Risk Protection Arrangement Cyber Response Plan

The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
Lancaster
LA1 4RR

t 01524 581872
e admin@baylearningtrust.com
website baylearningtrust.com

Document Control

This document has been approved for operation within:	**All Trust Establishments**
Date effective from	**September 2022**
Date of next review	**September 2023**
Review period	**12 months**
Status	**Statutory**
Owner	**The Bay Learning Trust**
Version	**v1.0**

Contents

1. Introduction

A Cyber Response Plan will be considered as part of an overall continuity plan that the Academy/School needs to ensure it maintains a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

If the Academy/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 will 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 will cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating cyber recovery. 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 this Cyber Response Plan, Directors of the Bay Learning Trust considered who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long it would be able to function without each one, establish plans for internal and external communications and have thought about how it would access registers and staff and pupil contact details. This will allow the school:

2.1 To ensure immediate and appropriate action is taken in the event of an IT incident.

2.2 To enable prompt internal reporting and recording of incidents.

2.3 To have immediate access to all relevant contact details (including backup services and IT technical support staff).

2.4 To maintain the welfare of pupils and staff.

2.5 To minimise disruption to the functioning of the school.

2.6 To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.

2.7 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. Preparation and Additional Resources

3.1 Preventative Strategies

It is vital we regularly review our existing defences and take the necessary steps to protect our networks. We will regularly review:

3.1.1 Regularly review IT Security Policy and Data Protection Policy.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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:

3.1.6 If external RDP connections are used, MFA should be used

3.1.7 Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect

3.1.8 Enable an account lockout policy for failed attempts

3.1.9 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

3.1.10 Review NCSC advice regarding measures for IT teams to implement: Mitigating malwareand ransomware attacks - NCSC.GOV.UK

3.1.11 Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

3.2 Advice and guidance

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

3.3 Acceptable Use

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

3.3.2 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.

3.4 Communicating the Plan

We will 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.

3.5 Testing and Review

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

We will train key staff members to feel confident following and implementing the plan. We will 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

3.6 Making Templates Readily Available

We will ensure templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

4. Actions in the event of an incident

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

4.1 Enact our Cyber Recovery Plan

4.2 Contact the 24/7/365 RPA Cyber Emergency Assistance:
By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**

4.3 Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk

4.4 Contact the local police via Action Fraud Action Fraud website or call **0300 123 2040**

4.5 Contact our Data Protection Officer

4.6 Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**

4.7 Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

We are 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.

5. Cyber Recovery Plan

1. We will verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. We will 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 will isolate devices from the network.
4. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **will 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.
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 school's Data Protection Officer and the police*
11. Execute the communication strategy which will include a media / press release if applicable.

- *Communications with staff, governors and parents / pupils will follow in this 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.

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

The following sections are completed to produce a bespoke Cyber Recovery Plan for our school:

5.1 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		Headteacher	
Data Management		Service Manager	
IT Restore / Recover			
Site Security		Site Manager	
Public Relations			
Communications			
Resources / Supplies			
Facilities Management			

This procedure will be published with contact details included due to the risk of a data breach.

5.2 Server Access

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

Role	Name	Contact Details
Headteacher		
School Business Manager		
IT Support Technician		
Third Party IT Provider		

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

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 Business Manager		
MIS Provider		
Data Manager		

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, we have considered how we will access the following:

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

5.4 Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server		
School MIS		
Cloud Services		
Third Party Applications / Software		
Email Server		
Curriculum Files		
Teaching Staff Devices		
Administration Files		
Finance / Purchasing		
HR / Personnel Records		
Inventory		
Facilities Management / Bookings		
Website		
USBs / portable drives		

5.5 Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection		
Backup Provider		
Telecom Provider		
Website Host		
Electricity Supplier		
Burglar Alarm		
Text Messaging System		
Action Fraud		
Local Constabulary		
Legal Representative		
LA / Trust Press Officer		

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

5.6 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 will 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 Media Liaison(s):

Name: Role: Headteacher

Name: Role: Deputy Headteacher

5.7 Key Roles and Responsibilities

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 Manager to contact parents, if required, as necessary

Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

Site Manager / Caretaker

- Ensures site access for external IT staff. • Liaises with the Headteacher to ensure access is limited to essential personnel.

School Business Manager

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the standard response and knows who the media contact within school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical

support staff

- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO)

- Supports the school, using the school data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Chair of Governors and determines if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

Chair of Governors

- Supports the Headteacher throughout the process and ensure decisions are based on sound judgement and relevant advice.
- Understands there may be a need to make additional funds available – have a process to approve this.
- Ensures all governors are aware of the situation and are advised not to comment to third parties / the media.
- Reviews the response after the incident to consider changes to working practices or school policy.

IT Lead / IT Staff

Depending upon whether the school has internal or outsourced IT provision, the roles for IT Coordinators 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.
- 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
- Record any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed

5.8 Critical Activities - Data Assets

We have listed all the data assets our school has access to and have decided which are critical and how long we 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.

We have completed the required column with the timescale we believe is necessary for recovery.

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

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address	4 hours	
	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	4 hours	
	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	4 hours	
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	Schemes of work, lesson plans and objectives	4 hours	
	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	4 hours	
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records, including house points or conduct points	72 hours	
	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	72 hours	
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
	Exam results		
Governance	School development plans	72 hours	
	Policies and procedures		
	Governors meeting dates / calendar		
	Governor attendance and training records		
	Governors minutes and agendas		
Administration	Admissions information	4 hours	
	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	72 hours	
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision	24 hours	
	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	4 hours	
	CCTV access		
	Site maps		
	Maintenance logs, including legionella and fire records		
	Risk assessments and risk management systems		
	COSHH register and asbestos register	4 hours	
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

We have used 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)

Existing Recovery can be promptly facilitated with the resources which are Resources readily available to the school.

	Facilitated by	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?	

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:		