



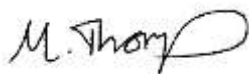
Pennine Academies Yorkshire

Cyber Response Plan

POLICY HISTORY

Version: V1
Date written: March 2024
Review date: September 2025
Ratified by: Executive Board September 2024

Approved by (signature):



Chief Executive Officer

Date issued: September 2024
Responsibility of: EXECUTIVE BOARD
Review period: Annual
Date to be reviewed: September 2025

KEY AMENDMENTS TO THIS POLICY

February 2024

This policy has been converted to the new Trust policy format and all links to legislation and guidance have been checked. There are no substantive changes to content.

CONTENTS

1. INTRODUCTION	4
2. AIMS OF A CYBER RESPONSE PLAN	4
3. ACTIONS IN THE EVENT OF AN INCIDENT	5
4. CYBER RECOVERY PLAN	5
5. CYBER RECOVERY TEAM	6
6. SERVER ACCESS	7
7. MANAGEMENT INFORMATION SYSTEM (MIS) ADMIN ACCESS	7
8. SCHOOL ACCESS CONSIDERATIONS	8
9. BACKUP STRATEGY	8
10. KEY CONTACTS	9
11. STAFF MEDIA CONTACTS	9
12. KEY ROLES AND RESPONSIBILITIES	10
Designated Safeguarding Lead (DSL)	10
Site Manager / Caretaker	10
School Operations Manager	10
Data Protection Officer (DPO)	11
Chief Executive Officer	11
IT Support company	11
Cyber Security Business Partner	11
Teaching Staff and Teaching Assistants	11
13. CRITICAL ACTIVITIES - DATA ASSETS	12
APPENDIX A: INCIDENT IMPACT ASSESSMENT	16
APPENDIX B: COMMUNICATION TEMPLATES	17
1. School Open	17
2. School Closure	18
3. Staff Statement Open	19
4. Staff Statement Closed	19
5. Media Statement	21
APPENDIX C: INCIDENT RECOVERY EVENT RECORDING FORM	22
APPENDIX D: POST INCIDENT EVALUATION	23

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 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. 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](#)
- Contact Endsleigh Cyber insurance - call back within 30 minutes
- Inform the National Cyber Security Centre (NCSC) - <https://report.ncsc.gov.uk>
- Do not offer to pay any ransom request, notify centre who will communicate with the ESFA
- 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
- Follow the PAY Standard Operating Procedure for referring a Cyber Incident to the Trust Central Team.

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.

4. CYBER RECOVERY PLAN

Verify the initial incident report as genuine and record on the [Incident Recovery Event Recording Form](#) at Appendix C.

1. 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.
2. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
3. In order to assist data recovery, if damage to a computer or backup 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.
4. Contact CFC Helpline 08009753034 or cyberclaims@cfc.com
5. Start the [Actions Log](#) to record recovery steps and monitor progress.
6. Convene the [Cyber Recovery Team](#) (CRT).
7. Liaise with IT staff to estimate the recovery time and likely impact.

8. Make a decision as to the safety of the school remaining open.
 - *This will be in liaison with relevant Local Authority Support Services / Trust*
9. 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*
10. Execute the [communication](#) strategy which should include a media / press release if applicable.
 - *Communications with staff, Trustees and parents / pupils should follow in that order, prior to the media release.*
11. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
12. 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.
13. 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.

5. 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:

	Central Team Role	Contact Details
Recovery Team Leader	Chief Operations Officer	07494 474785
Data Management	FireBird DPO	07943 659447
IT Restore / Recover	IT Technician	07398 574947 01535 616000
Site Security	Estates Business Partner	07904659903
Public Relations/Communications	CEO	07581 197391
Resources / Supplies		
Facilities Management	Estates Business Partner	07904 659903

6. SERVER ACCESS

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

Role	Contact Details
ICT Support	01535 616000
IT Technician	07398 574947

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

7. MANAGEMENT INFORMATION SYSTEM (MIS) ADMIN ACCESS

Please detail all the people with administrative access to the MIS

MIS Admin Access	Contact Details
Headteacher	
Operations Manager	
MIS Provider	02080502086
IT Technician	07398 574947

8. SCHOOL ACCESS CONSIDERATIONS

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

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

Clayton Village Primary school have paper fire registers which are kept in the main office for staff to access registers. We also have folders in a locked cabinet with each pupil's data sheets in to allow staff access to pupil contact details. Paper

copies of the telephone tree are also stored in the office allowing us to be able to make contact with staff members. The DSL and deputy DSL's are all aware of all current child protection concerns.

Staff and pupil contact numbers should be backed up in Wondes backup

9. BACKUP STRATEGY

School Process	Backup Type (include on-site / off-site)	Frequency
Google Drive	1 remote backup	Daily
	1 onsite backup to NAS	Continuous
School MIS	Offsite	Daily
Parago including assets inventory	Offsite	Daily, Weekly, Monthly
Email Server	Remote	Daily
CPOMS	Remote	Daily
PS Financials	Remote	Daily
HR / Staff Safe	Remote	Daily
Website	Remote	Daily

10. KEY CONTACTS

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection	Talk Straight / 01133 222333	School postcode
Backup Access	Datacable 01535 616000	School address
Telecom Provider	BT - 03301234150	School postcode
Website Host	Primary ICT Support / 011342642664	School postcode
Electricity Supplier	Corona Energy / 08008048589	School address
Burglar Alarm	TI Security / 0113 2812106	School address
Text Messaging System	PING / 03334559424	School address
Action Fraud	0300 123 2040	

11. STAFF MEDIA CONTACTS

All media contact will be dealt with as per the PAY Media Handling Policy.

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.

12. KEY ROLES AND RESPONSIBILITIES

Headteacher (with support from Deputy Head)

- Seeks clarification from the person notifying the incident.
- Sets up and maintains an incident log, including dates / times and actions.
- Convenes the Cyber Recovery Team (CRT) to inform of the incident and enact the plan.
- Liaises with the Chief of Operations.
- Liaises with the trust 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 Operations 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/ROPA and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher/Chief Operations Officer and determines if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

Chief Executive Officer

- Supports the Headteacher throughout the process and ensures 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 Trustees 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 Support company

- Verifies the most recent and successful backup.
- Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase.
- If necessary, arrange for access to the off-site backup.
- Protects any records which have not been affected.
- Ensures on-going access to unaffected records.

Cyber Security Business Partner

- 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.
- Provides an estimate of any downtime and advises which systems are affected / unaffected.

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

13. 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		
	Minutes of SLT meetings and agendas		
	Head's reports to Trustees (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		

Critical Activities	Data item required for service continuity	When Required	Workaround (Yes / No)
	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		
Critical Activities	Data item required for service continuity	When Required	Workaround (Yes / No)
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		
	Trustees meeting dates / calendar		
	Governor attendance and training records		
	Trustees minutes and agendas		
Administration	Admissions information		
	School to school transfers		
	Transition information		

Critical Activities	Data item required for service continuity	When Required	Workaround (Yes / No)
	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		

Critical Activities	Data item required for service continuity	When Required	Workaround (Yes / No)
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		

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 predetermined 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.

APPENDICE 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 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		
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:		