**Cyber Response Plan for**

**(Insert name of school)**

|  |  |
| --- | --- |
| DfES Number |  |
| Plan Created Date |  |
| Last Reviewed Date |  |
| Reviewed By |  |
| Next Review Date |  |

**The document containing contact information should be restricted and only shared with the individuals named in the school’s Cyber Recovery Team.**

**A copy of this document should be printed out in hard copy and secured somewhere safe.**

# Cyber Recovery Team

In the event of this plan having to be initiated, the personnel named below will form the school’s Cyber Recovery Team and manage the incident. This group will determine all actions that are needed to manage the incident; the timescales for these; third parties that need to be involved; frequency of meetings; and how any information will be communicated to the school and wider community.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Name | Role in School | 24-hour Contact Details |
| Cyber Recovery Team Leader / Meeting Chair |  |  |  |
| Cyber Incident Response Company \* |  |  |  |
| Headteacher or designated member of SLT |  |  |  |
| School’s Cyber Lead |  |  |  |
| IT provider / partner |  |  |  |
| LA Civil Contingencies / Major Incident Manager |  |  |  |
| LA Data Protection Officer |  |  |  |
| LA Press/PR/ Communications Officer |  |  |  |
| School Business Manager or School Support Officer |  |  |  |
| Administrator – to record minutes and actions |  |  |  |

\* Your school might want to identify an incident response company in advance of any actual incident taking place https://www.ncsc.gov.uk/schemes/cyber-incident-response/introduction

If the extent of the cyber incident gives concerns about opening the school, any decision to close the school can only be made by the Chair of Governors after consideration of advice from the Headteacher.

# Infrastructure, Comms Room, Server, and Cloud Storage Access

In the event of this plan having to be initiated, the personnel named below may need to be contacted to provide administrative access to the school’s digital infrastructure, comms rooms, server or cloud storage solutions.

|  |  |  |
| --- | --- | --- |
| Role | Name | 24-hr Contact Details |
| Headteacher or designated member of SLT |  |  |
| School Business Manager or School Support Officer |  |  |
| IT Provider |  |  |
| Third Party IT Provider |  |  |
| Site Manager or Key Holder |  |  |

# Management Information System (MIS) Admin Access

In the event of this plan having to be initiated, the personnel named below will provide administrative access to the school’s MIS:

|  |  |  |
| --- | --- | --- |
| MIS Admin Access | Name | Contact Details |
| Headteacher |  |  |
| School Business Manager or School Support Officer |  |  |
| MIS Provider |  |  |
| LA MIS Link Officer |  |  |
| Third Party IT Provider |  |  |
| Data Manager |  |  |

# Other Key Contacts

In the event of this plan having to be initiated, the individuals and organisations named below are key business continuity contacts for the school. It is important to make sure everyone knows their responsibilities and has agreed to work together.

|  |  |  |
| --- | --- | --- |
| Supplier | 24-hr Contact (Tel Number) | Account / Reference Number (if applicable) |
| Internet provider |  |  |
| Internal network provider |  |  |
| Backup provider |  |  |
| Telephony provider |  |  |
| Website host |  |  |
| CCTV supplier |  |  |
| Electricity supplier |  |  |
| Intruder alarm provider |  |  |
| Text messaging system |  |  |
| Action Fraud |  |  |
| NCSC |  |  |
| School Designated Safeguarding Person (DSP) |  |  |
| Local Authority Safeguarding Lead |  |  |
| Education Closures |  |  |
| Local Police |  |  |
| Fire Officer |  |  |
| Regional Organised Crime Unit |  |  |
| School catering provider |  |  |
| Fire alarm provider |  |  |
| Lift alarm provider |  |  |
| Door entry access provider |  |  |
| Hwb contact |  |  |

# Media Contact

The local authority’s PR or Communications team will coordinate with the media. Any contact from the media made to the school itself should be redirected to the local authority’s PR or Communications team who will respond on behalf of the school. The local authority’s PR or Communications team will also draw up any press releases, media communications, or social media posts required by the school.

# Critical Information Recovery - Data Assets

The data assets the school has access to, an identification of those which are critical and how long the school is able to function without each one (4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 3 weeks / 1 month) is identified below. This information also includes temporary workarounds or if outsourcing is possible.

**\*\* (4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 3 weeks / 1 month)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Critical Activities** | **Data item required for service continuity** | **When Required \*\*** | **Workaround? (Yes / No)** |
| Leadership and Management | Access to Headteacher’s email address |  |  |
| Minutes of SLT meetings and agendas |  |  |
| Headteacher's reports to governors (past and present) |  |  |
| School self-evaluation data |  |  |
| Key stage, departmental and class information |  |  |
| Safeguarding / Welfare | Pupil records and contact information |  |  |
| Access to systems which report and record safeguarding concerns |  |  |
| Attendance registers |  |  |
| Class groups / teaching groups, and staff timetables |  |  |
| Referral information / outside agency support and involvement |  |  |
| Child protection records |  |  |
| Looked After Children (CLA) records / PEPs |  |  |
| Pupils who are eligible for free school meals (eFSM) |  |  |
| 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 |  |  |
| ALN Data | ALN list and records of provision |  |  |
| Accessibility tools |  |  |
| Access arrangements and adjustments |  |  |
| IDPs and statements where applicable |  |  |
| Conduct and Behaviour | Reward system records, including year/class/house points or conduct points |  |  |
| Behaviour system records, including negative behaviour points |  |  |
| Sanctions |  |  |
| Exclusion records, past and current |  |  |
| Records of racism and other incidents related to a protected characteristic |  |  |
| Behavioural observations / staff notes and incident records |  |  |
| 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 |  |  |
| School calendar |  |  |
| 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 |  |  |
| Arrangements for covering absent staff |  |  |
| Disciplinary / grievance records |  |  |
| Staff timetables |  |  |
| Performance Management Records |  |  |
| Contact details of staff |  |  |
| Office Management | Photocopying / printing provision |  |  |
| Telephony - 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 providers |  |  |
| School meals payment records |  |  |
| Special dietary requirements / allergies |  |  |

**To be completed at the point of a cyber incident:**

**Of these items, the most important data assets or networked services that are critical for recovery at the point of the cyber incident are:**

**1.**

**2.**

**3.**

**4.**

**5**

**Examples of Communication**

It is always helpful to have access to examples of correspondence that can be referred to when a school is managing a serious incident.

However, the following are examples only and should be adapted before use to suit the context of the school and the incident being dealt with. Included in the examples are variations in wording/terminology that the school may find useful to consider when planning how to communicate with others about any incident.

A cyber incident brings with it a risk of reputational damage. Taking this into account, any communication and correspondence must only be issued after working with the local authority PR or Communications team to draw up an agreed statement. All correspondence should be agreed by the local authority. Where appropriate, the approval of the Chair of Governors should also be sought.

## 1: Example of information that may be circulated after a confirmed cyber incident

You may be aware that the school has experienced significant issues with IT. This is because the school *has experienced an IT outage / has been part of a cyber incident*. As a result of this *IT outage / cyber incident*, some of the school’s IT systems are unavailable. This means that we do not have access to *telephones / emails / pupil data and information/school meals provision.* The school though, remains open as normal. We are uncertain about how long it will take to restore these systems and will let you know of any temporary changes that will be put in place to cover these. *[OR it is anticipated it may take XXXX to restore these systems].*

We are working with our IT provider, the local authority, police and other partners to restore functionality and help us return to normal working as soon as possible. They will help us take appropriate action to minimise disruption and address any concerns about data loss. We will also work with our Data Protection Officer to report any potential data protection breaches to the Information Commissioners Office.

In the meantime, thank you for your support; we will endeavour to keep you updated you on an ongoing basis.

## 2: Example of information that may be circulated after a confirmed cyber incident which means the school will need to be closed

You may be aware that the school has experienced significant issues with IT. This is because the school *has experienced an IT outage / has been part of a cyber incident*. As a result of this *IT outage / cyber incident* some of the school’s IT systems are unavailable. This means that we do not have access to *telephones / emails / pupil data and information/school meals provision.* We are uncertain about how long it will take to restore these systems.

As a result of this incident, we have completed a risk assessment to ensure we are still able to complete our day-to-day work. The risk assessment has identified that we are unable to appropriately safeguard our learners and staff as we are without access to key information about pupils, and some of our safety systems are not fully working. This means that we have no option other than to close the school to learners on *[XXXXXXXXXX].* I know this will cause problems for parents and carers but please be assured that we have no other option at this time. We will contact you with guidance on blended learning arrangements for pupils as soon as possible.

We are working with our IT provider, the local authority, police and other partners to restore functionality and help us re-open as soon as possible. They will also help us address any concerns about data loss. We will work with our Data Protection Officer to report any potential data protection breaches to the Information Commissioners Office.

We will continue to assess the situation and update parents and carers by the end of the day via *the local authority website/ school website/ text messaging service.*

## 3: Example of staff statement that may be circulated after a confirmed cyber incident

The school *experienced an IT outage / detected a cyber-incident* on *[date]* which has affected the following school IT systems: *(Provide a description of the services affected)*

Following discussion with the local authority and the Chair of Governors, the school will remain open with the following changes to working practice: *(Detail any workarounds / changes)*

We are working with our IT provider, the local authority, police and other partners to restore functionality and help us re-open as soon as possible. They will also help us address any concerns about data loss. We will work with our Data Protection Officer to report any potential data protection breaches to the Information Commissioners Office.

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. Staff will be regularly updated 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 the Headteacher or Deputy Headteacher who will then direct these to the Local Authority PR/Communications team for response.

## 4: Example of staff statement that may be circulated after a confirmed cyber incident and the schools is to be closed to learners

The school *experienced an IT outage / detected a cyber-incident* on *[date]* which has affected the following school IT systems: *(Provide a description of the services affected)*

Following discussion with the local authority and the Chair of Governors, the school will close to learners *[on DATE or with immediate effect].* We will contact you with further guidance on blended learning arrangements for pupils as soon as possible.

We are working with our IT provider, the local authority, police and other partners to restore functionality and help us re-open as soon as possible. They will also help us address any concerns about data loss. We will work with our Data Protection Officer to report any potential data protection breaches to the Information Commissioners Office.

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. Staff will be regularly updated 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 the Headteacher or Deputy Headteacher who will then direct these to the Local Authority PR/Communications team for response.

# Appendix 1: Incident Recovery Event Recording Form

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

|  |  |
| --- | --- |
| **Description or reference of incident:** |  |
| **Date of the incident:** |  |
| **Date of the incident report:** |  |
| **Date/time incident recovery commenced:** |  |
| **Date recovery work was completed:** |  |
| **Was full recovery achieved?** | If ‘no’ further information about this should be detailed in Appendix 2 |

## Relevant Referrals

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

## Actions Log

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Recovery Tasks**  **(*In order of completion)*** | **Person Responsible** | **Completion Date** | | **Comments** | **Outcome** |
| Estimated | Actual |
| 1. |  |  |  |  |  |
| 2. |  |  |  |  |  |
| 3. |  |  |  |  |  |
| 4. |  |  |  |  |  |
| 5. |  |  |  |  |  |
| 6. |  |  |  |  |  |
| 7. |  |  |  |  |  |
| 8. |  |  |  |  |  |
| 9. |  |  |  |  |  |
| 10. |  |  |  |  |  |

# Appendix 2: 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 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? If not, why not? |  |  |
| What are the lessons learned from this incident? |  |  |
| Log any requirements for additional training and suggested changes to policy / procedure: | | |

# Appendix 3: Breakdown of additional cyber response plan steps

## Prepare

|  |  |
| --- | --- |
| **Prepare** | |
| **Phase Objectives** | The key to minimising the impact and quickly recovering from a cyber incident is in the planning and preparation. A well-trained team has access to a comprehensive up-to-date set of documentation and with a well-managed and monitored IT estate will greatly improve the response times to a cyber incident. |
| **Activity** | **Description** |
| **Required Documentation** | Please refer to the Identifying and reducing the risks section. |

## Identify & Report

|  |  |
| --- | --- |
| **Identify & Report** | |
| **Phase Objectives** | When reporting a cyber incident, it is important to collect as much information about the incident as possible to enable the incident to be given an initial priority. This will then determine whether this classed as a cyber incident or a significant cyber incident. |
| **Activity** | **Description** |
| **Information capture** | Key information to be captured should include:   * contact information of the person reporting the incident and related parties * nature of incident * the potential impact of the incident and on what systems * description of the activity and supporting evidence e.g., logs |
| **Classify incident** | The known or possible consequences of a **significant cyber incident** can include, but are not limited to:   * life-changing impact on victim(s) * high public visibility * threat to life or vulnerable individual(s) * disruption to schools or other educational establishments * loss of sensitive data * impact on critical communications * impact on critical systems / processes required to support an emergency response (e.g., vulnerable people databases, community care services etc.) |

## Analyse / Investigate

|  |  |
| --- | --- |
| **Analyse / Investigate** | |
| **Phase Objectives** | Analysis and categorisation of cyber incidents is a fundamental step in the cyber incident response process. |
| **Activity** | **Description** |
| **Triage** | The Cyber Recovery Team will perform an initial triage and classification of all suspected cyber incidents to confirm the validity and the potential impact of the incident. The initial classification may be changed once more detailed investigation has been carried out. The initial classification should be retained so that this can be used to help refine and improve the overall incident response process.  Once an alert has been received, the cyber recovery team (as outlined in the schools Cyber Response Plan) should work with to research the event, leveraging rapid data collection and initial analysis (triage). The goal of the triage is to acquire enough pertinent preliminary information to appropriately determine both the data classification involved and the estimated severity of the incident. The team should appropriately note or close out incidents involving false-positives according to the appropriate incident-tracking procedures. |
| **Guidance** | The prioritisation of how to resource the response to the incident is a critical decision point in the process. |

## Contain

|  |  |
| --- | --- |
| **Contain** | |
| **Phase Objectives** | The cyber recovery team will take actions to contain and isolate the incident from the network. |
| **Activity** | **Description** |
| **Contain and isolate** | Containment actions may include:   * isolating a system from the network * removing users access privileges * removing users from the premises * stopping services running * isolating connections to external networks to prevent spread |

## Eradicate

|  |  |
| --- | --- |
| **Eradicate** | |
| **Phase Objectives** | Correct the incident and prevent its immediate reoccurrence.  Cyber Incident Response plan will provide the details of eradication considerations for specific attacks and should be referred to as appropriate. |
| **Activity** | **Description** |
| **Correct** | Correct the incident by addressing its symptoms (e.g., healing malware infections or correcting access). |
| **Prevent** | Prevent its immediate reoccurrence by addressing its root cause. |

## Recover

|  |  |
| --- | --- |
| **Recover** | |
| **Phase Objectives** | Actions can be taken to restore services back to the pre-incident state once the Cyber Recovery Team confirm the remediation actions have been successful. |
| **Activity** | **Description** |
| **Recovery** | The recovery actions will include the following:   * ensure impacted services are accessible again * ensure performance is in line with known (pre-attack) baseline * switch back traffic to the original network * restart stopped services |
| **Monitoring** | Monitoring of the estate should be taken to ensure any vulnerabilities have been successfully closed, action will include:   * monitor the performance/activities of the affected systems * confirm application behaviour is as expected * conduct vulnerability scan if deemed appropriate |

## Review & Learn

|  |  |
| --- | --- |
| **Review & Learn** | |
| **Phase Objectives** | A cyber incident review is important so the business can improve the systems and procedures to reduce the impact of future cyber incidents. |
| **Activity** | **Description** |
| **Report** | Details to be captured in a cyber incident report include:   * how and when the incident was initially detected * how and when the incident was initially classified * list of people notified * actions and timelines of Cyber Recovery Team * whether any internal or external escalation was required * list positive and negative points of the response to the incident * lessons identified * recommendation for improvements to policy, procedure, systems, and services * could any technical controls be implemented to prevent reoccurrence? * implementation plan for the identified improvements to the plan |

## Improve / Prevent Recurrence

|  |  |
| --- | --- |
| **Improve / Prevent Recurrence** | |
| **Phase Objectives** | Improve systems and procedures to reduce the impact of future cyber incidents |
| **Activity** | **Description** |
| **Prevent** | Following the publication of the Cyber Incident Report, the cyber recovery team shall:   * seek recipient feedback in relation to the incident report * confirm the viability of each security control. change/addition recommended in the incident report * identify the approximate cost of, and timeframe for, delivering each security control change/addition recommended in the report which appears viable (i.e., to which report recipients did not object) * identify a proposed action owner and action target date for delivering each proposed recommendation * identify the proposed funding route for each proposed recommendation that requires financial expenditure * seek endorsement of the proposed actions and associated funding routes * seek the action owner’s acceptance of the relevant actions and target dates * inform relevant stakeholders of the action plan * if action owner acceptance of the proposed actions is not forthcoming, escalate to the appropriate SIRO * review, at not less than monthly intervals, progress with each action with each action owner * notify the appropriate SIRO of any action at risk of not being delivered prior to its target date |