Cyber Response Policy

Approval date:	22 May 2023
Approved by:	Board of Trustees
Next review:	Summer 2025

Together we **Exceed**

Contents

Together we **Exceed**

1. Introduction

1.1   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.

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

1.3   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.

1.4   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.

1.5   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

2.1   When developing a Cyber Response Plan, consideration will be given to who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long the school/Trust would be able to function without each one, plans for internal and *external* communications and access to registers and staff and pupil contact details. This will allow the Trust / 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 Trust / School.
- To ensure that Trust schools 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 Trust which are unaffected.

3. Actions in the event of an incident

3.1 In the event of a suspected ransomware attack or other cyber incident, the following steps should be taken immediately:

- Enact the 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 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

3.2 **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

4.1 The following steps should taken when enacting the Cyber Recovery Plan:

- Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix D.
- Assess and document the scope of the incident using the Incident Impact Assessment at Appendix B to identify which key functions are operational / which are affected.
- In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
- 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.
- Contact RPA Emergency Assistance Helpline.
- Start the Actions Log to record recovery steps and monitor progress.

Together we **Exceed**

- Convene the <u>Cyber Recovery Team</u> (CRT).
- Liaise with IT staff to estimate the recovery time and likely impact.
- Make a decision as to the safety of the school remaining open.
  - *This will be in liaison with the Trust and any other relevant Support Services*
- 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*
- Execute the <u>communication</u> strategy which should include a media / press release if applicable.
  - *Communications with staff, trustees / governors and parents / pupils should follow in that order, prior to the media release.*
- Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
- Upon completion of the process, evaluate the effectiveness of the response using the <u>Post Incident Evaluation</u> at Appendix E and review the Cyber Recovery Plan accordingly.
- Educate employees on avoiding similar incidents / implement lessons learned.

5. Cyber Recovery Team

5.1   In the event of the Cyber Revovery Plan having to be initiated, the personnel named below will form the Cyber Recovery Team and take control of the following:
       Yellow sections to be updated by each school if different to the details below.

	Name	Role in Trust	Contact Details
Recovery Team Leader	R Crabtree	Chief Estates Officer	07577650468
Data Management	B Batty	ICT Manager	07845113908
IT Restore / Recover	B Batty	ICT Manager	07845113908
Site Security and Facilities Management	Head of affected site	Headteacher	TBD
Public Relations	R Jarvis	Chief Operating Officer	07576866787
Communications	P Taylor	Governance Manager	07747065002
Resources / Supplies	S Murray	Chief Finance Officer	07771550210

5.2 Server Access
Please detail all the people with administrative access to the server.

Role	Name	Contact Details
ICT Technical Lead	B Batty	07845113908
ICT Support Technician (s)	Various	01274600550
Third Party IT Provider	Virtue Technologies	01695731233

Together we **Exceed**

5.3 Management Information System (MIS) Admin Access
Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Headteacher	School to add	School to add
ICT Technical Lead	B Batty	07845113908
MIS Provider	Schools ICT - SIMS	03452226802
Data Manager	B Batty	07845113908

5.4 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

5.5 Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
School MIS	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Cloud Services (M365)	N/A	Under Review
Third Party Applications / Software	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Email Server (M365)	N/A	Under Review
Curriculum Files	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Administration Files	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Finance Documentation and data	Cloud based backup with PSF	Daily and monthly backups
HR / Personnel Records	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
InVentry	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Facilities Management	Onsite, Onsite and Airgapped	Daily with retention 90/30/30
Website	School to add	

5.6 Key Contacts

Supplier	Company	Contact
Internet Connection	BLN	01274434835
Backup Provider	Virtue Technologies	01695731233
Telecom Provider	Virtue Technologies	01695731233
Website Host	School to add	School to add
Electricity Supplier	Northern Powergrid	0800375675
Action Fraud	Action Fraud	03001232040
Local Constabulary	West Yorkshire Police	01274376059
Legal Representative	Stone King	01133024701

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

Together we **Exceed**

5.8 **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.

5.9 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.

5.10 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?

5.11 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.

5.12 Assigned Media Liaison(s):
Name: _____   Role:_____
Name: _____   Role:_____

6. Key Roles and Responsibilities

6.1 Every school is unique and the structure and staffing levels will determine who will be assigned which task. This example provides an overview of potential roles and responsibilities, but this is not an exhaustive or a definitive list.

6.2 **Headteacher**
- 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

6.3 **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.

Together we **Exceed**

6.4   **Site Manager / Caretaker**
- Ensures site access for external IT staff.
- Liaises with the Headteacher to ensure access is limited to essential personnel.

6.5   **School 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.

6.6   **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.

6.7   **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.

6.8   **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.
- 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.

Together we **Exceed**

- 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.

6.9 Teaching Staff and Teaching Assistants

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

Appendix A: Critical Activities - Data Assets

Schools should use this form to list all the data assets the school has access to and decide which are critical and how long the school 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.

Please 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 governors (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns		
	Attendance registers		
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Pupil Premium pupils and funding allocations		
	Pastoral records and welfare information		
Medical	Access to medical conditions information		
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	Schemes of work, lesson plans and objectives		
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
	Pupil reports and parental communications		
SEND Data	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		

Together we **Exceed**

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

Together we **Exceed**

Appendix B: 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.

Together we **Exceed**

Appendix C: 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, 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 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 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, 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 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 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].

Together we **Exceed**

5. Media Statement

[Inset school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the Trust 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.

Together we **Exceed**

Appendix D: 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.					

Together we **Exceed**

Appendix E: 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:		

Together we **Exceed**