Department for Education

Risk Protection Arrangement
Cyber Response Plan

[Moorgate Primary Academy]

[#1]

Last Reviewed	02-10-2024
Reviewed By	Jon Williams + Kate Bennett
Next Review Date	Autumn 2025
Date of Issue	02-10-2024
Approved By	Hope Brooks
Location of Document Copies	The Academy Sharepoint
Person Responsible for Next Review	Kate Bennett

Contents

1. Introduction

A Cyber Response Plan should be considered as part of an overall continuity plan that schools need to ensure they maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

If a school fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.

Incidents may occur during the school day or out of hours. The Cyber Response Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.

The plan should cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating cyber recovery. It is also important that the plan is well communicated and readily available.

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

This document is to be used in conjunction with the Business Continuity Plan if required.

2. Aims of a Cyber Response Plan

When developing a Cyber Response Plan, you will need to consider who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long you would be able to function without each one, establish plans for internal and external communications and have thought about how you would access registers and staff and pupil contact details. This will allow the school:

- To ensure immediate and appropriate action is taken in the event of an IT incident.
- To enable prompt internal reporting and recording of incidents.
- To have immediate access to all relevant contact details (including backup services and IT technical support staff).
- To maintain the welfare of pupils and staff.
- To minimise disruption to the functioning of the school.
- To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.
- To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.

3. Risk Protection Arrangement Cover

The Risk Protection Arrangement (RPA) now includes cover for Cyber Incidents, which is defined in the RPA Membership Rules as:

"Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data."

RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, you must contact the RPA Emergency Assistance.

If you require urgent assistance, please call 0800 368 6378 or email: RPAresponse@cyberclan.com

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

1. **Have offline backups**. Help and guidance on backing up is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog Offline backups in an online world - NCSC.GOV.UK

   It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups.

   Academies should ask their IT teams or external IT providers to ensure the following:

   a) Backing up the right data. Ensuring the right data is backed up is paramount. A suggested list of critical data is included in this Cyber Response Plan template.

   b) Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

   c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

   Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK

2. **All Employees and Governors (including LAC members) who have access to the Academy's information technology system must undertake NCSC Cyber Security Training**. It is available as a 36 minute video that can be distributed to all staff to watch individually when they have time. There is a link to the certificate in the video description which should be downloaded to show that training has been completed. The content is also available as PowerPoint slides and can be watched by groups of staff as part of an INSET day. Completion can be recorded centrally for all staff on the compliance platforms that schools currently use to record mandatory training, such as safeguarding, as it provides an audit of completion. If the training is being delivered to a number of staff a register should be kept, which all staff attending sign against their name confirming they have undertaken the training. **In the event of a claim the Academy will be required to provide this evidence.**

3. **Register with Police CyberAlarm**. Registering will connect Members with their local police Cyber Protect team. In the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. Installation of the software tool is not a condition of cover as it is not yet possible for it to be installed for all settings.

4. **Have a Cyber Response Plan in place**. A template is available for you to use to draft a school-specific plan if you do not already have one. It can be downloaded from the RPA Information & Documents page on the TopMark Claims Management website, from the RPA members portal or by emailing RPA.DFE@education.gov.uk

For full terms and conditions of Cyber cover, please refer to the relevant Membership Rules on gov.uk.

4. Preparation and Additional Resources

Preventative Strategies

It is vital education providers regularly review their existing defences and take the necessary steps to protect their networks. In addition to the 4 conditions of cover detailed above, there are several suggested measures that schools can implement to help themselves to improve their IT security and mitigate the risk of a cyber-attack:

- Regularly review IT Security Policy and Data Protection Policy.
- Assess the school's current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.
- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
    - If external RDP connections are used, MFA must be used

  - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
  - Enable an account lockout policy for failed attempts
  - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Advice and guidance

- **The NCSC website has an extensive range of practical resources to help improve Cyber Security for Schools - NCSC.GOV.UK**

Acceptable Use

Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices.

Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

Communicate the Cyber Recovery Plan to all those who are likely to be affected and be sure to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

Testing and Review

During an incident there can be many actions to complete, and each step should be well thought out, cohesive, and ordered logically.

Train key staff members to feel confident following and implementing the plan. Review the plan regularly to ensure contact details are up-to-date and new systems have been included. NCSC have resources to test your incident response with an Exercise in a Box - NCSC.GOV.UK

Making Templates Readily Available

It is recommended that templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

5. Actions in the event of an incident

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

- In accordance with Section 6, enact your Cyber Recovery Plan
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
    - You will receive a guaranteed response within 15 minutes
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
- Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
- Contact SUAT
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112** in consultation with the DPO and data breach management plan
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

6. Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational / which are affected.
3. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
4. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not:**
    - Turn off electrical power to any computer.
    - Try to run any hard drive, back up disc or tape to try to retrieve data.
    - Tamper with or move damaged computers, discs or tapes.
5. Contact RPA Emergency Assistance Helpline.
6. Start the Actions Log to record recovery steps and monitor progress.
7. Convene the Cyber Recovery Team (CRT).
8. Liaise with IT staff to estimate the recovery time and likely impact.
9. Make a decision as to the safety of the school remaining open.
    - *This will be in liaison with the Trust*
10. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the Data Protection Officer and the police*
11. Execute the communication strategy which should include a media / press release if applicable.
    - *Communications with staff, governors/LAC and parents / pupils should follow in that order, prior to the media release.*
12. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
13. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.
14. Educate employees on avoiding similar incidents / implement lessons learned.
15. Undertake actions to develop system resilience and cyber security measures.

Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.

Cyber Response and Recovery Plan

Staff should be made aware not to share this plan with members of the public or leave it unattended, as the plan will contain confidential information. Staff must also be vigilant about who can access this plan, as the plan has the potential to be used with malicious intent, e.g. cyber attacks.

Cyber Recovery Team

In the event of this plan having to be initiated, the personnel named below will form the Cyber Recovery Team and take control of the following:

	Name	Role	Contact Details
Recovery Team Leader	Jon Williams	Exec HT	headteacher@moorgateacademy.co.uk
Data Management	Kate Bennett	Office Manager	Admin1@moorgateacademy.co.uk
IT Restore / Recover	Staffs Tech	ICT Support company	support@staffs-tech.co.u
Site Security	Scott Cartwright	Site Supervisor	s.cartwright@moorgateacademy.co.uk
Public Relations	Jon Williams	Exec HT	headteacher@moorgateacademy.co.uk
Communications	Jon Williams	Exec HT	headteacher@moorgateacademy.co.uk
Resources / Supplies	Kate Bennett	Office Manager	Admin1@moorgateacademy.co.uk
Facilities Management	Scott Cartwright	Site Supervisor	s.cartwright@moorgateacademy.co.uk
Finance	Kate Bennett	Office Manager	Admin1@moorgateacademy.co.uk
SUAT	James Capper	SUAT CEO	JCapper@suatrust.co.uk
SUAT	Sam Ashley	SUAT Deputy CEO/DLSI	SAshley@suatrust.co.uk
SUAT	Liz Allen	SUAT Deputy CEO/Finance Director	LAllen@suatrust.co.uk
SUAT	Hope Brooks	SUAT Operations Director/DPO	HBrooks@suatrust.co.uk

This procedure should not be published with contact details included due to the risk of a data breach. There is no requirement to publish this procedure online.

Server Access

Please detail all the people with administrative access to the server.

Role	Name	Contact Details
Headteacher	Jon Williams	headteacher@moorgateacademy.co.uk
Business / Office Manager	Kate Bennett	Admin1@moorgateacademy.co.uk
IT Support Technician	Jordan Bough	support@staffs-tech.co.uk
Third Party IT Provider	Staffs Tech	support@staffs-tech.co.uk

This procedure should not be published with contact details included due to the risk of a data breach. There is no requirement to publish this procedure online.

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Headteacher	Jon Williams	headteacher@moorgateacademy.co.uk
Office/Business Manager	Kate Bennett	Admin1@moorgateacademy.co.uk
MIS Provider	Bromcom	020 8290 7177
Data Manager	Staffs Tech	support@staffs-tech.co.uk

This procedure should not be published with contact details included due to the risk of a data breach.

In the event of a cyber incident, it will be helpful to consider how you would access the following:

- Registers
- Staff / Pupil contact details
- Current Child Protection Concerns
- Business continuity plan
- Risk management information
- Business critical information
- Any further critical information (please list)

Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	✓	Daily
School MIS	✓	Web based
Cloud Services	✓	Web based
Third Party Applications / Software	✓	Web based
Email Server	✓	
Curriculum Files	✓	Web based
Teaching Staff Devices	✓	Web based
Administration Files	✓	Web based

Finance / Purchasing	✓	Web based
HR / Personnel Records	✓	Web based
Inventory	✓	Web based
Facilities Management / Bookings		
Website	✓	Web based
USBs / portable drives (please note that it is not recommended that storage mediums of this nature are used).		

Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection / Service Provider	**Staffs Tech – 0330 016 5568**	
Backup Provider	**Staffs Tech – 0330 016 5568**	
Telecom Provider	**Telecom 150- 01889 220820**	T100031
Mobile Provider		
IT Support Provider	**Staffs Tech – 0330 016 5568**	
Website Host	**Plinkfizz**	01782 630777
Electricity Supplier	**Npower – 2623229W**	**08456729209**
Burglar Alarm	**Chubb Fire & Security – 52157998**	**03448791740**
Text Messaging System	**Teachers2parents**	**08453885515**
Action Fraud		
Local Constabulary	**Staffordshire Police**	
Legal Representative		
LA / Trust Press Officer	**Hope Brookes**	
RPA		
DfE Incident Helpline (8am – 4pm)	**0800 046 8687**	
Electricity Provider		
Academy Security Systems		
MIS Provider	**Bromcom**	
Local MP		

This procedure should not be published with contact details included due to the risk of a data breach. There is no requirement to publish this procedure online.

Staff Media Contact

Assigned staff will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications, in conjunction with and approval from SUAT.

The staff media contact should only provide verified facts. It is likely that verifying details will take some time and stating, “I don’t know at this stage”, is a perfectly acceptable response.

It is likely the following basic questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications **must not respond** to requests for information and should refer callers or media representatives to assigned staff.

Assigned Media Liaison(s):

Name: Jon Williams Role: Executive HT

Name: Vicki Eaglefield Role: Head of School

Key Roles and Responsibilities

Every Academy is unique and the structure and staffing levels will determine who will be assigned which task. This example will help you to assign roles and responsibilities, but this is not an exhaustive or a definitive list.

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 the LAC.
- ✓ Liaises with the Data Protection Officer.
- ✓ Convenes and informs staff, advising them to follow the ‘script’ when discussing the incident. Script to be prepared in conjunction with SUAT and media / communications advisers.
  Prepares relevant statements / letters for the media, parents / pupils.
- ✓ Liaises with 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.

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 / social media.
- ✓ Assesses whether payroll, finance or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO)

- ✓ Supports the school, using GDPRis / information asset register / data maps to consider whether data has been put at risk, is beyond reach, or lost.
- ✓ Liaises with the Headteacher / CEO and determines if a report to the ICO is necessary.
- ✓ Advises on the appropriateness of any plans for temporary access / systems.
- ✓ Supports investigations.
- ✓ Reviews the response after the incident to consider changes to relevant policies / practices.

Chair of the LAC and CEO

- ✓ 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 in accordance with the Scheme of Delegation.
- ✓ Ensures all LAC members 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 policy.

IT Lead / IT Staff

Depending upon whether the school has internal or outsourced IT provision, the roles for IT Co-ordinators and technical support staff will differ.

- ✓ 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, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss **(ensure that this support is included within IT Support SLAs).**
- ✓ 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.

Critical Activities - Data Assets

List all the data assets your school has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month.

Complete the required column with the timescale you believe is necessary for recovery. You may find it helpful to refer to your Inventory / Data Map.

Assign: 4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 3 weeks / 1 month.

Also decide if there are any temporary workarounds or if outsourcing is possible. It is useful to consider the cost of any additional resources which may be required in an emergency situation.

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)	Critical Information? (Yes / No)
Leadership and Management	Access to Headteacher's email address	**24 hrs**	yes	Yes
	Minutes of SLT meetings and agendas	**1 week**	No	No
	Head's reports to the LAC (past and present)	**1 month**	No	No
	Key stage, departmental and class information	**1 week**	No	No
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns	**4 hrs**	No	Yes
	Attendance registers	**24 hrs**	No	Yes
	Class groups / teaching groups, and staff timetables	**1 month**	No	No
	Referral information / outside agency / TAFs	**24 hrs**	No	Yes
	Child protection records	**4 hrs**	No	Yes
	Looked After Children (LAC) records / PEPs	**24 hrs**	No	Yes
	Pupil Premium pupils and funding allocations	**24 hrs**	No	Yes
	Pastoral records and welfare information	**24 hrs**	No	Yes
Medical	Access to medical conditions information, allergens – of staff and pupils	**4 hrs**	No	Yes
	Administration of Medicines Record	**4 hrs**	No	Yes
	First Aid / Accident Logs	**24 hrs**	No	Yes
Teaching	Schemes of work, lesson plans and objectives	**1 week**	yes	Yes
	Seating plans	**N/A**	N/A	N/A
	Teaching resources, such as worksheets	**24 hrs**	No	No
	Learning platform / online homework platform	**24 hrs**	No	No
	Curriculum learning apps and online resources	**24 hrs**	No	No
	CPD / staff training records	**1 week**	No	No
	Pupil reports and parental communications	**4 hrs**	No	Yes
SEND Data	SEND List and records of provision	**4 hrs**	No	Yes
	Accessibility tools	**24 hrs**	No	No
	Access arrangements and adjustments	**N/A**	N/A	N/A
	IEPs / EHCPs / GRIPS	**24 hrs**	No	No
Conduct and Behaviour	Reward system records, including house points or conduct points	**N/A**	N/A	N/A
	Behaviour system records, including negative behaviour points	**N/A**	N/A	N/A

	Sanctions	**N/A**	N/A	N/A
	Exclusion records, past and current	**24 hrs**	No	No
	Behavioural observations / staff notes and incident records	**24 hrs**	No	Yes
Assessment and Exams	Exam entries and controlled assessments	**24 hrs**	No	Yes
	Targets, assessment and tracking data	**4 hrs**	yes	Yes
	Baseline and prior attainment records	**4 hrs**	yes	Yes
	Exam timetables and cover provision	**4 hrs**	yes	Yes
	Exam results	**4 hrs**	yes	Yes
Governance	Academy development plans	**1 week**	yes	No
	Policies and procedures	**1 week**	yes	No
	Governors meeting dates / calendar	**1 week**	yes	No
	Governor attendance and training records	**1 week**	yes	No
	Governors minutes and agendas	**1 week**	yes	No
Administration	Admissions information	**24 hrs**	yes	Yes
	School to school transfers	**24 hrs**	yes	Yes
	Transition information	**N/A**	N/A	N/A
	Contact details of pupils and parents	**4 hrs**	yes	Yes
	Access to absence reporting systems	**24 hrs**	yes	Yes
	School diary of appointments / meetings	**N/A**	N/A	N/A
	Pupil timetables	**N/A**	N/A	N/A
	Letters to parents / newsletters	**1 week**	yes	No
	Extra-curricular activity timetable and contacts for providers	**N/A**	N/A	N/A
	Census records and statutory return data	**1 week**	yes	Yes
Human Resources	Payroll systems	**1 week**		
	HR files, staff attendance, absences, and reporting facilities	**1 week**		
	Disciplinary / grievance records	**1 week**		
	Staff timetables and any cover arrangements	**N/A**	N/A	N/A
	Contact details of staff	**1 week**		
Office Management	Photocopying / printing provision	**24 hrs**		
	Telecoms - school phones and access to answerphone messages	**4 hrs**		
	Email - access to school email systems	**4 hrs**		
	School website and any website chat functions / contact forms	**24 hrs**		
	Social media accounts (Facebook / Twitter)	**24 hrs**		
	Management Information System (MIS)	**24 hrs**		
	School text messaging system	**4 hrs**		
	School payments system (for parents)	**4 hrs**		
	Financial Management System - access for orders / purchases, Online Banking	**4 hrs**		
Site Management	Visitor sign in / sign out	**24 hrs**		
	CCTV access	**24 hrs**		
	Site maps	**N/A**	N/A	N/A
	Maintenance logs, including legionella and fire records	**1 week**		
	Risk assessments and risk management systems	**1 week**		
	COSHH register and asbestos register	**1 week**		
Catering	Contact information for catering staff / supplier contact information	**1 week**		

	Maintenance records, compliance and HACCP information	**1 week**		
	Payment records for food & drink	**24 hours**		
	Special dietary requirements / allergies	**4 hrs**		Yes
	Stock taking and orders	**N/A**	N/A	N/A

Back Up Strategy

Below is the back-up strategy. It shows where certain back-up information is held, who it is held by (including third party holders), the frequency that it is backed up, whether it is considered critical information, and an estimate for how long the school could manage without access to this information before the loss of access would cause disruption.

The risk of disruption to the usual route of access to this information and the risk of disruption to the back-up location of this information has been indicated using the following risk matrix:

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major**	High	High	Medium
	Severe	High	Medium	Low
	Minor	Medium	Low	Low

Information Type	Risk of Disruption	Back Up Type	Provider	Frequency	Location
Pupil attendance registers	Major	Server	Bromcom	Daily	Offsite
Admissions register	Major	Server	Bromcom	Daily	Offsite
Pupils' contact details	Major	Server	Bromcom	Daily	Offsite
Pupils' emergency contact details	Major	Server	Bromcom	Daily	Offsite
Current child protection concerns	Severe	Online cloud storage	My Concern	Daily	Offsite
Child protection concerns records	Severe	Online cloud storage	My Concern	Daily	offsite

Personnel records	Minor	Server	My View/Bromcom	Daily	Offsite
SCR	Major	Server	Online SCR	Daily	Offsite
Staff contact details	Minor	Server	Bromcom/My View	Daily	Offsite
Staff emergency contact details	Major	Server	Bromcom	Daily	Offsite
Information held on staff work devices	Severe	Server/ Online cloud storage	Microsoft One Drive/ Bromcom	Daily	Offsite
Main filer server	Severe	Server	Staffs Tech	Hourly	Offsite
Academy MIS	Severe	Server	Bromcom	Daily	Offsite
Cloud services	Major	Online cloud services	Staffs Tech	Daily	Offsite
Third-party software	Severe	Server	Teachers2Parents/ School Grid etc	Daily	Offsite
Email server	Severe	Server	Staffs Tech	Daily	Offsite
Curriculum information	Minor	Online cloud storage		Daily	Offsite
Administration files	Severe	Server	Bromcom/ My view/ DFE	Daily	Offsite
Financial information	Severe	Server	PSF/BPS/MyView/Online banking	Daily	Offsite
Purchasing information	Major	Server	PSF/Online banking	Daily	Offsite
Asset information	Minor	Server	Share drive	Daily	Offsite
Inventory	Minor	Server	Share drive	Daily	Offsite
Facilities management information	Minor	Server	Share drive	Daily	Offsite
Bookings and lettings information	Minor	Server	Share drive	Daily	Offsite
School website	Major	Server	Plinkfizz	Daily	Offsite
USBs and other portable storage devices	N/A	N/A	N/A	N/A	N/A

Testing Details

Cyber response and recovery plan	
Date plan was last tested	
Test approved by	
Date of next test	
Person responsible for next testing	
Back-up strategy	
Date back-up strategy was last tested	
Test approved by	
Date of next test	
Person responsible for next testing	

Appendix A: 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.
Inf or	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.

Appendix B: Communication Templates

1. School Open

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the school IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc] At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems]

We are in liaison with our school Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR. Every action has been taken to minimise disruption and data loss.

The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible.

In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. The school will remain open with the following changes [detail any changes required]

I appreciate that this will cause some problems for parents/carers with regards to school communications and apologise for any inconvenience.

We will continue to assess the situation and update parents/carers as necessary. [If possible, inform how you will update i.e. via website/text message]

Yours sincerely,

2. School Closure

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down the school IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc]. At present we have no indication of how long it will take to restore our systems.

We are in liaison with our school Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / GDPR.

In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff.

I feel that we have no option other than to close the school to students on [XXXXXXXXXX]. We are currently planning that the school will be open as normal on [XXXXXXXXXX]

I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience but feel that we have no option other than to take this course of action.

The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible.

We will continue to assess the situation and update parents / carers as necessary. [If possible, inform how you will update i.e. via website / text message].

Yours sincerely,

3. Staff Statement Open

The school detected a cyber-attack on [date] which has affected the following school IT systems:

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will remain open with the following changes to working practice:

(Detail any workarounds / changes)

The school is in contact with our Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, limit severity, and restore systems.

All staff are reminded that they must not make any comment or statement to the press, parents or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name]

4. Staff Statement Closed

The school detected a cyber-attack on [date] which has affected the following school IT systems:

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will close to pupils [on DATE or with immediate effect].

(Detail staff expectations and any workarounds / changes or remote learning provision)

The school is in contact with our Data Protection Officer, and we have reported the incident to the ICO, in line with the statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].

All staff are reminded that they must not make any comment or statement to the press, parents, or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name].

5. Media Statement

[Inset school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the [Trust / LA] the school [will remain open / is currently closed] to pupils.

The school is in contact with their Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities and the school has taken immediate remedial action to limit data loss and restore systems.

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the school in initial media responses.

Standard Response

The information provided should be factual and include the time and date of the incident.

Staff should not speculate how long systems will take to be restored but can provide an estimate if this has been agreed.

If no restoration date has been advised, staff should merely state that work is on-going and that services will resume as soon as practically possible.

Staff should direct further enquiries to an assigned contact / school website / other pre-determined communication route.

Standard Response for Pupils

For staff responding to pupil requests for information, responses should reassure concerned pupils that incidents are well prepared for, alternative arrangements are in place and that systems will be back online shortly.

Staff should address any outlandish or suggested versions of events by reiterating the facts and advising pupils that this has been confirmed in letters / emails to parents / carers.

Staff should not speculate or provide pupils with any timescales for recovery, unless the sharing of timescales has been authorised by senior staff.

Appendix C: 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?	
If not, what was not recovered and why?	

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.					

Reference number	Description of action	Tick when complete
1	Where required, e.g. during a cyber-attack, isolate all devices from the affected network.	
2	Assess whether electrical power to devices should remain on; however, **do not** turn off the power to a device if damage to the device or back-up material is suspected.	
3	Communicate to staff **not** to run any hard-drives, back-up discs, or try to retrieve data until instructed that it is safe to do so.	
4	Communicate to staff **not** to move or tamper with any devices or device components until instructed that it is safe to do so.	
5	Ensure the communication steps outlined in this plan have been followed before continuing.	
6	Begin recording your recovery steps and monitor recovery progress.	
7	Convene the cyber response team.	
8	Liaise with ICT staff to estimate the recovery time and likely impact.	
9	Assess the safety of the school and decide, with the advice of the trust whether the school can remain open.	
10	Where there has been a crime committed, ensure this has been reported the police.	
11	Where a data breach has occurred, ensure this has been reported to the ICO.	
12	Identify whether any other statutory reporting requirements are required and have been carried out.	
14	Ensure the following groups of stakeholders have been made aware of the incident, in the following order: 1. Staff 2. Governors 3. Parents and pupils	
15	Execute the media communication strategy, where required. Do not inform the media prior to informing your school's stakeholders.	
16	Assess the timescales needed for recovery and ensure stakeholders have been informed.	
17	Evaluate the effectiveness of the cyber response and recovery plan and ensure processes are put in place for it to be reviewed.	
18	Implement a 'lessons learnt' strategy to minimise the risk of the incident reoccurring.	

Appendix D: Post Incident Evaluation

Response Grades 1-5 1 = Poor, ineffective and slow / 5 = Efficient, well communicated and effective.

Action	Response Grading	Comments for Improvements / Amendments
Initial Incident Notification		
Enactment of the Action plan		
Co-ordination of the Cyber Recovery Team		
Communications Strategy - stakeholders		
Communications Strategy – external agencies		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved?		
Log any requirements for additional training and suggested changes to policy / procedure:		
What are the lessons learnt upon reflection of this incident?		