



DIOCESE OF SOUTHWELL
& NOTTINGHAM

MULTI ACADEMY TRUST

SNMAT

Cyber Recovery Plan

A template for SNMAT schools

Policy:	Cyber Recovery Plan – A template for SNMAT schools
Prepared For:	SNMAT Partner Schools
Approved by:	SNMAT Board of Directors
Date:	March 2026
Review Cycle:	Annual

Versions:			
VERSION	DATE	AUTHOR	CHANGES
2023	SEPT 2023	MJH – Trust IT Manager	Initial version.
2024	MAY 2024	MJH – Trust IT Manager	Updated with correct Job Descriptions. Updated Third-Party IT Support Provider list and contact information. Added Catering Systems. Updated IT Team response setups.
2025	APRIL 2025	MJH	Updated Recovery Teams.
2026	FEB 2026	MJH	Revised Summary. Revised GDPR warning. Added need to customise document. Added testing. Added Trust DSL. Removed Redstor. Revised MIS with Arbor. Updated & Reformatted Cyber Recovery Teams. Added Payroll System Info. Added Cyber Incident & Disaster Recovery – Risk and Action Plans and Cyber Incident & Disaster Recovery – Backup Strategy references. Backup strategy moved to accompanying document.

USAGE & CUSTOMISATION

Academy IT Support Teams should customise this plan to meet their own requirements and implement it as they see fit.

CONTENTS

USAGE & CUSTOMISATION.....	2
CONTENTS.....	3
EXECUTIVE SUMMARY.....	5
RATIONALE.....	5
SCOPE.....	5
CUSTOMISATION.....	5
GDPR.....	5
LINKING WITH OTHER POLICIES.....	5
REVIEW.....	5
CYBER RECOVERY TEAM.....	6
KEY CONTACTS.....	6
SERVER ACCESS.....	7
MANAGEMENT INFORMATION SYSTEM ACCESS.....	7
FINANCIAL INFORMATION SYSTEM ACCESS.....	7
CATERING SYSTEM ACCESS.....	7
SAFEGUARDING INFORMATION SYSTEM ACCESS.....	8
PAYROLL SYSTEM ACCESS.....	8
KEY DIGITAL DOCUMENTS.....	8
BACKUP STRATEGY.....	9
BACKUP STRATEGY – ON PREMISES SERVICES.....	9
BACKUP STRATEGY – ADDITIONAL SERVICES.....	9
KEY ROLES AND RESPONSIBILITIES.....	9
PREVENTATIVE STRATEGIES.....	10
CLOUD FIRST STRATEGY.....	10
IT SECURITY & DATA PROTECTION POLICIES.....	11
FIREWALL.....	11
PREVENTING MALWARE FROM BEING DELIVERED.....	11
PREVENT MALWARE FROM RUNNING ON DEVICES.....	11
NATIONAL CYBER SECURITY CENTRE EARLY WARNING.....	11
POLICE CYBER ALARM.....	12
ACCEPTABLE USE.....	12
COMMUNICATING THE PLAN.....	12
COMMUNICATION PLAN TEMPLATE.....	12
CYBER RECOVERY PLAN.....	13
INCIDENT RECOVERY EVENT RECORDING FORM.....	14
Relevant Referrals.....	14
Actions Log.....	14
CRITICAL DATA ASSETS.....	15
INCIDENT IMPACT ASSESSMENT.....	17

EXECUTIVE SUMMARY

This Cyber Recovery Plan is part of an overall digital security plan that the Trust IT Team and Academy IT Support Teams use to protect IT data and systems and restore school IT services after a disaster or cyber incident to an operational standard.

RATIONALE

This document ensures that in the event of a cyber-attack, school staff and all stakeholders will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

SCOPE

The plan covers all essential and critical IT infrastructure, contacts, systems and networks. The template ensures that communications can be quickly established whilst recovering and restoring systems.

CUSTOMISATION

Academies should customise this plan with key information pertaining to their schools.

GDPR

This plan should not be publicly published due to the risk of a data breach.

LINKING WITH OTHER POLICIES

The Cyber Recovery Plan must be read in conjunction with the other following policies:

- Cyber Security Policy
- Cyber Incident & Disaster Recovery – Risk and Action Plans
- Cyber Incident & Disaster Recovery – Backup Strategy
- IT Policy
- Bring Your Own Device (BYOD) Policy
- Data Protection Policy

REVIEW

The application and outcomes of this policy will be monitored and reviewed annually to ensure it is working effectively.

The Plan will be kept up-to-date and reviewed with any change to information such as personnel, contact information, suppliers or key details that would affect the policy.

CYBER RECOVERY TEAM

SNMAT Trust IT Team

	Name	Role	Contact Details
Team Lead	Mark Hardisty	Trust IT Manager	
	David Price	Trust Assistant Manager	

SNMAT Executive Team

	Name	Role	Contact Details
	Chris Moodie	CEO	
	Sarah Perry	Business Director	
	James Clark	Estates Manager	

Academy IT Support Teams

	Name	Role	Contact Details
SCA Team Lead	Andrew Kirkland	Network Manager	
MAG Team Lead	Jon Gillum	Senior IT Engineer	
WGSA	Chris Herrick	IT Engineer	
SCA	Lewis Bentley	IT Engineer	

IT Support Providers

	Name	Role	Contact Details
Restore & Recovery	Jasmine IT		helpdesk@jasmineit.co.uk
	Orchestrate IT		support@orchestrateit.co.uk
	Atom IT		support@atomit.co.uk
	900 IT		shaun.beverley@ninehundred.co.uk

NCSC assured Cyber Incident Response Partners

<https://www.ncsc.gov.uk/schemes/cyber-incident-response>

Local School

	Name	Role	Contact Details
Site Security			
Media & PR			
Communications			
Staff Liaison			
Resources			
Facilities Management			

KEY CONTACTS

Supplier	Name & Contact Information	Account or another Reference
Internet		
Backups		
Telecoms		
Website Host		
Site Utilities		
Security Cameras		
Burglar Alarm		
Parent Comms & SMS		

Action Fraud		
Local Constabulary		
Legal Representative		

SERVER ACCESS

ON PREMISES

Role	Name	Contact Details
Head/Principal		
Business Manager		
IT Support Engineer		
Third Party IT Support		

MICROSOFT 365 AND G-SUITE TENENTS

Role	Name	Contact Details
Trust IT Team	Mark Hardisty	
Trust IT Team	David Price	
SCA IT Team	Andrew Kirkland	
MAG IT Team	Jon Gillum	
WGSA IT Team	Chris Herrick	
SCA IT Team	Lewis Bentley	
Third Party IT Support	Jasmine IT	
	Orchestrate IT	
	Atom IT	
	900 IT	

MANAGEMENT INFORMATION SYSTEM ACCESS

	Name	Contact Details
Trust IT Team	Mark Hardisty	
Trust IT Team	David Price	
Head/Principal		
Business Manager		
MIS Provider		
Data Manager		

FINANCIAL INFORMATION SYSTEM ACCESS

	Name	Contact Details
Trust Business Directorate	Sarah Perry	
Trust Business Directorate	Kellyanne Harkness	
Head/Principal		
Business Manager		
FIS Provider		

CATERING SYSTEM ACCESS

	Name	Contact Details
Trust IT Team	Mark Hardisty	
Trust Business Directorate	Kellyanne Harkness	
Business Manager		

Catering Manager		
Catering Provider		

SAFEGUARDING INFORMATION SYSTEM ACCESS

	Name	Contact Details
Trust Safeguarding Lead	Sam Dennis	
Head/Principal		
DSL		
Safeguarding Provider		

PAYROLL SYSTEM ACCESS

	Name	Contact Details
Trust Business Directorate	Jo Smith	
Head/Principal		
Finance Manager		

KEY DIGITAL DOCUMENTS

DIGITAL STORES

Abor and Bromcom MIS holds:

Central Register
Registers
Staff / Pupil Contact Details
Current Child Protection Concerns

SNMAT Safeguarding Microsoft Team holds:

Central Register

PSF Financials holds:

Finance, Purchasing and Ledgers.

CPOMS holds:

Safeguarding and Wellbeing information.

EduPay holds:

Payroll information.

CONTINGENCY ACCESS

In the event of a network outage, or cyber-attack in school, Abor and Bromcom MIS systems, PSF Financials, EduPay and CPOMS (and any other Saas cloud service) can be accessed by ransomware and virus scanned devices that are air-gapped, isolated from the affected network and can access the internet.

BACKUP STRATEGY

KEY ROLES AND RESPONSIBILITIES

Headteacher / Principal (with support from Deputy Head / Vice Principal)

- Seeks clarification from person notifying incident.
- Sets up and maintains an incident log, including dates / times and actions.
- Convenes the Cyber Recovery Team (CRT) to inform of incident and enact the plan.
- Liaises with the Chair of Governors.
- Liaises with the school Data Protection Officer.
- Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.
- Liaises with School Business Officer / Manager to contact parents, if required, as necessary

Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

Site Manager / Caretaker

- Ensures site access for external IT staff.
- Liaises with the Headteacher to ensure access is limited to essential personnel.

School Business Officer / Manager

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the standard response and knows who the media contact within school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical support staff
- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO)

- Supports the school, using the school data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Chair of Governors and determines if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

Chair of Governors

- Supports the Headteacher throughout the process and ensure decisions are based on sound judgement and relevant advice.
- Understands there may be a need to make additional funds available – have a process to approve this.
- Ensures all governors are aware of the situation and are advised not to comment to third parties / the media.
- Reviews the response after the incident to consider changes to working practices or school policy.

Academy IT Teams

- Liaises with the Trust IT Team for support.

- Secure backups and isolate from the network to contain the infection.
- Secure servers and endpoints and isolate from the network to contain the infection.
- Verifies the most recent and successful backup.
- Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged.
- Prioritises services and restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.
- Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase.
- Provides an estimate of any downtime and advises which systems are affected / unaffected.
- If necessary, arranges for access to the off-site backup.
- Protects any records which have not been affected.
- Ensures on-going access to unaffected records.

Teaching Staff and Teaching Assistants

- Reassures pupils, staying within agreed pupil standard response
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed.

PREVENTATIVE STRATEGIES

CLOUD FIRST STRATEGY

SNMAT's IT Strategic Target is to move all Academies to a Cloud First premise. Moving data and decommissioning on-premises servers into Microsoft 365 services reduces the potential for attack and takes advantage of OneDrive and SharePoint security features such as ransomware and data protection policies.

IT SECURITY & DATA PROTECTION POLICIES

Each Academy has standard policies that overlap and enhance the protection from cybercrime, including SNMAT IT Technical Guidelines, SNMAT Cyber Security Policy, a Cyber Incident & Disaster Recovery – Risk Assessment and Action Plan and a Cyber Incident & Disaster Recovery Backup & Recovery Strategy.

These policies can be provided locally, via a Third-Party IT Provider, or via the SNMAT IT Team.

FIREWALL

Each Academy has an edge firewall that bridges and protects their internal network from internet traffic and potential malicious actions.

Products used across the MAT are:

- EXA SurfProtect Quantum+
- FortiGuard FortiGate
- Sophos XGS Series
- Smoothwall

MULTI-FACTOR AUTHENTICATION

All SNMAT staff accounts are secured with MFA and geofenced to the UK for access.

ENPOINT PROTECTION

Software from leading providers is deployed to servers and end-user devices to prevent file-based malware attacks, detect malicious activity, and provide the ability to investigate and remediate any security incidents.

Products used across the MAT are:

- Microsoft Defender
- Sophos Intercept X

PREVENTING MALWARE FROM BEING DELIVERED

All SNMAT email accounts are protected with Microsoft's Exchange Online Protection policies that protect against spam and phishing attacks.

In addition, key stakeholder email accounts are protected with Defender for Office 365 – a cloud-based email filtering service that protects against malware, viruses and other harmful links.

PREVENT MALWARE FROM RUNNING ON DEVICES

In addition to Endpoint Protection, controls are in place on end-user devices to enhance security and prevent malware from running. Devices are managed either via controlled group policies when on-premises, or via cloud management services such as Google's G-Suite and Microsoft's Intune.

Policies control and prevent the running of unauthorised applications.

NATIONAL CYBER SECURITY CENTRE EARLY WARNING

SNMAT is a member of the NCSC's Early Warning system; a threat-notification service that informs about potentially suspicious activity on our networks.

POLICE CYBER ALARM

SNMAT is registered with the Police Cyber Alarm for our Primaries and Secondary Academies.

Secondaries have the Police Cyber Alarm software tool installed on the network that gathers data that can identify any malicious activity or assess if an attack has taken place.

PATCHING REGIME

SNMAT IT Teams and Third-Party IT Providers are advised to follow NCSC Cyber Essential Requirements guidance to ensure that critical and security patches are applied to all relevant devices within 14 days of release.

ACCEPTABLE USE

Every user of SNMAT IT is required to agree to an acceptable use policy that provides guidance and information on best practise and responsibilities.

COMMUNICATING THE PLAN

This plan should be communicated to all those who are likely to be affected and to all key staff to inform them of their roles and responsibilities in the event of an incident.

COMMUNICATION PLAN TEMPLATE

<https://www.rpaclaimforms.co.uk/membership-information-page/>

CYBER RECOVERY PLAN

1. Quickly evaluate and verify that the incident is genuine.
2. Contact the relevant IT Team for them to isolate devices from the network, disconnect from the internet, mitigate the attack and start the recovery process.
3. Record the incident into the Incident Recovery Event Recording Form.
4. Document the incident scope to identify in the Incident Impact Assessment table which key functions are operational, and which are affected.
5. To assist data recovery, if damage to a computer or backup material is suspected, staff should not:
 - Turn off electrical power.
 - Try to run any storage mechanism to retrieve data.
 - Tamper with, or move any damaged computers, or other device.
6. Contact the RPA Cyber Emergency Assistance Helpdesk via 0800 368 6378 or RPAresponse@cyberclan.com.
7. Convene the relevant Cyber Recovery Team.
8. Liaise with the relevant IT Team to estimate the recovery time and likely impact.
9. Liaise with the MAT Executive Team and Local Authority and decide as to the safety of the school remaining open. Evaluate alongside the ability to access to key documents referenced in this plan.
10. Identify any legal obligations and required statutory reporting – i.e., a criminal offence to the local police via Action Fraud, or via the Academy Data Protection Officer and a report to the Information Commissioner's Office in the event of a data breach.
11. Enact a communication plan. Communicate with parents/carers to the decision made above, to whether the school remains open or closed. Follow this with clear communication to staff and the media.
12. Constantly review and adjust recovery timescales, keeping all stakeholders informed of progress.
13. Upon completion of the process, evaluate the effectiveness of the Response Plan and review accordingly.
14. Educate employees on avoiding similar incidents in the future and implement any hardware, software or other infrastructure or training shortcomings from lessons learned.

INCIDENT RECOVERY EVENT RECORDING FORM

This form can be used to record all key events completed whilst following the stages of the Cyber Response Plan.

Description or reference of incident:	
Date of the incident:	
Date of the incident report:	
Date/time incident recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved?	

Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

Actions Log

Recovery Tasks (In order of completion)	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

CRITICAL DATA ASSETS

This is a list of data assets that schools require access to. The template should be amended to show which are critical and how long the school could function without access to each one. This could be recorded in hours, days, weeks, or months. A workaround could exist where data can be accessed via other methods, or services could be outsourced. It is useful to consider the costs of any additional resources that may be required.

Critical Activities	Data item required for service continuity	When Required?	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address		
	Minutes of SLT meetings and agendas		
	Head's reports to governors (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns		
	Attendance registers		
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Pupil Premium pupils and funding allocations		
Medical	Pastoral records and welfare information		
	Access to medical conditions information		
	Administration of Medicines Record		
Teaching	First Aid / Accident Logs		
	Schemes of work, lesson plans and objectives		
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
SEND Data	Pupil reports and parental communications		
	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
Conduct and Behaviour	IEPs / EHCPs / GRIPS		
	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
Assessment and Exams	Behavioural observations / staff notes and incident records		
	Exam entries and controlled assessments		
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
Governance	Exam results		
	School development plans		
	Policies and procedures		
	Governors meeting dates / calendar		
	Governor attendance and training records		
	Governors minutes and agendas		

Administration	Admissions information		
	School to school transfers		
	Transition information		
	Contact details of pupils and parents		
	Access to absence reporting systems		
	School diary of appointments / meetings		
	Pupil timetables		
	Letters to parents / newsletters		
	Extra-curricular activity timetable and contacts for providers		
Census records and statutory return data			
Human Resources	Payroll systems		
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision		
	Telecoms - school phones and access to answerphone messages		
	Email - access to school email systems		
	School website and any website chat functions / contact forms		
	Social media accounts (Facebook / Twitter)		
	Management Information System (MIS)		
	School text messaging system		
	School payments system (for parents)		
	Financial Management System - access for orders / purchases		
Site Management	Visitor sign in / sign out		
	CCTV access		
	Site maps		
	Maintenance logs, including legionella and fire records		
	Risk assessments and risk management systems		
	COSHH register and asbestos register		
Catering	Contact information for catering staff		
	Supplier contact details		
	Payment records for food & drink		
	Special dietary requirements / allergies		
	Stock taking and orders		

INCIDENT IMPACT ASSESSMENT

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	No Impact	There is no noticeable impact on the school's ability to function.
	Minor Impact	There is some loss in the ability to function which is minor. Functions can be carried out, but may take longer and there is a loss of efficiency.
	Medium Impact	The school has lost the ability to provide some critical services (administration or teaching and learning) to some users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
	High Impact	The school can no longer provide any critical services to users. It is likely the school will close or disruption will be considerable.
Informational	No Breach	No information has been accessed / compromised or lost.
	Data Breach	Access or loss of data which is not linked to individuals and classed as personal. This may include school action plans, lesson planning, policies and meeting notes.
	Personal Data Breach	Sensitive personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the person / people concerned requires a report to the ICO within 72 hours.
	Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. (This also includes corruption of data)
Restoration	Existing Resources	Recovery can be promptly facilitated with the resources which are readily available to the school.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.