Department for Education

Risk Protection Arrangement Cyber Response Plan

Margaret McMillan Nursery School

Last Reviewed	October 2025
Reviewed By	Karen Smith
Next Review Date	October 2026

Based on a document produced by the Derbyshire County Council Education Data Hub. Additional cyber resilience resources for schools are available at Resources - Education Data Hub

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.

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 *e*xternal 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. Cyber Protection Arrangement

"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."

The following 4 considerations have been taken into account:

a. 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, the following steps should be undertaken:
   a) Backing up the right data. Ensuring the right data is backed up is paramount.
   b) Backups are held fully offline and not connected to systems or in cold storage.
   c) Backups are held both on and off site.
   d) Backups are tested appropriately, and regularly to ensure that services can be restored, and data recovered.

b. All Employees or Governors who have access to the School's information technology system must undertake NCSC Cyber Security Training . Upon completion, a certificate can be downloaded by each person.

c. Register with Police CyberAlarm. Registering will connect the school with their local police cyber protect team.be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. When registering, use the code "RPA Member" in the Signup code box.

d. Have a Cyber Response Plan in place.

4. Preparation and Additional Resources

Preventative Strategies

The school deems it vital to regularly review their existing defences and take the necessary steps to protect their networks. In addition to the 4 conditions detailed above, we implement the following:

- 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.
- 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.
- Routinely install security and system updates with a regular patching regime to ensure any internet-facing device is not susceptible to an exploit.
- 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.

Acceptable Use

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

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

We review the plan regularly. 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:

- Enact your Cyber Recovery Plan
- 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**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**
- 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

a. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
b. 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.
c. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
d. 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.

e. Start the Actions Log to record recovery steps and monitor progress.
f. Convene the Cyber Recovery Team (CRT).
g. Liaise with IT staff to estimate the recovery time and likely impact.
h. Make a decision as to the safety of the school remaining open.
- *This will be in liaison with relevant Local Authority Support Services / Trust*

i. 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 school's Data Protection Officer and the police*

j. Execute the communication strategy which should include a media / press release if applicable.
- *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*

k. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
l. 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.
m. Educate employees on avoiding similar incidents / implement lessons learned.

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

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 in School	Contact Details
Recovery Team Leader	Karen Smith	Headteacher	02072812745
Data Management	Connetix	IT Support	02038138702
IT Restore / Recover	Connetix	IT Support	02038138702
Site Security	Barry Turner and Son	Premises Management	07973669235
Public Relations	Karen Smith	Headteacher	02072812745
Communications	Karen Smith	Headteacher	02072812745
Resources / Supplies			
Facilities Management			

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

Server Access

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

Role	Name	Contact Details
Headteacher	Karen Smith	02072812745
Network Manager	Connetix	02038138702

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

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Headteacher	Karen Smith	
School Business Manager	Lisa Lee	
MIS Provider	ESS /LB Islington	

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, the following documents are held in paper form:

- Registers
- Staff / Pupil contact details
- Current Child Protection Concerns

Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	On-site	Daily, weekly, monthly
Main File Server	Off-site	weekly
School MIS	Managed by provider	
Cloud Services	On-site	Daily, weekly, monthly
Cloud Services	Off-site	weekly
Third Party Applications / Software	Managed by provider (Egress)	
Email Server	See cloud services	
Curriculum Files	See main file server	
Teaching Staff Devices	Not backed up	
Administration Files	See main file server	
Finance / Purchasing	Managed by provider	
HR / Personnel Records	See School MIS	
Inventory	See main file server	
Facilities Management / Bookings	See main file server	
Website	Off-site	Following changes

Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection	Plusnet (+44 800 432 0200)	Account name: margaretmcmillan
Telecom Provider	BT	
Website Host	ZEN (01706 902000)	Site ID: 98564
Electricity Supplier	SSE	
Burglar Alarm	Chubb	
Action Fraud		
Local Constabulary		
Legal Representative	Local Authority - LBI	
LA / Trust Press Officer	Local Authority - LBI	

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

Key Roles and Responsibilities

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

Headteacher / (with support from Deputy Head)

- 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

- 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.

Network manager

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 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

- 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)
Leadership and Management	Access to Headteacher's email address		**Y**
	Head's reports to governors (past and present)		
	Homebase 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		
	Teaching resources, such as worksheets		
	CPD / staff training records		
	Pupil reports and parental communications		
	SEND List and records of provision		
	Access arrangements and adjustments		
	STPs / EHCPs ?SEN profiles		
Conduct and Behaviour	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		
Assessment	Targets, assessment and tracking data		
	Two year and leavers' reports		
Governance	School development plans		
	Policies and procedures		
	Governors meeting dates / calendar		
	Governor attendance and training records		
	Governors minutes and agendas		
Administration	Admissions information		
	Transition information		
	Contact details of pupils and parents		
	Access to absence reporting systems		
	School diary of appointments / meetings		

	Letters to parents / newsletters		
	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		
	Management Information System (MIS)		
	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		
	Free school meals		
	Special dietary requirements / allergies		

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.

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.

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.

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.
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 **should not respond** to requests for information and should refer callers or media representatives to assigned staff. Assigned

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?	

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.					

Appendix D: Post Incident Evaluation

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

Action	Response Grading	Comments for Improvements / Amendments
Initial Incident Notification		
Enactment of the Action plan		
Co-ordination of the Cyber Recovery Team		
Communications Strategy		
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:		