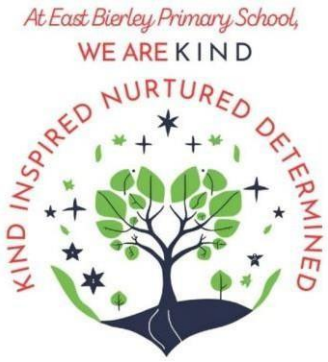
East Bierley CE (VC) Primary School

Risk Protection Arrangements

&

Cyber Response Plan

THE CHURCH OF ENGLAND
Diocese of Leeds



Our vision:

To be a vibrant and inclusive Christian School where everybody is known, valued and inspired to reach their full potential. We nurture curiosity, creativity and a love of learning, equipping our pupils with knowledge, skills and character to flourish in an ever-changing world.

Friendship, Courage, Kindness, Respect, Forgiveness, Faith

Contents

1. Introduction 3
2. Aims of a Cyber Response Plan 3
3. Risk Protection Arrangement Cover 3
4. Preparation and Additional Resources 4
5. Actions in the event of an incident 5
6. Cyber Recovery Plan 6
7. Appendix A: Incident Impact Assessment 13
8. Appendix B: Communication Templates 14
9. Appendix C: Incident Recovery Event Recording 18
10. Appendix D: Post Incident Form 19

1. Introduction

A Cyber Response Plan should be considered as part of the overall continuity plan that East Bierley CE (VC) Primary Schools need 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 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 will be well communicated and readily available. This 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 the Cyber Response Plan

When developing the Cyber Response Plan, East Bierley Primary School 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 thought about how we would access registers and staff and pupil contact details. This will allow the school:

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

3. Risk Protection Arrangement Cover

From 1st September 2022, our Risk Protection Arrangement (RPA) membership will include cover for Cyber Incidents, which is defined in the RPA Membership Rules as: “Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data.”

Our RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, we must contact the RPA Emergency Assistance. To be eligible for RPA Cyber cover, there are 4 conditions that we as members must meet:

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

It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ask their IT teams or external IT providers to ensure the following:

a) Backing up the right data. Ensuring the right data is backed up is paramount.

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

c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups. Further Help and guidance on backing up can be found at: Step 1 - Backing up your data. https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

2. All Employees or Governors who have access to the Member's information technology system must undertake NCSC Cyber Security Training by the November or the start of the Membership Year, whichever is later. Upon completion, a certificate can be downloaded by each person. In the event of a claim the Member will be required to provide this evidence.
3. 3. Register with Police CyberAlarm. Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed, the tool will record traffic on the network without risk to personal data. When registering, use the code "RPA Member" in the Signup code box.
4. 4. Have a Cyber Response Plan in place.

4. Preparation and Additional Resources

Preventative Strategies

- Regularly review our IT Security Policy and Data Protection Policy.
- Assess our current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role-based user access.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis.
- 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:
    - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
    - Enable an account lockout policy for failed attempts
    - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Advice and guidance

The NCSC website has an extensive range of practical resources to help improve Cyber Security for the school. This is regularly reviewed to ensure we are operating the most up to date interventions.

Acceptable Use

The school will ensure that all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices. Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

The school will communicate the Cyber Recovery Plan to all those who are likely to be affected and we will inform key staff/Governors/Visitors of their roles and responsibilities in the event of an incident, prior to any issue arising.

Testing and Review

During an incident there will be many actions to complete, and each step will be well thought out, cohesive, and ordered logically. Key staff members will be trained so that they feel confident following and implementing the plan. The school will review the plan regularly to ensure contact details are up-to-date and new systems have been included. NCSC have resources which can test our incident response with an Exercise in a Box.

5. Actions in the event of an incident

If the school suspects that they have been the victim of a ransomware or other cyber incident, they will take the following steps immediately:

1. Enact their Cyber Recovery Plan;
2. Contact their Data Protection Officer;
3. Assess the cyber incident and impact, if required follow the relevant steps below, based on the assessment;

- Contact the 24/7/365 RPA Cyber Emergency Assistance by telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com, where the following will take place:
    - 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 their local police via Action Fraud website
- Contract their Local Authority (LA)
- Consider whether reporting to the ICO is necessary (a joint decision between the Cyber Response Team and the Data Protection Officer)
- Contact the Sector Security Enquiries Team at the Department for Education.

6. Cyber Recovery Plan

In the case of a cyber security incident the Cyber Response Team will implement the following steps.

1. Verifying the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Convene the Cyber Recovery Team (CRT).
3. Contact your Data Protection Officer.
4. 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.
5. In the event of a suspected cyber-attack, IT staff will isolate devices from the network.
6. 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.
7. Contact RPA Emergency Assistance Helpline (if required).
8. Start the Actions Log to record recovery steps and monitor progress.
9. Liaise with IT staff to estimate the recovery time and likely impact.
10. Make a decision as to the safety of the school remaining open.
    - This will be in liaison with relevant Local Authority Support Services/School/school SLT

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 should include a media/press release if applicable.
12. Communications with staff, governors and parents/pupils should follow in that order, prior to the media release.
13. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
14. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation Form at Appendix D and review the Cyber Recovery Plan accordingly.
15. Educate employees on avoiding similar incidents / implement lessons learned.

Cyber Recovery Team

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

	Name	Role in School	Contact Details
Recovery Team Leader	Victoria Meek	Headteacher	headteacher@eastbierleyprimary.com
Data Management	Kyle Smith	IT Manager	kyle.smith@globalcs.co.uk
IT Restore/Recover	Kyle Smith	IT Manager	Kyle.smith@globalcs.co.uk
Site Security	Victoria Meek	Headteacher	headteacher@eastbierleyprimary.com
Public Relations	Sara Hunter	Business Manager	office@eastbierleyprimary.com
Communications	Sara Hunter	Business Manager	office@eastbierleyprimary.com
Resources/Supplies	Sara Hunter	Business Manager	office@eastbierleyprimary.com
Facilities Management	Sara Hunter	Business Manager	office@eastbierleyprimary.com

Server Access

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

Role	Name	Contact Details
Headteacher	Victoria Meek	headteacher@eastbierleyprimary.com
School Business Manager	Sara Hunter	office@eastbierleyprimary.com
IT Support Technician	Kyle Smith	Kyle.smith@globalcs.co.uk
Third Party IT Provider		

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

Backup Strategy

School Process	Backup Type, include (onsite/offsite)	Frequency
Main file server (each school has own onsite server)	Onsite and offsite	Daily
System State (active directory etc)	Onsite and offsite	Daily
School MIS services	Offsite	Daily cloud back up
Third party applications	Offsite	Daily cloud back up
Software email (google/Microsoft)	Offsite	Daily via cloud
Curriculum files	Onsite and offsite	Daily
Teaching staff devices (laptop, IPad, Phone)	Onsite and offsite	Daily
Administration files	Onsite and offsite	Daily
Finance/purchasing files	Onsite and offsite	Daily

HR/Personnel records	Onsite and offsite	Daily
Inventories	Onsite and offsite	Daily
Facilities management/Bookings	Onsite and offsite	Daily
Website	Onsite and offsite	Daily
USBs/portable drives	Onsite and offsite	Daily

Key Contacts

Supplier	Contact/Tel Number	Account Reference Number
Internet provider	0113 5216055	NextGen
Anti-Virus provider	0113 5216055	NexGEN/WatchGuard Cloud
Backup provider		
Telecoms provider	0800 8499984	Direct Voice and Data/LOG03197
Website host	0800 9553999	GreenHouse
Email provider	0800 0260329	Outlook
Electricity provider	0800 111 999	EDF Energy
Burglar Alarm	01924 473890	AC Secure
Action Fraud	0300 123 2040	
Local Police	07725648595	Sanda Beaumont
Legal Representative	0800 232 1927	Zurich/QLA-03G035-0433
Data Protection Officer	07747 611662	Re DPO Sarah Smith

Please Note: Any personal data in this document must not be published as this may risk a data breach. Also ensure this plan is kept up-to-date with new contact details, and changes to policy.

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 Media Liaison(s):

- Name: Victoria Meek Headteacher
- Name: Sara Hunter Business Manager

Key Roles and Responsibilities

Head Teacher (with support from The Business Manager)

- Liaise with IT Manager and seek 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 Governors.
- Liaises with the school Data Protection Officer.
- Convenes and informs the school's SLT, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.

Headteacher (with support from Deputy Head)

- Liaise with IT Manager and seek 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)

- To seek 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.
- If action required will liaise with the Cyber Recovery Team and the Data Protection Officer.

Caretaker

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

School Business Manager (role responsibilities dependent on action required)

- 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/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 CEO/Headteacher / IT Manager/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 Cyber Response Team 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

- Liaise with relevant SLT and seeks clarification from person notifying incident.
- Isolate device/system.
- Assess incident and likely impact.
- Liaise with Anti-Virus provider on action required.
- 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 CEO/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

- Reassure pupils.
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed.

Critical Activities -Data Assets

Critical Activities	Data item required for service continuity	When required	Work around (Yes or No)
Leadership & Management	Files/folders/emails	4 hours	Yes
Safeguarding & Welfare	Access to systems that record and report safeguarding concerns	24 hours	Yes
	Attendance registers	24 hours	Yes
	Class groups, teachings groups, teacher's timetables	24	Yes
	Referral information/outside agency/TAF	24	Yes
	Child protection records	24	Yes

	Looked after children records/PEPs	24	Yes
	Pupil premium pupils and funding allocation	24	Yes
	Pastoral records and welfare information	24	Yes
Medical	Access to medical conditions information	4 hours	Yes
	Administration of medicines records	4 hours	Yes
	First Aid/accident logs	4 hours	Yes
Teaching	Schemes of work, lessons plans and objectives	4 hours	Yes
	Seating plans	48 hours	Yes
	Teaching resources	48 hours	Yes
	Learning Platform/Homework Platform	48 hours	Yes
	Curriculum learning apps/online resources	48 hours	Yes
	CPD & staff records	48 hours	Yes
	Pupil reports and parental communications	48 hours	Yes
SEND Data	SEND list and records provision	24 hours	Yes
	Accessibility tools	24 hours	Yes
	Access arrangement and adjustments	24 hours	Yes
	IEPs / EHCPs / GRIPS	24 hours	Yes
Conduct & Behaviour	Reward system records, including house points or conduct points	48 hours	Yes
	Behaviour system records, including negative behaviour points	48 hours	Yes
	Sanctions	48 hours	Yes
	Exclusion records, past & current	48 hours	Yes
	Behavioural observations / staff notes and incident records	48 hours	Yes
Assessment & Exams	Exam entries and controlled assessments	1 week	Yes
	Targets, assessments, tracking data	1 week	Yes
	Baseline and prior attainment records	1 week	Yes
	Exam timetables and cover provision	1 week	Yes
	Exam results	1 week	Yes
Governance	School development plans	1 week	Yes
	Policies and procedures	1 week	Yes
	Governor's meeting dates/calendar	1 week	Yes
	Governor attendance and training records	1 week	Yes
	Governor minutes and agendas	1 week	Yes

Critical Activities	**Data item required for service continuity**	**When required**	**Work around (Yes or No)**
Administration	Admissions information	48 hours	Yes
	School to school transfers	48 hours	Yes
	Transition information	48 hours	Yes
	Contact details of pupils and parents	48 hours	Yes
	Access to absence reporting systems	48 hours	Yes
	School diary of appointments and meetings	48 hours	Yes
	Pupil timetables	48 hours	Yes
	Letters to parents/newsletters	48 hours	Yes
	Extra-curricular activity timetable and contacts for providers	48 hours	Yes
	Census records and statutory return data	48 hours	Yes
Human Resources	Payroll systems	72 hours	Yes

	Staff attendance, absence, reporting facilities	72 hours	Yes
	Disciplinary and Grievance records	72 hours	Yes
	Staff timetables and any cover arrangements	72 hours	Yes
	Contact details of staff	72 hours	Yes
Office Management	Photocopying/printing provision	72 hours	Yes
	Telecoms - school phones and access to answerphone messages	72 hours	Yes
	Email – access to school email systems	24 hours	Yes
	School website and any website chat functions / contact forms	72 hours	Yes
	Social media accounts (Facebook / Twitter)		Yes
	Management Information System (MIS)		Yes
	School text messaging system		Yes
	School payment system (ParentPay)		Yes
	Financial Management System - access for orders / purchases		Yes
Site Management	Visitor sign in/sign out	72 hours	Yes
	CCTV access		No
	Site maps		Yes
	Maintenance logs, including legionella and fire logs		Yes
	Risk assessments and risk management systems		Yes
	COSHH register and asbestos register		Yes
Catering	Contact information for catering staff	24 hours	Yes
	Supplier contact details	72 hours	Yes
	Payment records for food and drink	72 hours	Yes
	Special dietary requirements & allergies	24 hours	Yes
	Stock taking & orders	24 hours	Yes

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).

Recovery

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

a) School Open

Dear Parent/Carer,

I am writing to inform you that it appears the school/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 [School / 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 [School / 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,

b) School Closure

Dear Parent/Carer,

I am writing to inform you that it appears the school/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 [School / 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 [School / 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,

c) Staff Statement – School 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 [School / LA] the school will remain open with the following changes to working practice:

- (Detail any workarounds / changes)

The school/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 their on-going investigation, please provide it promptly. The school/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].

d) Staff Statement – School Closed

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

- (Provide a description of the services affected)

Following liaison with the [School / 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/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/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].

Media Statement

[INSERT SCHOOL/SCHOOL NAME] detected a cyber-attack on [date] which has affected the school/school IT systems.
Following liaison with the [School / LA] the school/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.

Standard Staff Response

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.

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 (Date/Time)	Contacted by	Response

Actions Log

Recovery Tasks (In order of completion)	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		

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 and procedures:		