

**Disaster Recovery Procedure and Plan**

 [Insert School Name]

[Version]

|  |  |
| --- | --- |
| **Last Reviewed** |  |
| **Reviewed By** |  |
| **Next Review Date** |  |

**Contents**

[**1.1** **Introduction** 4](#_Toc52464796)

[**1.2** **Scope** 4](#_Toc52464797)

[**1.3** **Aims** 5](#_Toc52464798)

[**1.4** **Objectives** 5](#_Toc52464799)

[**1.5** **Preparation** 6](#_Toc52464800)

[1.5.1 Preventative Strategies 6](#_Toc52464801)

[1.5.2 Acceptable Use 6](#_Toc52464802)

[1.5.3 Communicating the Plan 6](#_Toc52464803)

[1.5.4 Testing and Review 6](#_Toc52464804)

[1.5.5 Making Templates Readily Available 6](#_Toc52464805)

 [**1.6** **IT Disaster Recovery Team and Access Rights** 7](#_Toc52464806)

[1.6.1 Server Access 7](#_Toc52464807)

[1.6.2 MIS Admin Access 7](#_Toc52464808)

[**1.7** **Backup Strategy** 8](#_Toc52464809)

[**1.8**  **Key Contacts** 8](#_Toc52464810)

[**1.9** **Disaster Recovery Plan** 9](#_Toc52464811)

[**1.10** **Data Recovery** 9](#_Toc52464812)

[**1.12** **Insurance** 12](#_Toc52464813)

[**1.13** **Staff Media Contact** 12](#_Toc52464814)

[**1.14** **Critical Activities - Data Assets** 13](#_Toc52464815)

[**1.15** **Contact List and Notification Calling Tree** 15](#_Toc52464816)

**Appendices**

[**A.1.** **Incident Impact Assessment** 16](#_Toc52464817)

[**A.2.** **Risk Management**  17](#_Toc52464818)

[**A.3.** **Communication Templates** 18](#_Toc52464819)

[A.3.1 School Open 18](#_Toc52464820)

[A.3.2 School Closure 19](#_Toc52464821)

[A.3.3 Staff Statement Open 20](#_Toc52464822)

[A.3.4 Staff Statement Closed 21](#_Toc52464823)

[A.3.5 Media Statement 22](#_Toc52464824)

[A.3.6 Standard Response 22](#_Toc52464825)

[A.3.7 Standard response for pupils 22](#_Toc52464826)

[**A.4** **Disaster Recovery Event Recording Form** 23](#_Toc52464827)

[1.18.1 Relevant Referrals 23](#_Toc52464828)

[1.18.2 Actions Log 23](#_Toc52464829)

[**A.5** **Post Incident Evaluation** 24](#_Toc52464830)

# **1.1 Introduction**

An IT Disaster Recovery Plan forms part of the overall continuity plan that schools need to ensure they maintain a minimum level of functionality to safeguard pupils and staff, and restore the school back to an operational standard.

If a 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 Disaster Recovery Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.

The plan should cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating disaster recovery. It is also important that the plan is well communicated and readily available.

***It is important that this procedure is understood by key stakeholders, and the plan is followed as closely and promptly as possible. This prevents inappropriate, incorrect, or unilateral decisions.***

***If the incident involves legal action, a well-documented and formulated response to the incident may need to be verified by more than one person.***

# **1.2 Scope**

This policy is to ensure that in the event of an IT disaster such as fire, flood, acts of vandalism, terrorism, malicious cyber-attack, or hardware / software failure, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

This policy covers incidents which directly affect IT systems only. As such, this IT Disaster Recovery Plan will form part of a wider Critical Incident Response Plan.

# **1.3 Aims**

1. To manage and respond to unexpected, disruptive IT events.
2. To safeguard the staff, pupils, and school.
3. To minimise disruption to the functioning of the school.
4. To enable normal working to be resumed in the shortest possible time.

# **1.4 Objectives**

* To enable prompt internal reporting and recording of incidents.
* To maintain the welfare of pupils and staff.
* To identify the nature of any threat and assess whether there is a safeguarding concern / immediate threat to individuals.
* To promptly assess whether there is a criminal aspect to the incident, and if so, to report to the police.
* To have immediate access to all relevant contact details (including backup services and IT technical support staff).
* To ensure immediate and appropriate action is taken in the event of an IT incident, or a disaster affecting the IT system.
* To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.
* To inform the [Disaster Recovery Team](#_IT_Disaster_Recovery), the membership of which is known to all relevant parties. (This may be the same as Critical Incident Team)
* To have in place an up-to-date IT Incident / [Disaster Recovery Plan](#_Disaster_Recovery_Plan), the details of which are familiar to all relevant parties.
* To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.
* To acknowledge the additional demands placed upon staff members, and where appropriate and applicable, to offer support during incident handling and subsequent recovery.

# **1.5 Preparation**

## **1.5.1 Preventative Strategies**

1. Regularly review relevant policies e.g. IT Security Policy, Data Protection Policy, Health and Safety.
2. Assess the school’s current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access.
3. Routinely install security and system updates.
4. Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

## **1.5.2 Acceptable Use**

Ensure 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.

## **1.5.3 Communicating the Plan**

Communicate the Disaster Recovery Plan to all those who are likely to be affected, and be sure to inform key staff of their roles and responsibilities in the event of an incident, *prior* to any issue arising.

## **1.5.4 Testing and Review**

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

Train key staff members to feel confident following and implementing the plan. Review the plan regularly to ensure contact details are up-to-date and new systems have been included.

## **1.5.5 Making Templates Readily Available**

It is recommended that templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

# **1.6 IT Disaster Recovery Team and Access Rights**

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Name | Role in School | Contact Details |
| Recovery Team Leader |  |  |  |
| Data Management |  |  |  |
| IT Restore / Recover |  |  |  |
| Site Security |  |  |  |
| Public Relations |  |  |  |
| Communications |  |  |  |
| Resources / Supplies |  |  |  |
| Facilities Management |  |  |  |

This procedure should not be published with contact details included.

It may be preferential to append contact information.

## **1.6.1 Server Access**

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

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

## **1.6.2 MIS Admin Access**

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

|  |  |  |
| --- | --- | --- |
| MIS Admin Access | Name | Contact Details |
| Headteacher |  |  |
| School Business Manager |  |  |
| MIS Provider |  |  |
| Data Manager |  |  |

In the event of an incident it may be helpful to consider how you would access the following:

* Registers
* Staff / Pupil contact details
* Current Child Protection Concerns
* Fire risk assessment and register of chemicals and substances retained on site

# **1.7 Backup Strategy**

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

# **1.8 Key Contacts**

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

# **1.9 Disaster Recovery Plan**

This is a suggested order for the Disaster Recovery Plan. It is likely that some steps may naturally change order or occur simultaneously as the team work together to ensure a swift response.

1. Verify the initial incident report as genuine and accurate.
2. Assess and document the scope of the incident.
	* + *Which key functions are operational / which are affected?*
3. Start the [Actions Log](#_Actions_Log) to record recovery steps and monitor progress.
4. Convene the [Disaster Recovery Team](#_1.6_IT_Disaster) (DRT).
5. Liaise with IT staff to estimate the recovery time and likely impact.
6. Make a decision as to the safety of the school remaining open.
	* + *This will be in liaison with relevant Local Authority Support Services / Trust*
7. 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*
8. Execute the [communication](#_1.17_Communication_Templates) 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.*
9. Identify what can be salvaged (physical and virtual assets) and where there are crucial gaps that take priority.
10. Implement contingency plans e.g. possible workarounds such as remote learning / combining office spaces.
11. IT support staff to continue restoring and facilitating alternative services as required.
12. Document any losses and damages.
13. Contact insurers and file insurance claims, as necessary.
14. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
15. Upon completion of the process, evaluate the effectiveness of the response and review the Disaster Recovery Plan accordingly.
16. Educate employees on avoiding similar incidents / implement lessons learned.

**Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.**

# **1.10 Data Recovery**

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.

In the event of a suspected cyber-attack, IT staff should isolate devices from the network.

**1.11 Key Roles and Responsibilities**

**Every school is unique and the structure and staffing levels will determine who will be assigned which task. This example will help you assign roles and responsibilities, but this is not an exhaustive or a definitive list.**

**Headteacher / Principal (with support from Deputy Head / Vice Principal)**

* Seeks clarification from person notifying of incident.
* Calls emergency services if appropriate.
* Sets up and maintains an incident log, including dates / times and actions.
* Convenes the Disaster Recovery Team (DRT) to inform of incident and enact the plan.
* Liaises with the Chair of Governors.
* Liaises with the school Data Protection Officer.
* Convenes and informs staff, advising them to follow the ‘script’ when discussing the incident.
* Prepares relevant statements / letters for the media, parents / pupils.
* Liaises with School Business Officer / Manager to contact parents, if required, as necessary

**DSL**

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

**Site Manager / Caretaker**

* Assesses the security of the site (may need to prevent access to certain areas of the school and / or put additional security in place).
* Ensures site access for emergency services and external IT staff.
* Liaises with the Headteacher to ensure access is limited to essential personnel.
* Ensures health and safety measures are in place.
* Supports any required risk assessments.
* Supports the salvage of any equipment which can be saved.
* Liaises with any insurance assessor and starts an inventory of damaged equipment.

**School Business Officer / Manager**

* Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
* Ensures office staff understand the [standard response](#_Standard_Response) and knows who the media contact within school is.
* Contacts relevant external agencies – IT services / technical support staff / insurers.
* Manages the communications, website / texts to parents / school emails.
* Assesses whether payroll or HR functions are affected and considers if additional support is required.

**Data Protection Officer (DPO)**

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

**Chair of Governors**

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

**IT Lead / IT Staff**

**Depending upon whether the school has internal or outsourced IT provision, the roles for IT Co-ordinators and technical support staff will differ.**

* Verifies the most recent and successful backup.
* Assesses whether the backup can be restored or if server(s) themselves are damaged.
* Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase.
* Provides an estimate of any downtime and advises which systems are affected / unaffected.
* If necessary, arranges for access to the off-site backup.
* Protects any records which have not been affected.
* Ensures on-going access to unaffected records.
* Restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.

**Teaching Staff and Teaching Assistants**

* Reassure pupils, staying within agreed [pupil standard response](#_Standard_response_for)
* Record any relevant information which pupils may provide.
* Ensure any temporary procedures for data storage / IT access are followed.
* Ensure a return to normal working practices once temporary arrangements are superseded.

# **1.12 Insurance**

As part of the company’s disaster recovery and business continuity strategies, contact with the school insurers is essential.

There may be omissions, liability clauses and other requirements which, if not met, could invalidate any cover.

Insurance contacts

Business hours, please contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Out of hours, please contact:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Location of policy: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Policy** **Name** | **Coverage** **Type** | **Coverage** **Period** | **Amount** **Of** **Coverage** | **Known Exemptions** | **Next** **Renewal** **Date** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **1.13 Staff Media Contact**

Assigned staff will coordinate with the media, working to guidelines that have been previously approved (for example as detailed in your Critical Incident Plan) 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Role:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **1.14 Critical Activities - Data Assets**

List all the data assets your school has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month.

Complete the required column with the timescale you believe is necessary for recovery. You may find it helpful to refer to your Inventory / Data Map.

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

Also decide if there are any temporary workarounds or if outsourcing is possible. It is useful to consider the cost of any additional resources which may be required in an emergency situation.

|  |  |  |  |
| --- | --- | --- | --- |
| **Critical Activities** | **Data item required for service continuity** | **When Required** | **Workaround? (Yes / No)** |
| Leadership and Management | Access to Headteacher’s email address |  |   |
| Minutes of SLT meetings and agendas |  |   |
| Head's reports to governors (past and present) |  |   |
| Key stage, departmental and class information |  |   |
| Safeguarding / Welfare | Access to systems which report and record safeguarding concerns |  |   |
| Attendance registers  |  |   |
| Class groups / teaching groups, and staff timetables |  |   |
| Referral information / outside agency / TAFs |  |   |
| Child protection records  |  |   |
| Looked After Children (LAC) records / PEPs |  |   |
| Pupil Premium pupils and funding allocations |  |  |
| Pastoral records and welfare information |  |   |
| Medical | Access to medical conditions information |  |   |
| Administration of Medicines Record |  |   |
| First Aid / Accident Logs |  |   |
| Teaching | Schemes of work, lesson plans and objectives |  |   |
| Seating plans |  |   |
| Teaching resources, such as worksheets |  |   |
| Learning platform / online homework platform |  |   |
| Curriculum learning apps and online resources |  |   |
| CPD / staff training records  |  |   |
| Pupil reports and parental communications |  |   |
| SEND Data | SEND List and records of provision |  |   |
| Accessibility tools |  |   |
| Access arrangements and adjustments |  |   |
| IEPs / EHCPs / GRIPS |  |   |
| Conduct and Behaviour | Reward system records, including house points or conduct points |  |   |
| Behaviour system records, including negative behaviour points |  |   |
| Sanctions  |  |   |
| Exclusion records, past and current |  |   |
| Behavioural observations / staff notes and incident records |  |   |
| **Critical Activities** | **Data item required for service continuity** | **When Required** | **Workaround? (Yes / No)** |
| Assessment and Exams | Exam entries and controlled assessments |  |   |
| Targets, assessment and tracking data |  |   |
| Baseline and prior attainment records |  |   |
| Exam timetables and cover provision |  |   |
| Exam results |  |   |
| Governance | School development plans  |  |   |
| Policies and procedures |  |   |
| Governors meeting dates / calendar  |  |   |
| Governor attendance and training records |  |   |
| Governors minutes and agendas |  |   |
| Administration | Admissions information |  |   |
| School to school transfers |  |   |
| Transition information |  |   |
| Contact details of pupils and parents |  |   |
| Access to absence reporting systems |  |   |
| School diary of appointments / meetings |  |   |
| Pupil timetables |  |   |
| Letters to parents / newsletters |  |   |
| Extra-curricular activity timetable and contacts for providers |  |   |
| Census records and statutory return data |  |   |
| Human Resources | Payroll systems |  |   |
| Staff attendance, absences, and reporting facilities |  |   |
| Disciplinary / grievance records |  |   |
| Staff timetables and any cover arrangements |  |   |
| Contact details of staff |  |   |
| Office Management | Photocopying / printing provision |  |   |
| Telecoms - school phones and access to answerphone messages |  |   |
| Email - access to school email systems  |  |   |
| School website and any website chat functions / contact forms |  |   |
| Social media accounts (Facebook / Twitter) |  |  |
| Management Information System (MIS) |  |   |
| School text messaging system |  |   |
| School payments system (for parents) |  |   |
| Financial Management System - access for orders / purchases |  |   |
| Site Management | Visitor sign in / sign out |  |   |
| CCTV access |  |   |
| Site maps |  |   |
| Maintenance logs, including legionella and fire records |  |   |
| Risk assessments and risk management systems |  |   |
| COSHH register and asbestos register |  |   |
| Catering | Contact information for catering staff  |  |   |
| Supplier contact details |  |   |
| Payment records for food & drink |  |   |
| Special dietary requirements / allergies |  |   |
| Stock taking and orders |  |   |

# **1.15 Contact List and Notification Calling Tree**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Optional contacts |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |   |  |  |  |  | Notifying Person |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |   |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |   |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Headteacher |  |  |  |  |  |  |  |  |  |  |  |
|  |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |
|  |   |  |  |   |  |   |   |  | Police  (if required) |  |   |  |  |  |  |  |  |
|  |   |  |  |   |  |   |   |  |  |  |  |   |  |  |  |  |  |  |
| Chair of Governors |  | DSL (If not Headteacher) |  | Data Protection Officer |  |  |  |  | School Business Manager |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|   |   |  |  |   |  |  |   |  |  |  |  |   |  |  |  |  |  |  |
|   |   |  |  |   |  |  |   |  |  |   |   |   |   |   |   |  |  |  |
| Clerk to Governors |  | Other agencies as required |  | Refer to ICO as required. |  | IT Technician |  | Site Manager / Caretaker |  | Relevant Suppliers |  |  |
|  |  |  |  |  |  |  |
|   |   |  |  |  |  |  |  |  |  |   |  |  |  |  |  |  |  |  |
|   |   |  |  |  |  |  |  |  | Third party IT provision |  |  |  |  |  |  | Insurers |
| Governing Board |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Appendix 1**

# **A.1. Incident Impact Assessment**

|  |  |  |
| --- | --- | --- |
| **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. |

**Appendix 2**

# **A.2. Risk Management** (This is a sample assessment and should be reviewed by the school)

|  |  |  |  |
| --- | --- | --- | --- |
|  | 1 = Very High | 1 = Severe |  |
|  | 5 = Very Low | 5 = Minor |  |
| Disaster Scenario | Probability Rating | Impact Rating | Mitigations / Alternative Actions |
| Flood | 3 | 4 | Ensure servers are not located on the floor. Site servers and other computers as far away from water pipes as possible. Moisture detectors can be deployed to provide limited early warning. |
| Fire | 4 | 2 | Ensure there is an off-site backup. Keep server spaces well maintained, well ventilated and free from dust.Be aware that cabling / trunking can cause fires in other parts of the building to spread quickly to computer rooms. |
| Vandalism | 3 | 4 | CCTV used to deter and detect vandalism. Site security should include locks and physically restrict server access. Keys to server rooms should be individual and not generic to a whole department / suite of rooms. |
| Power Failure | 3 | 3 | UPS remote monitoring and available redundant UPS. |
| Cyber-Attack | 3 | 3 | Check backup rotations, install security updates, and monitor anti-virus and malware solutions. Strong filtering also protects the end users. |
| Loss of Communication / Network Services | 4 | 3 | WAN redundancy, voice network resilience and using diversely / alternatively routed trunks for telecoms connections can limit likely communication loss. |
| Loss of Building Access | 4 | 2 | Arrangement with another school or site to utilise their facilities can support critical systems in the event that school buildings can't be accessed. Also utilise cloud solutions to continue to provide education to pupils and communicate with staff. |

**Appendix 3**

# **A.3. Communication Templates**

## **A.3.1 School Open**

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / fire / flood / serious system outage]. This has taken down [some / all] of the school IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc] At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems]

We are in liaison with our school Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR. Every action has been taken to minimise disruption and data loss.

The school will be working with the [Trust / Local Authority], IT providers and other relevant third-parties [Health and Safety / NCSC / Derbyshire 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,

## **A.3.2 School Closure**

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / fire / flood / serious system outage]. This has taken down the school IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc]. At present we have no indication of how long it will take to restore our systems.

We are in liaison with our school Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / GDPR.

In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff.

I feel that we have no option other than to close the school to students on [XXXXXXXXXX]. We are currently planning that the school will be open as normal on [XXXXXXXXXX]

I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience, but feel that we have no option other than to take this course of action.

The school will be working with the [Trust / Local Authority], IT providers and other relevant third-parties [Health and Safety / NCSC / Derbyshire 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,

## **A.3.3 Staff Statement Open**

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

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will remain open with the following changes to working practice:

(Detail any workarounds / changes)

The school is in contact with our Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, limit severity, and restore systems.

All staff are reminded that they must not make any comment or statement to the press, parents or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name]

## **A.3.4 Staff Statement Closed**

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

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will close to pupils [on DATE or with immediate effect].

(Detail staff expectations and any workarounds / changes or remote learning provision)

The school is in contact with our Data Protection Officer and we have reported the incident to the ICO, in line with the statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].

All staff are reminded that they must not make any comment or statement to the press, parents, or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name].

## **A.3.5 Media Statement**

[Inset school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the [Trust / LA] the school [will remain open / is currently closed] to pupils.

The school is in contact with their Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities and the school has taken immediate remedial action to limit data loss and restore systems.

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the school in initial media responses.

## **A.3.6 Standard Response - Parents**

The information provided should be factual and include:

* Time / date of the incident
* Brief nature of the incident (fire, theft, flood, cyber-attack).

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.

## **A.3.7 Standard Response - 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 4**

# **A.4 Disaster Recovery Event Recording Form**

This form can be used to record all key events completed whilst following the stages of the Disaster Recovery Plan.

|  |  |
| --- | --- |
| **Description** **or reference of disaster:** |  |
| **Date of the incident:** |  |
| **Date of the incident report:** |  |
| **Date/time** **disaster recovery commenced:** |  |
| **Date recovery work was completed:** |  |
| **Was full recovery achieved?** |  |

## **1.18.1 Relevant Referrals**

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

## **1.18.2 Actions Log**

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

**Appendix 5**

# **A.5 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  |  |  |
| Coordination of the Disaster 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: |