DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

ST PETER'S
Church of England Primary Academy Mansfield

SNMAT

GDPR & Records Management

Information Security Policy

MARK HARDISTY & SARAH PERRY

Policy:	GDPR & Records Management – Information Security Policy
Prepared for:	Chief Executive Officer, Board of Directors
Approved by:	SNMAT Board of Directors
Date:	July 2026
Review Cycle:	Annually

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2026	04/2026	MJH – Trust IT Manager SKP – Data Protection Officer	Initial version.
2026.5	05/2026	MJH	Added Microsoft 365 sharing default expiry on links.

EXECUTIVE SUMMARY

The Diocese of Southwell and Nottingham Multi-Academy Trust's (SNMAT, the MAT or The Trust) infrastructure and digital resources are essential to the operation, support and delivery of education, but also present risks to data protection, online safety and safeguarding.

We are committed to using IT in an ethical, transparent and manner and are committed to understanding, identifying and mitigating information security risks we face.

LEGAL FRAMEWORK

This policy aligns with the following:

- Computer Misuse Act 1990
- General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018
- Keeping Children Safe in Education (2025)
- Department for Education Digital and Technology Standards in Schools and Colleges (2026)

AIMS & OBJECTIVES

The aim of this policy is to:

- Provide a positive culture and foundation for information security across the Trust.
- Ensure users of SNMAT IT are aware of their legal obligations with data protection
- Encourage consistent and professional practice in the use of IT.
- Build a foundation of information security to ensure the Trust's safeguarding obligation by protecting confidential data held about learners and staff.

Our objectives are that:

- All systems and data should be accessible only to those who have a need to access them in accordance with their role, or in cooperation with the Trust.
- All systems and data should be available, within the bounds of data protection.
- The Trust will take all measures possible to mitigate information security risks.
- The Trust will continuously improve its security culture to ensure our aims are met as the risk and threat landscape changes over time.

SCOPE

This policy applies to:

Any individual that carries out an employee-like role in the Trust and has need to access any Trust system or work with Trust data. This includes all contracted employees, pupils and students and depending on exact working practices, may include:

- Board of Director members
- Local Governing Body Members
- Trustees
- Exam Invigilators
- Contractors or Third-Party Organisations
- Volunteers

OBLIGATIONS

Every member of the SNMAT community, staff, student have a responsibility to ensure that data is collected, accesses, stored and handled appropriately and lawfully.

Although the Trust is responsible for ensuring the obligations of this policy are met, unless otherwise stated, these obligations may be met by academies on an individual basis.

ROLES & RESPONSIBILITIES

Every member of the SNMAT community, staff, student have a responsibility to ensure that data is collected, accesses, stored and handled appropriately and lawfully.

BOARD OF DIRECTORS

The Trust Board of Directors must ensure:

- MAT Executives are adequately managing information security risks.
- They challenge and assure the approach of the MAT is aligned with the legal framework set out in this policy.

TRUST CHIEF EXECUTIVE OFFICER

The Trust CEO must ensure:

- Ensure adequate resources are available centrally to manage security risk.
- They understand the Trust's security risk posture.
- The MAT Data Protection Officer is accountable for mitigating and reducing risk.

TRUST DATA PROTECTION OFFCER

The Trust DPO has responsibility for:

- The senior ownership of information security risk.
- Setting Information Security Policies.
- Supports academies in improving their security posture.
- Holding academies to account for policy implementation.
- Ensuring the MAT Executive and Board are updated with emerging security risks.
- Liaising with Heads/Principles and the Trust IT Manager to ensure security risks are managed.

TRUST IT MANAGER

The Trust IT Manager is responsible for:

- Ensuring the Trust DPO is aware of emerging issues.
- Escalating any security issues to the Trust DPO.
- Overseeing Academy Security Policies where required.
- Supporting Academy IT Teams to implement any technical requirements of this policy.

LOCAL GOVERNING BODIES

The responsibility for ensuring that academies comply with the relevant Information Security Policies has been delegated to Local Governing Bodies.

THE PRINCIPAL/HEADTEACHER

Academy Principals/Headteachers are responsible for:

- Ensuring appropriate resources are available in the academy to support the reduction of risk.
- Ensuring staff and students have appropriate data security and awareness training.
- Understanding their academy's information security risk posture.
- Escalating information security issues to the Trust IT Manager and Data Protection Officer.
- Holding Academy IT Managers accountable for the technical aspects of this policy.
- Ensuring that risks are recorded and managed in their Academy-Level Risk Register.

SLT MEMBERS RESPONSIBLE FOR DIGITAL TECHNOLOGY

SLT Members Responsible for Digital Technology must ensure they:

- Collaborate with Academy IT Support Teams to assess and monitor the information security posture of the academy.
- Liaise with Academy Heads/Principles & IT Support Teams to deliver training.
- Escalate information security issues to Academy IT Support Teams.

ACADEMY IT MANAGERS / NETWORK MANAGERS

Academy IT Managers / Network Managers are responsible for:

- Implementing and maintaining the technical requirements of information security policy
- Working with Heads/Principals and SLT members to train, assess and mitigate risk.
- Ensuring those in scope follow the policy and that any breaches are reported.
- Where necessary escalating security issues to the Trust IT Manager or Trust DPO.
- Ensuring that risks are recorded and managed in their Academy-Level Risk Register.

STAFF

Staff have a duty to:

- Report potential security issues and data breaches to local IT support teams.
- Engage with any training and awareness materials.
- Meet their individual obligations within this, and linked policies.

PUPILS AND STUDENTS

Pupils and students have a duty to:

- Report any potential security issues and data breaches to staff.
- Engage with security awareness delivered through the curriculum.
- Meet their individual obligations with this and linked policies and procedures.

LINKS WITH OTHER POLICIES

The Information Security Policy must be read, understood and agreed in conjunction with other SNMAT policies:

- GDPR and Data Protection Policy
- Artificial Intelligence (AI) Guidance & Checklist
- Bring Your Own Device (BYOD) Policy
- Risk Management Strategy Framework
- Cyber Security Policy
- Financial Regulations Manual
- MFA Guidance

And the following individual Academy Policies and Plans:

- Cyber Recovery Plan
- Cyber Incident and Disaster Recovery Risks & Action Plan
- Cyber Awareness Plan

RISK MANAGEMENT

Information security risks shall be managed as **Operational** and **Compliance Risks** (Data Protection) in accordance with the Trust Risk Management Strategy framework.

Where certain categories of risk are identified, introduced, or not mitigated these are captured in the:

- MAT Consolidated Risk Register.
- Academy-Level Risk Register.

See **SNMAT Risk Management Strategy** framework.

RISK APPETITE

The Trust's information security risk appetite is managed. This means that the Trust aims to reduce its security risk posture by implementing measures to mitigate risks and is cautious when embarking on initiatives that introduce additional security risks to the organisation.

OPERATIONAL INFORMATION SECURITY RISKS

Where certain categories of risk are identified, introduced, or not mitigated these are captured in the:

- MAT Consolidated Risk Register.
- Academy-Level Risk Register.

DATA PROTECTION RISK ASSESSMENTS

Academies must carry out a **Data Protection Impact Assessment (DPIA)** where the use of any information system to process data is likely to result in a high risk to the rights and freedoms of individuals, in accordance with **UK GDPR Article 35**.

A DPIA **must be completed** before:

- Introducing new systems or technologies.
- Processing children's data in new ways.
- Implementing monitoring, tracking or profiling tools.
- Deploying Artificial Intelligence or automated decision-making.
- Sharing data with new third parties.

DPIAs **must** be:

- Completed prior to processing.
- Reviewed and signed off by the Trust Data Protection Officer.
- Retained as evidence of compliance and accountability.

Where a DPIA identifies residual high risk that cannot be mitigated, the Trust will consult the ICO where required.

SYSTEM ADOPTION AND ASSURANCE

All new digital systems, platforms, tools or services the process Trust data must not be adopted, piloted or deployed unless the requirements of this section are met.

SYSTEM APPROVAL

Before adoption, new system owners must:

- Have a clearly defined business purpose.
- Assess safeguarding implications.
- Ensure information security requirements can be met.

RISK AND ASSURANCE

New systems must undergo:

- Information security risks assessments
- Data Protection Impact Assessments (DPIAs)
- Supplier due diligence.

ASSET MANAGEMENT

See **SNMAT Financial Regulations Manual**.

DEVICE REGISTER

The Trust maintains a register of all devices provisioned and managed.

The following management systems act as Device Registration Repositories and record information such as manufacturer/model/operating system and automatically apply software and firmware updates.

- Microsoft Intune
- Google Workspace
- PDQ Inventory
- Apple School Manager

DEVICE PROVISIONING

Provision and management of devices are uniform at MAT and Secondary Academy level:

- Microsoft Intune
- Google Workspace
- Microsoft Deployment Toolkit
- Group Policy
- Apple School Manager

ACCESS CONTROL

Access to data must be granted on a least-privilege basis.

User account access and access privileges must satisfy the DfE core **Cyber Security** Digital and Technology standard for **Control and secure user accounts and access privileges**.

Account control relates to, but is not limited to the following:

- Microsoft 365 and Google Workspace
- Management information systems

- Financial information systems
- HR systems
- Cashless Catering systems
- Payroll systems
- Door and Security Camera systems
- Network management systems

IT ADMINISTRATORS & SERVICE ACCOUNTS

- An inventory of administrator accounts must be maintained and reviewed annually.
- To ensure administrator access to systems is available in an emergency, systems must be configured with at least two administrator accounts.
- An inventory of system or service accounts, used for system-to-system interaction, must be maintained, and reviewed annually.
- Any unused accounts must be disabled.

STAFF

- Staff accounts must be issued no earlier than their formally agreed start date, unless access to systems is required to complete mandatory pre-start training
- If a staff account is issued earlier for training purposes, steps must be taken to limit access to other systems and services until the formally agreed start date.
- Staff must not be given access to detailed learner data, or detailed data about other staff, prior to their formally agreed start date.
- Unless technically prohibitive, the management of staff accounts must be automated and based on an appropriate central data source managed by human resources or equivalent role.

PUPIL AND STUDENT ACCOUNTS

- All students must be issued with an account from their central identity directory.

SUPPLY ACCOUNTS

- Unless prohibitive supply accounts should be managed via academy's MIS and provisioned using those systems.
- Generic supply accounts can only be used at the discretion of the Principal/Headteacher.
- Supply accounts must not be given access to data that is not required for the role.
- Steps must be taken to limit access to other systems and services that are required for the role.
- Accounts should be issued for an agreed period and disabled as soon as possible.
- Supply accounts should be limited to accessing systems when not on physical school premises.

GUEST ACCOUNTS

- Guest accounts can only be used at the discretion of the Principal/Headteacher.
- Accounts are issued for an agreed time and disabled as soon as possible.
- Guest accounts should have the minimum access required for the user to perform their roles.
- Guest accounts should be limited to accessing systems when not on physical school premises.

MULTI-FACTOR AUTHENTICATION

Unless technically prohibitive, multi-factor authentication must be enabled, required, and enforced for all staff and students accessing any system.

If a system does not support enforceable multi-factor authentication, the system must be captured on either the MAT Consolidated Risk Register or Academy-Level Risk Register.

See **SNMAT MFA Guidance** and **MFA Guidance for SLT & Governors** documents.

DATA SECURITY

DATA SECURITY PRINCIPLES

In compliance with **UK GDPR Article 32**, the Trust will ensure:

- Confidentiality of personal data.
- Integrity of systems and data.
- Availability and resilience of processing systems.

Security measures must be proportionate to the risk, particularly where personal data or special category data is processed.

DATA ENCRYPTION

All data must be:

- Encrypted in transit, using secure protocols and methodologies.
- Encrypted at rest, using secure protocols and methodologies.
- Encrypted on laptop/mobile devices that are issued to staff or pupils.
- Secured with modern authentication methods, such as biometrics or PIN.

DATA RETENTION & DISPOSAL OF DATA

See **Data Protection Policy**.

BACKUPS

See **Cyber & Disaster Recovery Backup Strategy.**

TIME-LIMITED ACCESS TO SHARED INFORMATION

To align with **ISO 27001** access to organisational information shared via collaborative platforms (including Microsoft OneDrive, Google Drive or Microsoft SharePoint) must be granted on a time-limited basis.

- Access must be restricted to named individuals wherever possible.
- Shared links must be configured to expire.
- Access must be reviewed and removed when no longer required.

The following enforced expiration durations on high-risk links will be set:

- Anonymous or unrestricted links: 7 days.
- Organisation wide: 7 days.

The following recommended expiry durations on set on lower-risk links:

- Named individuals: 30 days.

Setting short default expiry dates significantly reduces the risk of unintended onward sharing and ensures access is time-limited, proportionate to risk, and aligned to the duration of the business need.

DATA CLASSIFICATION & HANDLING

Data Loss Prevention solutions or controls must be in place within systems that may be easily used to share or exfiltrate data, including email systems and others that allow arbitrary file sharing.

ARTIFICAL INTELLIGENCE

The Trust recognises that Artificial Intelligence (AI) and automated tools present both opportunities and risks, particularly where personal data and children's data are involved.

See **SNMAT Artificial Intelligence Guidance** and **SNMAT Artificial Intelligence Checklist**.

IT INFRASTRUCTURE

GENERAL PRINCIPLES

The following security principles apply to Trust IT Infrastructure:

- **Secure by default:** secure as possible when provisioned.
- **Defence in depth**: multi-layered approach to securing data and systems.
- **Good cyber hygiene:** unused systems and accounts are decommissioned and removed.
- **Cloud First strategy:** adopt software-as-a-service and cloud systems when possible.

NETWORK ARCHITECTURE

Network diagrams and other documentation relevant to network architecture and configuration must be maintained and reviewed annually.

All network switching must conform to the DfE core **Network Switching** Digital and Technology standard.

Connections to networks must be limited to known managed devices. A dedicated personal-device network must adhere to configuration set out in the Trust's **Bring Your Own Device Policy**.

INTERNET BOUNDARIES & FIREWALLS

All networks must be secured with a correctly configured hardware boundary firewall and conform to the DfE core **Cyber Security** Digital and Technology standard for firewalls.

DEVICES

Must comply with all applicable requirements laid down in the DfE's **Laptops, desktops and tablets** Digital and Technology standard.

ANTI-MALWARE, ANTI-RANSOMWARE AND ANTI-VIRUS

All Microsoft servers and endpoints **must** have Sophos Intercept X Endpoint Detection and Response software installed and CryptoGuard configured.

Anti-virus, Anti-malware and Anti-Ransomware software must satisfy the DfE core **Cyber Security** Digital and Technology standard for **Anti-malware software**.

VULNERABILTY & PATCH MANAGAMENT

Unless technically prohibitive, vulnerability and patch management should follow National Cyber Security Centre guidance on **Keeping devices and software up to date**.

Vulnerability and patch management applies to servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, switches, security cameras, IaaS, PaaS, and SaaS.

Devices/Software security updates **must** be patched within 14 days if:

1. The vendor describes the vulnerability as "critical" or "high risk".
2. The vulnerability has a Common Vulnerability Scoring System (CVSS) rating of 7.0 or above.
3. The vendor hasn't disclosed the severity level.

Any other vulnerabilities should be patched within 30 days.

OUT OF SUPPORT SOFTWARE & SYSTEMS

If a system or software application no longer receives updates from the original vendor, then that system or software application should be decommissioned.

If the system or software application is unable to be decommissioned then steps should be taken to isolate the system from other systems and networks, and if possible, reduce the number of users accessing the system.

The choice to retain out of support systems must be captured on either the MAT Consolidated Risk Register or Academy-Level Risk Register.

DISPOSAL OF COMPUTING RESOURCES

See our **IT Acceptable Use Policy**.

PHYSICAL & ENVIRONMENTAL SECURITY

Building access and physical controls **must** protect areas where sensitive or confidential information is processed. Server access and access to network equipment, switches, telecoms and network access points is restricted to those staff with authorisation.

IT ACCEPTABLE USE

All users of SNMAT IT must read and agree to our **IT Acceptable Use Policy**.

CYBER SECURITY

See **Cyber Security Policy.**

INCIDENT MANAGEMENT

MAJOR INCIDENT AND RESPONSE PLANS

Cyber Recovery and Cyber Incident and Disaster Recovery Plans must be maintained in line with Risk Protection Arrangement (RPA) and the DfE core **Cyber Security** Digital and Technology standard for **Cyber Risk Assessment** and **Report Cyber Attacks**.

See individual academy **Cyber Recovery Plan** and **Cyber Incident and Disaster Recovery Risks and Action Plan.**

Where plans are not maintained this must be captured on either the MAT Consolidated Risk Register or Academy-Level Risk Register.

INCIDENT ESCALATION

Staff and students should report information security incidents by following the procedure set out in the **SNMAT Data Protection Policy**.

Suspected breaches involving sensitive information are considered **high-risk** and must be escalated to the Trust IT Manager and Data Protection Officer immediately.

Any personal data breach that is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within **72 hours** of awareness, in accordance with UK GDPR.

LOG MANAGEMENT & MONITORING

LOG MANAGEMENT

All systems must:

- Log security-relevant usage, operation and data transfer.
- Have logs detailed enough to investigate security incidents.
- Where possible, retain logs for at least 180 days.
- Standardise log timestamps to be GMT or UTC.

MONITORING AND ALERTING

All systems must:

- Be activity monitored and appropriate security alerts configured.
- Have monitoring and alerting cloud-based and centralised where possible.

TRAINING & AWARENESS

See individual academies **Cyber Awareness Plans** for cyber security training implementation.

STAFF

All staff must complete adequate training at least once per academic year:

1. Cyber awareness training.
2. Data handling and data protection.

STUDENTS & PUPILS

As part of the curriculum, academies must have a pupil/student **Cyber Security Awareness Programme** in place that contributes to their individual **Cyber Awareness Plan** and meets the DfE core **Cyber Security** Digital and Technology standard.

BREACHES OF POLICY

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Trust assets, or an event which is in breach of the security procedures and policies.

The Trust will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

Suspected misuse of the Trust's computer systems by a member of staff will be considered by the Senior

Leaders. In the case of an individual then the matter may be dealt with under the disciplinary process.