DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

ST PETER'S
Church of England Primary Academy Mansfield

SNMAT

Cyber Recovery Plan

St Peter's C of E Primary Academy

Policy:	Cyber Recovery Plan – A template for SNMAT schools
Approved by:	Board of Directors
Date:	July 2024
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.

CONTENTS

EXECUTIVE SUMMARY

This cyber response plan is part of an overall digital security plan that schools use to maintain a minimum level of functionality to safeguard pupils and staff and to restore the schools IT systems back 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 template and plan as they see fit.

GDPR

This plan should not be published with contact or backup details included due to the risk of a data breach.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
- ICT 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	IT Manager	01636 557390 / mhardisty@snmat.org.uk
	David Price	Technical Lead	01636 557390 / dprice@snmat.org.uk
	Andrew Kirkland	Network Manager	
	Jon Gillum	Senior IT Engineer	
	Chris Herrick	IT Engineer	
	Lewis Bentley	IT Engineer	

SNMAT Executive Team

	Name	Role	Contact Details
	Chris Moodie	CEO	01636 557390 / cmoodie@snmat.org.uk
	Jo Saville	Director of Operations	01636 557390 / jsaville@snmat.org.uk
	Sarah Perry	Business Director	01636 557390 / sperry@snmat.org.uk
	James Clark	Estates Manager	01636 557390 / jclark@snmat.org.uk

IT Support Providers

	Name	Role	Contact Details
Restore & Recovery	Jasmine IT	IT Contractor	helpdesk@jasmineit.co.uk
	Scholar Tech		info@scholartech.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	James Marshall Russ Goodall	Head Teacher Site Manager	01623 489980 / jmarshall@stpeters.snmat.org.uk 01623 489980 / rgoodall@stpeters.snmat.org.uk
Media & PR	Louise Brimble	PR Consultant	07808596244 / lbrimble@snmat.org.uk
Communications	Louise Joynt	Office Manager	01623 489980 / ljoynt@stpeters.snmat.org.uk
Staff Liaison	James Marshall	Head Teacher	01623 489980 / jmarshall@stpeters.snmat.org.uk
Resources	Louise Joynt	Office Manager	01623 489980 / ljoynt@stpeters.snmat.org.uk
Facilities Management	Russ	Site Manager	01623 489980 / rgoodall@stpeters.snmat.org.uk

KEY CONTACTS

Supplier	Name & Contact Information	Account or another Reference
Internet	Virgin Media (through Jasmine IT as Managers)	
Backups		
Telecoms	One2Call - 0114 2300080	
Website Host	Primary Site – 01636 616630	ID Number: 1518
Site Utilities		
Burglar Alarm	Chubb – 0344 8791755	A/C number: 51722585
Parent Comms & SMS	ScholarPack – 01522 716049	ID Number: 8912028
Action Fraud		
Local Constabulary	Nottinghamshire Police – Sgt Neil Priestley	neil.priestley@notts.police.uk
Legal Representative		

SERVER ACCESS

ON PREMISES

Role	Name	Contact Details
Head/Principal	James Marshall	01623 489980 / jmarshall@stpeters.snmat.org.uk
Office Manager	Louise Joynt	01623 489980 / ljoynt@stpeters.snmat.org.uk
IT Support Engineer	Mark Hardisty	01636 557390 / mhardisty@snmat.org.uk
Third Party IT Support	Sam Taylor / Jasmine IT	samtaylor@jasmineit.org.uk / 07841294208

MICROSOFT 365 AND G-SUITE TENENTS

Role	Name	Contact Details
Trust IT Team	Mark Hardisty	01636 557390 / mhardisty@snmat.org.uk
Trust IT Team	David Price	01636 557390 / dprice@snmat.org.uk
Third Party IT Support	Jasmine IT	samtaylor@jasmineit.org.uk / 07841294208

MANAGEMENT INFORMATION SYSTEM ACCESS

	Name	Contact Details
Trust IT Team	Mark Hardisty	01636 557390 / mhardisty@snmat.org.uk
Trust IT Team	David Price	01636 557390 / dprice@snmat.org.uk

Head/Principal	James Marshall	01623 489980 / jmarshall@stpeters.snmat.org.uk
Office Manager	Louise Joynt	01623 489980 / ljoynt@stpeters.snmat.org.uk
MIS Provider	ScholarPack	01522 716049 / ID Number: 8912028
Data Manager	Sarah Perry	01636 557390 / sperry@snmat.org.uk

FINANCIAL INFORMATION SYSTEM ACCESS

	Name	Contact Details
Trust Business Directorate	Sarah Perry	01636 557390 / sperry@snmat.org.uk
Trust Business Directorate	Kellyanne Harkness	01636 557390 / kharkness@snmat.org.uk
Head/Principal	James Marshall	01623 489980 / jmarshall@stpeters.snmat.org.uk
Office Manager	Louise Joynt	01623 489980 / ljoynt@stpeters.snmat.org.uk
FIS Provider	PSF Financials	

CATERING SYSTEM ACCESS

	Name	Contact Details
Trust IT Team	Mark Hardisty	01636 557390 / mhardisty@snmat.org.uk
Trust Business Directorate	Kellyanne Harkness	01636 557390 / kharkness@snmat.org.uk
Office Manager	Louise Joynt	01623 489980 / ljoynt@stpeters.snmat.org.uk
Catering Manager	Louise Ingleby	01158 040043 / Louise.Ingleby@nottscc.gov.uk
Catering Provider	Nottinghamshire County Council	

SAFEGUARDING INFORMATION SYSTEM ACESSS

	Name	Contact Details
Head/Principal	James Marshall	01623 489980 / jmarshall@stpeters.snmat.org.uk
DSL	James Marshall	01623 489980 / jmarshall@stpeters.snmat.org.uk
Safeguarding Provider	CPOMS	01756 797766

KEY DIGITAL DOCUMENTS

DIGITAL STORES

ScholarPack and Bromcom MIS holds:

Central Register
Registers
Staff / Pupil Contact Details

Current Child Protection Concerns

PSF Financials holds:

Finance, Purchasing and Ledgers

CPOMS holds:

Safeguarding and Wellbeing information

ACCESS

In the event of a network outrage, or cyber-attack in school, ScholarPack and Bromcom MIS systems, PSF Financials and CPOMS 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 – CLOUD SERVICES

The SNMAT IT Team and Third-Party IT Providers have been instructed to follow National Cyber Security Centre and DfE guidance for backups, ensuring that schools must maintain 3 backup copies of important data on 2 separate devices.

Data	Location	Frequency
Microsoft 365	Redstor, Synology – Cloud & Off-Site	Daily
G-Suite	Synology – Off-Site	Daily
MIS & SIS	ScholarPack – Amazon RDS SaaS	To The Minute
MIS & SIS	Bromcom – Azure UK South & UK West	6 Hour Backups
Finance	PSF Financials – Cloud	To The Minute
eSafeguarding	CPOMS – ISO27001	To The Minute

BACKUP STRATEGY – ON PREMISES SERVICES

Data	Location	Frequency
File Servers	SNMAT Cloud Archive, Redstor – Off-site	Daily
File Servers	Veeam	Daily
SIMS	Veeam	Daily
DCs	Redstor & Veeam	Daily
Catering	Veeam	Daily

BACKUP STRATEGY – ADDITIONAL SERVICES

Data	Location	Frequency
File Server	Redstor – Off-site	Daily
Facilities Management	Veeam	Weekly

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.

IT Teams

- Secure backups and isolate form 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 from September 2023. Moving data from on-premises servers into Microsoft 365 services 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 Disaster Recovery Policy and a Backup & Recovery Plan.

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,
- FortiGuard
- Sophos
- 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 identity 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 identity 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 Commisioner'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		
	Pastoral records and welfare information		
Medical	Access to medical conditions information		
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	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		
	Pupil reports and parental communications		
SEND Data	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		
Assessment and Exams	Exam entries and controlled assessments		
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
	Exam results		
Governance	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.