**Risk Protection Arrangement**

 **Cyber Response Plan**

Haybrook College Trust

 [Version1]

|  |  |
| --- | --- |
| **Last Reviewed**  |  June 2023 |
| **Reviewed By**  |  Jamie Rockman / Julia Shepard / Julian Curzon / Matthew Armsby |
| **Next Review Date**  |  June 2024 |

*This procedure should not be published outside of Haybrook College Trust with contact details included due to the risk of a data breach.*

**Contents**

[**1**. **Introduction** 3](#_Toc58153)

[**2. Aims of a Cyber Response Plan** 3](#_Toc58154)

[**3. Risk Protection Arrangement Cover** 4](#_Toc58155)

[**4. Preparation and Additional Resources** 6](#_Toc58156)

[**5. Actions in the event of an incident** 8](#_Toc58157)

[**6. Cyber Recovery Plan** 9](#_Toc58158)

[**Appendix A: Incident Impact Assessment** 17](#_Toc58159)

[**Appendix B: Communication Templates** 18](#_Toc58160)

[**Appendix C: Incident Recovery Event Recording Form** 23](#_Toc58161)

[**Appendix D: Post Incident Evaluation** 24](#_Toc58162)

# 1. Introduction

The Cyber Response Plan is considered as part of the overall continuity plan that Haybrook College (HBC) needs to ensure it maintains a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

HBC must plan effectively to ensure that recovery is not severely impacted, causing additional loss of data, time, and ultimately, reputation.

Incidents may occur during the school day or out of hours. The Cyber Response Plan 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.

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

This document is to ensure that in the event of a cyber attack, school staff have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

**What is a cyber incident**

The NCSC defines a cyber incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

**1. Attempts to gain unauthorised access to a system and/or to data.**

**2. The unauthorised use of systems for the processing or storing of data.**

**3. Changes to a systems firmware, software or hardware without the system owner’s consent.**

**4. Malicious disruption and/or denial of service.**

# 2. Aims of a Cyber Response Plan

The Cyber Response Plan will consist of a Cyber Recovery Team, and state the key roles and responsibilities of staff, what data assets are critical and how long you would be able to function without each one. It will establish plans for internal and *e*xternal communications, access registers and staff and pupil contact details. This will allow the school:

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

# 3. Risk Protection Arrangement Cover

From April 2022, the [Risk Protection Arrangement](https://www.gov.uk/guidance/the-risk-protection-arrangement-rpa-for-schools) (RPA) will include cover for Cyber Incidents, which is defined in the RPA Membership Rules as:

**“Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data.”**

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

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

1. Have offline backups. [Help and guidance on backing up](https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data) is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog [Offline backups in an online world - NCSC.GOV.UK](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)

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

* 1. Backing up the right data. Ensuring the right data is backed up is paramount. See Critical Activities for a suggested list of data to include.
	2. Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: <https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world>
	3. Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

The Trust complies with all of the above.

Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK. [https://www.ncsc.gov.uk/collection/small-businessguide/backing-your-data](https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data)

1. All Employees or Trustees who have access to the Member’s information technology system must undertake [NCSC Cyber Security Training](https://www.ncsc.gov.uk/information/cyber-security-training-schools) . Upon completion, a certificate can be downloaded by each person. In the event of a claim the Member will be required to provide this evidence. The training lasts 36 minutes on a YouTube video. This is complemented by the Cyber awareness training provided by the IT provider, BC Technologies.
2. Register with the [Police CyberAlarm](https://www.cyberalarm.police.uk/) which registers members with the local Police Cyber aware team.
3. Have a Cyber Response Plan in place.

# 4. Preparation and Additional Resources

## Preventative Strategies

Haybrook College must regularly review the existing defences to protect their networks. In addition to the 4 conditions of cover detailed above, HBC can implement other measures to improve their IT security and mitigate the risk of a cyber-attack:

* Regularly review IT Security Policy and Data Protection Policy.
* Retain a professional organisation to:
	+ Assess the school’s current security measures such as firewall rules, malware protection, and role based user access.
	+ Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user’s identity by using a combination of two or more different factors.
	+ Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis.
	+ Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible.
	+ Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
	+ Enable an account lockout policy for failed attempts
	+ The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
* Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities. Annual training in INSET or by Video.

## Acceptable Use

Ensure all users have read and signed IT acceptable use and loan agreements for school devices.

## Communicating the Plan

Communicate the Cyber Recovery Plan to all staff 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.

## 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.

Senior Leaders must ensure that there is training for 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.

# 5. Actions in the event of an incident

If HBC suspects that it has been the victim of a ransomware or other cyber incident, the following steps should be taken immediately:

* Enact your Cyber Recovery Plan
* Contact the 24/7/365 RPA Cyber Emergency Assistance:
	+ By telephone: **0800 368 6378** or by email: RPAresponse@CyberClan.com
* Contact BC technologies 01369 706656 or email support@bc-group.co.uk
* Contact your Data Protection Officer Julian Curzon dpo@haybrookcollege.co.uk, Tel 01628 353101

Once the initial incident is being dealt with the other agencies who will need to be contacted are:

* Inform the National Cyber Security Centre (NCSC) -[https://report.ncsc.gov.uk](https://report.ncsc.gov.uk/)
* Contact your local police [Action Fraud website](https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime) or call **0300 123 2040**
* Consider whether reporting to the [ICO is necessary](https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf) report at [www.ico.org.uk](http://www.ico.org.uk/) **0303 123 1112**
* Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

# 6. Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Contact BC Technologies (our IT provider) on 01369 706656 / 07764949734 / 07944379165. They will advise, basis this document (which they have reviewed), what HBC should do. The following steps will be guided by them:
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. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
5. 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.
6. Start the Actions Log to record recovery steps and monitor progress. HBC will then:
7. Convene the Cyber Recovery Team (CRT).
8. Contact RPA Emergency Assistance Helpline
9. Liaise with IT staff to estimate the recovery time and likely impact.
10. Make a decision as to the safety of the school remaining open.
11. 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.
12. Execute the communication strategy which should include a media / press release if applicable.
13. Adjust recovery timescales as time progresses and keep stakeholders informed.
14. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.
15. Educate employees on avoiding similar incidents / implement lessons learned.

## Cyber Recovery Team

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

|  |  |  |  |
| --- | --- | --- | --- |
|   | Name  | Role in School  | Contact Details  |
| Recovery Team Leader  |  Jamie Rockman |  Exec Headteacher | 07736890141 |
| Recovery Team No 2  |  Julian Curzon |  Dir of Finance | 07736889935 |
| IT Restore / Recover  | Matthew Armsby |  IT Support | 07764949734 |
| Facilities & Site Security  | Wendy Andrews |  Facilities Manager | 07867416555 |
| IT Support / Premises | Hensley Cunningham | Site Manager | 07736889907 |
| Pub Relations & Comms  |  Jamie Rockman |  Exec Headteacher | As above |

## Server Access (Emails and Print)

|  |  |  |
| --- | --- | --- |
| Role  | Name  | Contact Details  |
| Third Party IT Provider  |  Matthew Armsby |  BC Tech 07764949734 |

## Management Info System (MIS) Admin Access (Arbor, IRIS, CPOMs, EduPay)

|  |  |  |
| --- | --- | --- |
|  | Name  | Contact Details  |
| Arbor Admin Access |  |  |
| Exec Headteacher  |  Jamie Rockman |  07736890141 |
| PA to Exec Headteacher |  Suzanne Green |  07456191159 |
| Data Manager |  Jenny Tsang |  07563382204 |
| Software Company | Arbor Support  | 020 8050 2087 myteam@arbor-education.com |
| IRIS Admin Access |   |   |
| Finance Officer | Kam Randhawa | 07903236489 |
| Dir of Finance | Julian Curzon | 07736889935 |
| Software Company | IRIS Support Team |  |
| CPOMs Admin Access |  |  |
| Deputy Headteacher | Ian Johnson | 07769 290 209 |
| SENCO | Carol Goodridge | 07834 708 275 |
| Exec Headteacher | Jamie Rockman | 07736 890 141 |
| Software Company | CPOMs Support  | 01756 797 761 |
| EduPay & BPS Access |  |  |
| Dir of Finance | Julian Curzon | 07736 889 935 |
| HR and Data Manager | Jenny Tsang | 07563 382 204 |
| Software Company | Orovia (TES) | EduPay-Support@tes.com  |

It should be noted that the MIS (Arbor, IRIS, CPOMs, EduPay) are all web based and no data is held at HBC, which does mean that access can be made remotely to contact details and registers.

## Backup Strategy

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

## Key Contacts

|  |  |  |
| --- | --- | --- |
| **Supplier**  | **Contact / Tel Number**  | **Account / Ref Number**  |
| Internet Connection  |  Patrick Burke 01369706656 |  |
| Backup Provider  |  Patrick Burke 07944379165 |  |
| Telecom Provider  |  Matthew Armsby 07764949734 |  |
| Website Host  |  Matthew Armsby 07764949734 |  |
| Intruder Alarm  |  Chubb 0344 8791746 | as per confidential info. |
| Text Message System  |  Arbor 0208 050 2087 |  |
| Action Fraud  |  RPA / Police see above | N/A |
| Local Constabulary  |  Thames Valley Police 999 | N/A |
| Legal Representative  |  Winckworth Sherwood  | schoolsupport@wslaw.co.uk or 0345 070 7437 T Kerr (Partner) 07940514252 |

## Staff Media Contact

Exec Headteacher or in his absence the assigned deputy will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications.

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 Media contact.

Assigned Media Liaison(s):

Jamie Rockman Executive Headteacher

Ian Johnson Deputy Headteacher

## Key Roles and Responsibilities

**Executive Headteacher (with support from Deputy Head)**

|  |  |
| --- | --- |
|   | 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 Trustees.  |
|   | Liaises with the school Data Protection Officer.  |
|   | Convenes and informs staff, they should not respond to requests for information and advising them to follow the ‘script’ when discussing the incident.  |
|   | Liaises with Head PA / Centre Admin to contact parents, if required, as necessary. Manages the communications, website / texts to parents / school emails  |

### Designated Safeguarding Lead (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

 Ensures site access for external IT staff.

 Liaises with the Executive Headteacher to ensure access is limited to essential personnel.

### Director of Finance / Facilities 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 – RPA Emergency Assistance / IT services / technical support staff  |
|   | 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 Executive Headteacher / Chair of Trustees and determines if a report to the ICO is necessary.

 Advises on the appropriateness of any plans for temporary access / systems.

### Chair of Trustees

|  |  |
| --- | --- |
|   | Supports the Executive Headteacher throughout the process and ensure decisions are based on sound judgement and relevant advice.  |
|   | Ensures all Trustees 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 the school policy.  |

### External IT Support company

|  |  |
| --- | --- |
|   | Verifies the most recent and successful backup.  |
|   | Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.  |
|   | Liaises with the Dir of Finance as to the likely costs to reinstate services. |
|   | Provides an estimate of any downtime and advises systems status.  |
|   | 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.

 Ensures any temporary procedures for data storage / IT access are followed

## 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.

**Assign:** 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 Executive Headteacher’s email address  |  **4 hours** |  Use personal |
| Minutes of SLT meetings and agendas  |  **1 week** |  No |
| Executive Head's reports to Trustees (past and present)  |  **1 week** |  No |
| Key stage, departmental and class information  |  **1 day** |  Access Paper |
| Safeguarding / Welfare  | Access to systems which report and record safeguarding concerns  |  **1 day** |   |
| Attendance registers  |  **1 day** |   |
| Class groups / teaching groups, and staff timetables  |  **1 day** |   |
| Referral information / outside agency / TAFs  |  **1 week** |   |
| Child protection records  |  **1 day** |   |
| Looked After Children (LAC) records / PEPs  |  **1 day** |   |
| Pupil Premium pupils and funding allocations  |  **1 week** |   |
| Pastoral records and welfare information  |  **1 day** |   |
| Medical  | Access to medical conditions information  |  **1 day** |   |
| Administration of Medicines Record  |  **1 week** |   |
| First Aid / Accident Logs  |  **1 week** |   |
| Teaching  | Schemes of work, lesson plans and objectives  |  **1 day** |   |
| Seating plans  |  **1 week** |   |
| Teaching resources, such as worksheets  |  **1 day** |   |
| Learning platform / online homework platform  |  **1 week** |   |
| Curriculum learning apps and online resources  |  **1 week** |   |
| CPD / staff training records  |  **1 week** |   |
| Pupil reports and parental communications  |  **1 week** |   |
| SEND Data  | SEND List and records of provision  |  **1 day** |   |
| Accessibility tools  |  **1 week** |   |
| Access arrangements and adjustments  |  **1 week** |   |
| IEPs / EHCPs / GRIPS  |  **1 week** |   |
| Conduct and Behaviour  | Reward system records, including house points or conduct points  |  **1 week** |   |
| Behaviour system records, including negative behaviour points  |  **1 week** |   |
| Sanctions  |  **1 week** |   |
| Exclusion records, past and current  |  **1 week** |   |
| Behavioural observations / staff notes and incident records  |  **1 week** |   |
| **Critical Activities**  | **Data item required for service continuity**  | **When** **Required**  | **Workaround? (Yes / No)**  |
| Assessment and Exams  | Exam entries and controlled assessments  |  **1 week** |   |
| Targets, assessment and tracking data  |  **1 week** |   |
| Baseline and prior attainment records  |  **1 week** |   |
| Exam timetables and cover provision  |  **1 week** |   |
| Exam results  |  **1 week** |   |
| Governance  | School development plans  |  **1 week** |   |
| Policies and procedures  |  **1 week** |   |
| Trustee meeting dates / calendar  |  **1 week** |   |
| Trustee attendance and training records  |  **1 week** |   |
| Trustee minutes and agendas  |  **1 week** |   |
| Administration  | Admissions information  |  **3 days** |   |
| School to school transfers  |  **3 days** |   |
| Transition information  |  **3 days** |   |
| Contact details of pupils and parents  |  **1 day** |   |
| Access to absence reporting systems  | **3 days** |   |
| School diary of appointments / meetings  | **3 days** |   |
| Pupil timetables  | **3 days** |   |
| Letters to parents / newsletters  | **3 days** |   |
| Extra-curricular activity timetable and contacts for providers  | **3 days** |   |
| Census records and statutory return data  | **3 days** |   |
| Human Resources  | Payroll systems  |  **1 day** |   |
| Staff attendance, absences, and reporting facilities  |  **1 week** |   |
| Disciplinary / grievance records  |  **1 week** |   |
| Staff timetables and any cover arrangements  |  **1 week** |   |
| Contact details of staff  |  **1 day** |   |
| Office Management  | Photocopying / printing provision  |  **1 week** |   |
| Telecoms - school phones and access to answerphone messages  |  **1 day** |   |
| Email - access to school email systems  |  **1 day** |   |
| School website and any website chat functions / contact forms  |  **1 week** |   |
| Social media accounts (Facebook / Twitter)  |  **1 week** |   |
| Management Information System (MIS)  |  **1 day** |   |
| School text messaging system  |  **1 day** |   |
| School payments system (for parents)  |  **1 week** |   |
| Financial Management System - access for orders / purchases  |  **3 days** |   |
| Site Management  | Visitor sign in / sign out  |  **1 week** |   |
| CCTV access  |  **1 day** |   |
| Site maps  |  **1 week** |   |
| Maintenance logs, including legionella and fire records  |  **1 week** |   |
| Risk assessments and risk management systems  |  **1 week** |   |
| COSHH register and asbestos register  |  **1 week** |   |
| Catering  | Contact information for catering staff  |  **1 day** |   |
| Supplier contact details  |  **1 day** |   |
| Payment records for food & drink  |  **1 week** |   |
| Special dietary requirements / allergies  |  **1 week** |   |
| Stock taking and orders  |  **1 week** |   |

# Appendix A: Incident Impact Assessment

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

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

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

|  |  |  |
| --- | --- | --- |
| **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 B: Communication Templates

## 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 / 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 [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

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 / GDPR.

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

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

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

The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible.

We will continue to assess the situation and update parents / carers as necessary. [If possible, inform how you will update i.e. via website / text message].

Yours sincerely,

## 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]

## 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].

## 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.

**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.

# Appendix C: Incident Recovery Event Recording Form

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

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

**Relevant Referrals**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Referral To**  | **Contact Details**  | **Contacted On (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.  |   |   |   |   |   |

# Appendix D: Post Incident Evaluation

Response Grades 1-5 1 = Poor, ineffective and slow / 5 = Efficient, well communicated and effective.

|  |  |  |
| --- | --- | --- |
| **Action**  | **Response** **Grading**  | **Comments for Improvements / Amendments**  |
| Initial Incident Notification  |   |   |
| Enactment of the Action plan  |   |   |
| Co-ordination of the Cyber Recovery Team  |   |   |
| Communications Strategy  |   |   |
| Impact minimisation  |   |   |
| Backup and restore processes  |   |   |
| Were contingency plans sufficient?  |   |   |
| Staff roles assigned and carried out correctly?  |   |   |
| Timescale for resolution / restore  |   |   |
| Was full recovery achieved?  |   |   |
| Log any requirements for additional training and suggested changes to policy / procedure:        |