in realistic conditions. Results are reviewed by the Risk Working Party and used to inform future training priorities.

Staff who interact inappropriately with simulated phishing emails receive targeted follow-up support and guidance.

9. Acceptable Use of Trust Systems

All users of Trust digital systems are expected to:

- Use their individual Trust account for all Trust-related communication and work
- Not use personal email accounts or unapproved platforms for Trust business
- Log out of Trust systems when using shared or public devices
- Report any loss or theft of devices that have access to Trust systems
- Not install unauthorised software on Trust-managed devices
- Follow any Acceptable Use Policy in force at their school or within the Trust

The Trust reserves the right to monitor usage of Trust systems in accordance with its policies and legal obligations.

10. Cyber Incident Reporting and Response

A cyber incident is any event which compromises or threatens the confidentiality, integrity or availability of Trust systems, data or digital services.

- **Examples of Cyber Incidents**

- Phishing attacks or social engineering attempts

- Unauthorised access to systems or accounts
- Malware, ransomware or virus infection
- Compromised user credentials
- Data loss, leakage or unauthorised disclosure resulting from a cyber event
- Denial of service or system outages caused by malicious activity

- **Reporting**

All staff must report suspected or actual cyber incidents immediately. Reports should be made to:

- Their school Principal or line manager
- The Trust IT support team at itsupport@2itsystems.co.uk
- The CEO or central team where the incident is serious or involves a potential data breach

Speed of reporting is critical. Early notification enables the Trust and its IT provider to contain threats and minimise impact.

- **Response and Escalation**

On receipt of a report, the Trust's IT provider will assess and contain the incident. The CEO will be notified of any significant incident and will determine whether escalation is required to the Chair of the Board, the FAR Committee or external authorities.

Where a cyber incident involves a potential personal data breach, the Trust's Data Protection Officer will be informed and the incident will be managed in accordance with the Trust's data breach procedures.

Where required, notification will be made to:

- The Information Commissioner's Office (if a reportable personal data breach)
- Action Fraud (the national reporting centre for fraud and cyber crime)
- The Department for Education (where the incident meets reporting thresholds)
- Insurers and legal advisors as appropriate

- **Post-Incident Review**

Following any significant cyber incident, a post-incident review will be conducted to identify root causes, assess the effectiveness of the response and determine what improvements are needed. Lessons learned will be reported through the Risk Working Party and the FAR Committee.

11. Business Continuity and Recovery

The Trust's cloud-based infrastructure provides inherent resilience through geographic redundancy, automatic backup and high availability features within the Microsoft 365 environment.

In the event of a significant disruption to digital systems, the Trust will work with its IT provider to restore services as quickly as possible. Priority will be given to safeguarding systems, pupil data and communications with families.

The Trust will continue to develop its business continuity arrangements in respect of cyber events as part of its wider resilience planning.

12. Third-Party and Supplier Management

The Trust works with external IT providers and software suppliers to deliver and maintain its digital infrastructure. The Trust retains strategic oversight and accountability for cyber security even where operational delivery is outsourced.

The Trust expects its IT provider and other technology suppliers to:

- Maintain appropriate security certifications and standards
- Provide regular security reports and updates
- Notify the Trust promptly of any incident or vulnerability affecting Trust systems
- Support the Trust in meeting its obligations under data protection legislation
- Comply with any security requirements specified in contracts or service level agreements

13. Monitoring and Continuous Improvement

Cyber threats evolve rapidly. The Trust is committed to continuously reviewing and improving its cyber security posture.

This is achieved through:

- Regular reporting from the IT provider on system security, vulnerabilities and incidents
- Governance oversight through the Risk Working Party and FAR Committee
- Annual review of staff training completion and phishing simulation outcomes
- Monitoring of sector guidance and alerts from the DfE, NCSC and other bodies
- Internal scrutiny reviews and any recommendations arising from audit activity
- School-level cyber updates and incident reporting

Findings from monitoring, audit and review activity will inform ongoing improvements to policy, systems and practice.