Withinfields Primary School Cyber Security Incident Response Plan

Introduction

A cyber incident is defined by the National Cyber Security Centre ('NCSS') as 'a breach of a system's security policy in order to affect its integrity or availability and/or the authorised access or attempted unauthorised access to a system or systems.'

There are four types of cyber security incident that may occur in your school:

- Attempts to gain unauthorised access to a system or data;
- Unauthorised use of systems for storing or processing data;
- Unauthorised changes to a system's firmware, software or hardware; and/or
- Malicious disruption/denial of service.

The main types of cyber security incidents that affect schools and academies are ransomware attacks, phishing attacks and unauthorised access to data due to human error.

This Cyber Security Incident Response Plan sets out the school's plan on how to deal with the different cyber security incidents it may face.

This Cyber Security Incident Response Plan should be considered as part of an overall response/continuity plan that the school adopts to ensure that any breach/threat is contained, data is secured and at least a minimal level of functionality to safeguard pupil and staff is maintained before restoring the school back to an operational standard.

Having a Cyber Security Incident Response Plan in place ensures that all staff know what they need to do if a cyber security incident occurs and reduces the risks of additional data being compromised by dealing with the matter in a timely manner and reducing any adverse risk to reputation.

Key Personnel/Stakeholders and responsibilities

The following personnel/stakeholders will need to be involved in the Cyber Security Incident Response and will be known as the Cyber Response Team:

- **IT support/Network manager –** responsible for securing the network and IT systems, blocking the unauthorised access, restoring the IT systems/network and advising on any technical IT specific matters connected to the incident.
- **Data Protection Officer –** responsible for ensuring the personal data is protected, advising on the steps to be taken to secure the data and deal with the breach and reporting incidents to the ICO (where applicable) and documenting the incident on internal records. Advising on the data protection matters connected to the incident.
- **Headteacher/Principal (recovery team leader) –** responsible for liaising with, and following the advice provided by IT and the DPO. Managing communication to staff and/or parents assisted by the DPO and IT support. To assist in minimising the disruption caused to the

functionality of the school and overall responsibility for the welfare of the pupils and staff. Responsible for any communications/PR regarding the incident.

- **School Business Manager/PA –** responsible for assisting the headteacher with their obligations and taking the necessary action required for the Risk Protection Arrangement cover. To work with IT to gain immediate access to all registers and contact information.
- **Site Manager –** site security and access for members of the cyber recovery team.
- **All staff –** responsible for reporting any suspected data breaches or cyber security incidents to the headteacher/IT/DPO as soon as they are discovered.

If you have, or suspect that you have, encountered a cyber security incident then you must report this immediately to IT by contacting:

Primary T on 01274918777 or servicedesk@primaryt.co.uk

You must also contact the Data Protection Officer:

The DP Advice Service (info@thedpadviceservice.co.uk or telephone 01422 730 024). Please note the contact telephone number will redirect to a mobile number for out of hours advice.

Please ensure that contact details of key personnel are not published.

More information about roles and responsibilities of key personnel are contained within Appendix One.

Risk Protection Arrangement Cover

From April 2022, the Risk Protection Arrangement (RPA) 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."

RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, you must contact the RPA Emergency Assistance.

To be eligible for RPA Cyber cover, there are 4 conditions that 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 can 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. See Critical Activities for a suggested list of data to include.

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 - NCSC.GOV.UK.
https://www.ncsc.gov.uk/collection/small-businessguide/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 start of the Membership Year. 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. **Register with Police CyberAlarm**. Registering will connect Members with their local police cyber protect team and, in most 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. **Have a Cyber Response Plan in place.** For full terms and conditions of Cyber cover, please refer to the relevant Membership Rules on gov.uk.

Preventative measures

This Cyber Security Incident Response Plan focuses on what to do following a cyber security incident, but it is important to first mention the measures that are being taken to prevent an incident occurring.

To prevent an attack, the school:

- Regularly reviews the IT Security Policy and Data Protection Policy.
- Regularly assesses the Cyber Essentials requirements, ensuring appropriate and up-to-date firewalls rules, malware protection and role-based user access.
- Ensures Multi-Factor Authentication (MFA) and/or other security access measures are in place.
- Routinely installs security and system updates and a regular patching regime minimising the risk to any internet-facing device. This includes Exchange servers, web servers, SQL servers,

VPN devices and Firewall devices. Ensuring that security patches are checked for and applied on a regular basis.

- Enables and reviews 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:
  - If external RDP connections are used, MFA should be used
  - 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 school's 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
- Provides staff training on cyber security risks, how to recognise, report and appropriately respond to an incident.
- Implementing and updating an appropriate Acceptable Use Policy – this must be read and signed by all staff and pupils before use. (*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).*

Response Stage 1 – Detect

The school has measures in place to prevent a cyber security attack and measures to detect when an attack has taken place or has been attempted.

Detecting an incident will depend on the nature and circumstances of that incident. For example, an incident may be the loss of a laptop or USB stick and the quickest way to detect this will be when the member of staff reports the laptop/USB stick as lost. A cyber-attack will be detected using the school's security monitoring measures.

Security monitoring measures may detect things like multiple failed log-in attempts to a user account, attempts to access unauthorised websites or other unauthorised attempts to access the IT systems.

As soon as a potential incident has been detected, stage 2 of the response plan will be initiated.

A record will be kept of any incidents that are detected.

Response Stage 2 – Triage

As soon as an incident is detected IT will carry out an initial investigation to determine whether there has been a genuine incident or whether it is a false alarm.

This investigation should determine the nature of the incident, what systems/data has been affected, whether the threat has been contained or is ongoing and any other information relevant to addressing the incident.

The investigation should be carried out as quickly as possible and details of the investigation should be documented in writing on the Incident Impact Assessment at Appendix 3 and a record should be made on the Incident Report Form at Appendix 5.

If your IT support is outsourced to an external provider then, depending on the nature of the incident, they may have been the ones to detect this and already determine whether it is genuine before they have contacted you.

If your IT support is outsourced to an external provider and someone within your school has detected the incident, you will need to contact your IT provider as a matter of urgency for them to assess whether the incident is genuine or a false alarm and carry out the initial investigation.

If the incident is genuine, and you haven't already done so, you will need to take appropriate steps to contain the incident (for example – if you are aware of an attacker moving through your systems, you could force logout), secure the data and contact your Data Protection Officer.

Any further steps to be taken will depend on the nature of the incident.

Response Stage 3 - Report

If you suspect that the incident involves a ransomware attack or other such security breach, you should report this to the following organisations immediately:

- Convene the Cyber Recovery Team and liaise with IT.
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com
    - 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
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer who will determine whether it is necessary to report the matter to the ICO.

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

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and to help prevent further systems becoming affected.

Response Stage 4 – Remediate

Whilst this is listed as stage 4 it should be carried out immediately and, simultaneously to, if not before, reporting the matter in stage 3, in any instance where the threat is still active, or the risk of the threat remains present.

For example, if the incident involves a ransomware attack and the attacker still appears to be present in your system, you will need to force them out and secure your system.

You must contain the breach by securing the network/system and isolate devices from the network.

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 or tamper with or move damaged computers, discs or tapes.

All steps taken at this stage should be recorded on your incident log and shared with any relevant agencies that you have contacted in stage 3.

At this stage you should consider whether it is safe for the school to remain open. You should seek advice from those listed in Stage 3 to make that decision.

You should consider your communication plan for staff, governors/trust board and, where necessary, pupils/parents. (See template communications at Appendix 4).

Response Stage 5 – Recover

In this stage you will ensure that you take appropriate steps to get the school back up and running as normal. Any trace of malware or other cyber threats must be eradicated to restore the network/system safely from back-ups.

It is recommended that impacted systems are tested before connecting and using them as normal again.

It will be necessary to review the systems which have been impacted and complete the Critical Activities Data Asset schedule in Appendix Two in order to ascertain where the priorities lie for recovery.

It may be appropriate to implement the wider communication plan including any media/press release. (See template communications at Appendix 4).

All steps taken in the recovery stage should be documented in the incident form and progress of these steps should be monitored and any adjustments to recovery timescales should be made accordingly.

Response Stage 6 – Review

After full recovery from the incident, review and evaluate the effectiveness of the response plans, procedures, and other measures to identify scope for improvement and prevent further occurrence of the same incident.

Complete the Post Incident Evaluation at Appendix 6 and review this Cyber Recovery Plan accordingly.

Conduct any relevant staff training that may assist with the response to future incidents.

Ensure this plan is kept up-to-date.

Appendix 1 – Roles and Responsibilities

This appendix should be read in conjunction with the ‘Key personnel/stakeholders and responsibilities’ section of this response plan.

Priority access:

The School Business Manager will liaise with IT and when it is safe to do so, will access the following:
- Registers
- Staff / Pupil contact details

The DSL will liaise with IT and when it is safe to do so, will access the:
- Current Child Protection Concerns

Server Access:

The following people have administrative access to the server:

PrimaryT personnel

Management Information System (MIS) Admin Access:

The following people have administrative access to the MIS:
Head and School Business Manager

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): Deputy head

Key Roles and Responsibilities

Headteacher or Principal	School Business Manager or PA	Designated Safeguarding Lead	Site Manager or Caretaker	Chair of Governors	IT Lead or Provider	DPO
● Seeks clarification from person notifying of the incident. ● Sets up and maintains the incident log and completes the relevant dates/times and actions ● Convenes the Cyber Recovery Team to inform of the incident and enact the plan. ● Liaises with the Chair of Governors. ● Liaises with the DPO.	• 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	● Considers whether there is a safeguarding aspect to the incident. ● Assists the headteacher with ensuring that all pupils and staff are safe. ● Considers whether it is necessary to seek assistance from, or make a report to, cyber protect officers, early help or social services.	● Ensures site access for external IT staff and DPO. ● Liaises with headteacher to ensure site access is limited to relevant personnel.	• Supports the Headteacher throughout the process and ensures decisions are based on sound judgement and relevant advice. • Understands there may be a need to make additional funds available – have a process to approve this. • Ensures all governors are aware of the situation and are advised not to comment to third parties / the media. • Reviews the response after the	• 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.	• 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.

● Leads communication to all staff ● Prepares or signs off on any communication to pupils/parents. ● Prepares or signs off on any communication to the media. ● Liaises with the SBM or PA about for assistance with these actions.	parents / school emails – as approved by headteacher. • Assesses whether payroll or HR functions are affected and considers if additional support is required.			incident to consider changes to working practices or school policy.	• 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 Records any relevant information which pupils may provide. • Ensures any temporary procedures for data	

					storage / IT access are followed	

*Depending upon whether the school/academy has internal or outsourced IT provision, the roles for IT Coordinators and technical support staff will differ.

Appendix Two – Critical Activities – Data Assets

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	1 month	
	Head's reports to governors (past and present)	1 month	Print copies held
	Key stage, departmental and class information	1 week	Print copies held
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns	48 hours	CPOMS – paper records can be utilised to be scanned on when access restored
	Attendance registers	48 hours	SIMS – have printed registers to use
	Class groups / teaching groups, and staff timetables	48 hours	SIMS – have printed timetables and registers
	Referral information / outside agency / TAFs	48 hours	CPOMS – access can be sourced from other agencies
	Child protection records	48 hours	CPOMS – as above
	Looked After Children (LAC) records / PEPs	48 hours	CPOMS and LA records – access can be sourced from other agencies
	Pupil Premium pupils and funding allocations	1 month	
	Pastoral records and welfare information	48 hours	CPOMS – paper records can be utiilised to be scanned on when access restored
Medical	Access to medical conditions information	4 hours	Print copies held
	Administration of Medicines Record	NA	Print copies held
	First Aid / Accident Logs	NA	Print copies used
Teaching	Schemes of work, lesson plans and objectives	4 hours	Google drive access needed. Can be replanned but given time
	Seating plans	NA	
	Teaching resources, such as worksheets	4 hours	Google drive access needed. Can be replanned but given time
	Learning platform / online homework platform	4 hours	Google drive access needed. Can be replanned but given time
	Curriculum learning apps and online resources	1 week	Needed particularly for SEND pupils.
	CPD / staff training records	2 weeks	
	Pupil reports and parental communications	4 hours	Communication via ClassDojo important as main means of communication
SEND Data	SEND List and records of provision	2 weeks	Google drive access needed. Paper copies available of IDLPs but needed for reviews
	Accessibility tools	NA	

	Access arrangements and adjustments	2 weeks	
	IEPs / EHCPs / GRIPS	2 weeks	
Conduct and Behaviour	Reward system records, including house points or conduct points	72 hours	
	Behaviour system records, including negative behaviour points	1 week	Would revert to paper records adding to existing records when resolved. Google drive needed
	Sanctions	1 week	
	Exclusion records, past and current	48 hours	SIMS
	Behavioural observations / staff notes and incident records	1 month	Previous records can be managed without. Paper records to be kept while not available
Assessment and Exams	Exam entries and controlled assessments	72 hours	4 hours if during SATs week
	Targets, assessment and tracking data	2 weeks	Google drive needed
	Baseline and prior attainment records	48 hours	SIMS
	Exam timetables and cover provision	NA	
	Exam results	NA	
Governance	School development plans	72 hours	Google drive needed
	Policies and procedures	72 hours	Google drive needed. Some held on school website
	Governors meeting dates / calendar	1 month	Google drive needed. Held off site by clerk also
	Governor attendance and training records	1 month	
	Governors minutes and agendas	1 month	
Administration	Admissions information	4 hours	
	School to school transfers	72 hours	Unless in September when it would be needed more quickly. SIMS
	Transition information	1 month	Unless in July when it would be needed more quickly. SIMS and Google drive needed
	Contact details of pupils and parents	48 hours	Paper copies of some details held. Can access via CPOMS, SIMS or School Gateway if have access to one
	Access to absence reporting systems	Dependent on systems. If none, 12 hours	Can manage if we have access to one of: Telephones, SIMS, Classdojo or School Gateway. Can revert to paper copies until resolved.
	School diary of appointments / meetings	12 hours	Google drive needed
	Pupil timetables	NA	
	Letters to parents / newsletters	1 month	Google drive needed. Newsletter on school website and classdojo
	Extra-curricular activity timetable and contacts for providers	1 month	Registers printed
	Census records and statutory return data	1 month unless	PLASC returns printed. Held on server and backed up.

		census day	
Human Resources	Payroll systems	72 hours	Held off site by payroll. Access to information via iTrent
	Staff attendance, absences, and reporting facilities	By beginning of month	Held off site by payroll. Paper copies kept of staff absence.
	Disciplinary / grievance records	NA	Paper copies kept
	Staff timetables and any cover arrangements	NA	
	Contact details of staff	4 hours	SIMS
Office Management	Photocopying / printing provision	24 hours	RISO current provider
	Telecoms - school phones and access to answerphone messages	24 hours	Mobile phone could be purchased
	Email - access to school email systems	4 hours	
	School website and any website chat functions / contact forms	72 hours	Lee Gething – website manager
	Social media accounts (Facebook / Twitter)	NA	
	Management Information System (MIS)	4 hours	SIMS
	School text messaging system	4 hours	School Gateway/School Comms
	School payments system (for parents)	48 hours	School Gateway/School Comms
	Financial Management System - access for orders / purchases	48 hours	FMS/SIMS
Site Management	Visitor sign in / sign out	1 week	Can revert back to written records
	CCTV access	48 hours	Needed for barrier safety when installed
	Site maps	NA	Printed copies held
	Maintenance logs, including legionella and fire records	1 week	Printed copies held
	Risk assessments and risk management systems	1 week	Google drive needed and server
	COSHH register and asbestos register	4 hours	Some printed
Catering	Contact information for catering staff	NA	Held offsite
	Supplier contact details	NA	
	Payment records for food & drink	24 hours	SIMS
	Special dietary requirements / allergies	4 hours	SIMS
	Stock taking and orders	NA	Paper based

Appendix 3: 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:

	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 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 4: Communication Templates

Parent/Pupil 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 liaising 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,

Parent/Pupil 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 liaising 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,

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 [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].

Staff Statement – School 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].

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.)

Points to note:

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 5: Incident Report 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

Action Log

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

Appendix 6: 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:		

DATA PROTECTION SPECIALISTS