

Walton and Lees Hill CE Primary School

CYBER SECURITY AND RESILIENCE STRATEGY

Approved by	
Name:	Joss Scouler
Position:	Chair of Governors
Signed:	J Scouler
Date:	Sept 2024
Review date:	Sept 2025
<i>This procedure should not be published with contact details included due to the risk of a data breach</i>	

¹ The Governing body to approve.

² The Governing body are free to determine review period.

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original	Sept 2023
2	Review – minor changes to contact information.	Sept 2024

CONTENTS

PART A – CYBER SECURITY AND PREVENTATIVE MEASURES	5
1. Introduction	5
1.1 Cyber Security.....	5
1.2 Cyber Resilience.....	5
1.3 Purpose of this document	5
2. Preventative strategies	6
2.1 Identify.....	6
2.2 Protect	6
2.3 Detect.....	7
PART B - CYBER RESPONSE PLAN.....	8
1. Introduction	8
1.1 Aims of the Cyber Response Plan.....	8
2. Response and Recovery	9
2.1 Respond - Actions in the event of an incident	9
2.2 Recover - Restoring data and services	10
2.3 Post Incident Evaluation.....	10
Checklist A – Key People	10
Cyber Recovery Team	10
Server Admin Access.....	10
Management Information System (MIS) Admin Access	11
Checklist B - Key Roles and Responsibilities.....	11
Head Teacher (DSL)	11
Designated Safeguarding Lead (DSL) Role.....	Error! Bookmark not defined.
School Business Manager.....	11
Data Protection Officer (DPO)	12
Chair of Governors	12
IT Provider	12
Teaching Staff and Teaching Assistants	12
Checklist C - Key Contacts	Error! Bookmark not defined.
Checklist D - Critical Activities - Data Assets.....	Error! Bookmark not defined.
Checklist E - Backup Strategy	Error! Bookmark not defined.

[Appendix A - Incident Impact Assessment](#)

[Appendix B - Communication Templates](#)

[Appendix C - Incident Recovery Event Recording Form](#)

[Appendix D - Post Incident Evaluation](#)

PART A – CYBER SECURITY AND PREVENTATIVE MEASURES

1. Introduction

1.1 Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies.

Cyber security should be high on the agenda for any school with a reliance on IT and online systems. Over and above the disruption to business processes which cyber security breaches can involve, organisations that suffer cyber security breaches may face significant fines. There are also non-financial costs to be considered, like reputational damage.

1.2 Cyber Resilience

Cyber resilience is the ability of an organisation to enable business continuity by preparing for, responding to, and recovering from cyber security threats. Cyber resilience is built upon five pillars:

Identify

Firstly, schools must have in depth knowledge of the level of security and potential risks. Therefore, the school's essential information has to be meticulously identified and the infrastructure and information has to be evaluated, including the level of sensitivity, vulnerability and risk tolerance.

Protect

Implement the necessary protection measures. Protection measures for critical infrastructures and services have to be developed and implemented, with the aim of mitigating or reducing the level of vulnerability.

Detect

Appropriate actions must be implemented in order to rapidly identify an attack, evaluate the affected systems and guarantee a timely response. Furthermore, during this stage, the network must be continuously monitored in order to identify any other indicators related to that attack.

Respond

Schools need a response plan, headed by a team of people with specifically identified functions and responsibilities.

Recover

This phase involves developing and implementing systems and plans to restore data and services that may have been affected during a cyber-attack.

1.3 Purpose of this document

This document is purposely divided into two parts. Part A is designed to help the school to focus on the arrangements and precautions required in order to develop and maintain an appropriate level of cyber security within its IT infrastructure and its day to day operations. Accordingly, Part A concentrates on the 'Identify', 'Protect' and 'Detect' pillars of cyber resilience.

[Part B](#) of this document takes the form of a Cyber Response Plan, enabling the school to consider the arrangements we will need to put in place to successfully ensure that the 'Respond' and 'Recover' pillars of cyber resilience are effectively addressed.

The document has been designed this way so that Part B can be utilised independently of Part A in the event of a cyber-attack on the school. Part B contains a number of templates for forms and aide- mémoires which can be utilised by the Cyber Recovery Team to help manage the school's response to a cyber-attack.

2. Preventative strategies

It is vital that we understand our vulnerabilities and regularly review our existing defences and take the necessary steps to protect our networks. As well as having a current and cohesive Cyber Response Plan in place, there are several measures that we can implement to help to improve our IT security and mitigate the risk of a cyber-attack. These measures fall under the 'Identify, Protect and Detect' pillars of effective cyber resilience and are outlined below.

2.1 Identify

In order to identify our vulnerabilities, we must understand not only the hardware and software components which make up our IT infrastructure and networks, but also the types of threats that these components may be exposed to. In order to achieve this we will, in conjunction with our IT provider(s), implement the following measures:

- i. Maintain an up to date inventory of **all** IT hardware and software utilised by the school in our day to day operations.
- ii. Maintain an up to date inventory of **all** information/data sets to which the school has access (see [Checklist D](#)). Include an evaluation of the level of sensitivity, vulnerability and risk tolerance associated with individual information/data sets and understand which are critical to business continuity in the event of a cyber-attack.
- iii. Regularly review our IT Security Policy and Data Protection Policy and procedures to ensure they remain current and stay abreast of developments and emerging threats in relation to IT security.
- iv. Assess the school's current security measures against [Cyber Essentials](#) requirements such as firewall rules, secure device configuration, security update management, user access control and malware protection. [Cyber Essentials](#) is a government-backed baseline standard, which we will strive towards achieving wherever possible.

2.2 Protect

Once we properly understand the scope of our IT infrastructure, we can ensure that appropriate protection measures are developed and implemented with the aim of mitigating or reducing our level of vulnerability. In order to achieve this we will follow the guidance for '[meeting digital and technology standards in schools and colleges](#)' set out by the Department for Education (DfE) and ensure, in conjunction with our IT partner(s) where appropriate, that the following safeguards are in place:

- i. All devices on every school network are protected with a properly configured boundary or software firewall.
- ii. All devices that can access the school's network are known and recorded with their security features enabled, correctly configured and kept up to date.
- iii. Account holders only have the access they require to perform their role and will be authenticated to access data and services.
- iv. Account holders with access to personal or sensitive operational data and functions are protected by multi-factor authentication (a method of confirming a user's identity by using a combination of two or more different factors).

- v. Anti-malware software is used to protect all devices in the network, including cloud-based networks
- vi. An administrator will check the security of all applications downloaded onto a network.
- vii. All online devices and software must be licensed for use and will be patched with the latest security updates.
- viii. We will have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 of which will be off-site and at least 1 will be offline at any given time. Backups will be tested regularly to ensure that services can be restored, and data recovered from them.
- ix. Our school Emergency Plan will include a regularly tested contingency plan in response to a cyber-attack – our ‘Cyber Response Plan’ – designed to be implemented by a team of people with specifically identified functions and responsibilities in the event of a cyber-attack. We will communicate the Cyber Response Plan to all those who are likely to be affected and will inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.
- x. We will ensure that the measures which we have in place comply with the requirements of our insurers.
- xi. We will report any suspicious cyber incident to the relevant agency. This may include [Action Fraud](#), the [DfE sector cyber team](#), the [Information Commissioners Office \(ICO\)](#), and the [NCSC](#), depending upon the type and seriousness of the incident.
- xii. We will conduct a Data Protection Impact Assessment by statute for personal data we hold as required by the UK General Data Protection Regulation (UK GDPR).
- xiii. Employees or Governors who have access to the school’s IT system may undertake [NCSC Cyber Security Training](#). If staff choose to complete, a certificate will be downloaded by each person, a copy of which will be held centrally by the school.
- xiv. We will make use of the extensive range of free practical resources available on the [NCSC website](#) to help improve Cyber Security within our school. These include the following topics:
 - [Cyber security in schools: questions for governors and trustees](#)
 - [Cyber security toolkit for boards](#)
 - [Cyber security training for school staff](#)
 - [Early Years practitioners: using cyber security to protect your settings](#)
 - [Resources for schools](#)
- xv. We can also access a range of support from the [North West Cyber Resilience Centre \(NWCRC\)](#). They offer a range of paid for services including security awareness training and website vulnerability assessments but will also provide free advice to schools.
- xvi. We will make staff aware that if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the Police.

2.3 Detect

Early detection of cyber threats can help to significantly mitigate the impact upon our IT infrastructure and help preserve the continuity of business functions through the timely

deployment of counter measures and our response plan. The following measures will help us to identify threats at an early stage and initiate a timely response:

- i. Installation and regular updating of anti-malware software will help to detect and mitigate the effects of a cyber-attack.
- ii. Delivery of cyber security training to all staff and Governors will serve to heighten their awareness of cyber threats and help them to identify and understand the importance of reporting potential security breaches immediately.
- iii. We will use the [NCSC Exercise in a Box](#) toolkit to help our staff understand what a cyber-attack might look like and to test our response plans to identify any weaknesses.
- iv. We will register with [Police CyberAlarm](#). Registering will connect our school with the local police cyber protect team and should allow a cyber-alarm software tool to be installed for free to monitor cyber activity. The tool, when installed, will record traffic on the network without risk to personal data.
- v. As soon as an attack is detected we will:
 - work with our IT partner(s) to evaluate the affected system(s) and continuously monitor them in order to identify any other indicators related to the attack.
 - Initiate our Cyber Response Plan and convene our cyber recovery team to ensure that we effectively deliver the 'Respond' and 'Recover' pillars of our cyber resilience strategy. [SEE PART B – CYBER RESPONSE PLAN](#)

PART B - CYBER RESPONSE PLAN

1. Introduction

This Cyber Response Plan has been developed and is required in order to ensure that we maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard following a cyber-attack. The Cyber Response Plan will cover all essential and critical IT infrastructure, systems, and networks.

1.1 Aims of the Cyber Response Plan

The aim of our Cyber Response Plan is to ensure that we can effectively deliver the 'Respond' and 'Recover' pillars of our cyber security strategy in the event of a cyber-attack. The plan will enable school staff and key stakeholders to have a clear understanding of who should be contacted, and the actions necessary to minimise disruption and facilitate a recovery to normal business functioning.

Within the Plan we have 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 we would be able to function without each one. We have also established plans for internal and external communications and have 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;
- enable prompt internal reporting and recording of incidents;
- have immediate access to all relevant contact details (including backup services and IT technical support staff);
- maintain the welfare of pupils and staff;

- minimise disruption to the functioning of the school;
- ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity;
- restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected;
- report cyber incidents to the relevant authorities.

2. Response and Recovery

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.

2.1 Respond - Actions in the event of an incident

Where we suspect, or are informed by others, that we have been the victim of a ransomware or other cyber incident, we will take the following steps immediately:

1. Convene the Cyber Recovery Team.
2. Verify the initial incident report as genuine and record on the [Incident Recovery Event Recording Form](#) at Appendix C.
3. 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.
4. Start the [Actions Log](#) to record actions taken.
5. Contact our insurance provider for further advice and guidance regarding assistance which they can provide.
6. In the event of a suspected cyber-attack, our IT partner(s) will be asked to isolate devices from the network.
7. In order to assist subsequent data recovery, if damage to a computer or back up material is suspected, we will ensure that staff **do 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.
8. Make a decision as to the safety of the school remaining open.
 - *This will be in liaison with relevant Local Authority Support Services/Trust*
9. Identify legal obligations and any required statutory reporting e.g. criminal acts/reports to the [Information Commissioner's Office](#) in the event of a data breach.
 - *This may involve the school's Data Protection Officer and the Police*
10. Execute the [communication](#) strategy which should include a media/press release if applicable.
 - *Communications with staff, governors and parents/pupils should follow in that order, prior to the media release.*
11. Contact the local Police via the [Action Fraud website](#) or call **0300 123 2040**.
12. Contact our Data Protection Officer.

2.2 Recover - Restoring data and services

When we are sure that the initial threat has been contained and either quarantined or removed, we will begin the process of restoring normality to our business functions as far as practicable. To help facilitate this we will undertake the following actions:

1. Continue to liaise with our insurance provider for advice and guidance.
2. Agree a process with our IT partner(s) for safely restoring any systems/databases which have been affected.
3. Maintain the [Actions Log](#) to record recovery steps and monitor progress.
4. Maintain a dialogue with our IT partner(s) to estimate the recovery time and likely impact.
5. Keep stakeholders informed of progress and likely timescales.

2.3 Post Incident Evaluation

Upon completion of the 'Respond' and 'Recover' processes we will evaluate the effectiveness of the response using the [Post Incident Evaluation](#) at Appendix D and review the Cyber Response Plan accordingly.

In particular we will consider if there was any information/data which would have significantly helped our response, but which was difficult or impossible to obtain. We will plan to gather this information/data ahead of any future attacks.

We will communicate the evaluation findings to staff and key stakeholders to ensure that relevant learning is disseminated appropriately.

We will ensure that the Cyber Response Plan is kept up to date with new suppliers, new contact details, and any changes to policy as appropriate.

Checklist A – Key People

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	Louise Lyons	Office Manager	admin@leeshill.cumbria.sch.uk
Data Management	Sensible Solution	IT Consultants	vsupport@sitscloud.co.uk
IT Restore / Recover	Sensible Solutions	IT Consultant	vsupport@sitscloud.co.uk
Site Security	Lynn Rooney	Head Teacher	head@leeshill.cumbria.sch.uk
Communications	Lynn Rooney	Head Teacher	head@leeshill.cumbria.sch.uk

Server Admin Access

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

Role	Name	Contact Details
Head teacher	Lynn Rooney	0169772577
Office Manager	Louise Lyons	0169772577
IT Support Technician	Sensible Solutions	01228212010

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Head teacher	Lynn Rooney	head@leeshill.cumbria.sch.uk
Office Manager	Louise Lyons	admin@leeshill.cumbria.sch.uk

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

Checklist B - Key Roles and Responsibilities

Every school is unique and the structure and staffing levels will determine who will be assigned which task. We have used the following checklist to assist us to assign roles and responsibilities. This is not an exhaustive or a definitive list.

Head Teacher (DSL)

- 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.
- Ensures site access for external IT staff.
- 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.

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 – Insurance provider / 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 Head teacher / 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 Head teacher 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 Provider

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 insurance provider technical support team 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 Head teacher 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](#)
 - Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed.

Incident Impact Assessment

Understanding the type and severity of an incident allows you to determine how urgent your response is. It also enables you ensure that the correct people are involved from the outset. Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	No Impact	There is no noticeable impact on the school's ability to function.
	Minor Impact	There is some loss in the ability to function which is minor. Functions can be carried out but may take longer and there is a loss of efficiency.
	Medium Impact	The school has lost the ability to provide some critical services (administration or teaching and learning) to some users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
	High Impact	The school can no longer provide any critical services to users. It is likely the school will close or disruption will be considerable.

Informational	No Breach	No information has been accessed/compromised or lost.
	Data Breach	Access or loss of data which is not linked to individuals and classed as personal. This may include school action plans, lesson planning, policies and meeting notes.
	Personal Data Breach	Sensitive personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the person/people concerned requires a report to the ICO within 72 hours.
	Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. (This also includes corruption of data)

Restoration	Existing Resources	Recovery can be promptly facilitated with the resources which are readily available to the school.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.

Communication Templates

1. School Open (notification to parent/carer)

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 / UK 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 (notification to parent/carer)

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 / UK 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 [XXXX]. We are currently planning that the school will be open as normal on [XXXX].

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 (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 / UK 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 (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 / UK 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 / UK 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.

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.

1. Incident Details

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?	
------------------------------------	--

2. Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

3. Actions Log

Recovery Tasks (In order of completion)	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

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:		