Cyber Incident Response Plan

Based on template from Risk Protection Arrangement

Richard Huish Trust

[v3]

Last Reviewed	08/01/2024
Reviewed By	Scott Upham / Richard Anderson
Next Review Date	08/07/2024

Contents

1. Introduction

1.1 Purpose of the Cyber Incident Response Plan

A Cyber Incident Response Plan is required to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of Richard Huish Trust Information System Resources. This adverse event may be malicious code attack, unauthorized access to Richard Huish Trust systems, unauthorized use of Richard Huish Trust services, denial of service attacks, general misuse of systems, and accidental loss or hoaxes.

1.2 General Purpose of the Cyber Incident Response Team

The purpose of the Cyber Incident Response Team is to:

- Protect Information assets.
- Provide a central organization to handle incidents.
- Comply with requirements.
- Prevent the use of systems in attacks against other systems (which could cause us to incur legal liability)
- Minimize the potential for negative exposure.

1.3 Operational Objectives of the Cyber Incident Response Team

The objectives of Cyber Incident Response Team are to:

- Limit immediate incident impact to customers and partners.
- Recover from the incident.
- Determine how the incident occurred.
- Find out how to avoid further exploitation of the same vulnerability.
- Avoid escalation and further incidents.
- Assess the impact and damage in terms of financial impact, loss of image etc.
- Update policies and procedures as needed.
- Determine who initiated the incident.
- Document all information, events, and efforts to provide to law enforcement. If an establishment fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.

Incidents may occur during the 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.

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 cyber recovery. It is also important that the plan is well communicated and readily available.

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

This will allow the college/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 college/school.
- To ensure that the college/school responds in a consistent and effective manner 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.

2. Incidents

2.1 Incident Categories

An incident will be categorized as one of four severity levels. These severity levels are based on the impact and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to our image etc. The table below provides a listing of the severity levels and a definition/description of each severity level.

Severity Level	Description
0	Incident where the impact is minimal. Examples are e-mail SPAM, isolated Virus infections, etc.
1	Incident where the impact is significant. Examples are a delayed ability to provide services, delayed delivery of critical electronic mail or data transfers, etc.
2	Incident where the impact is severe or has the potential to damage the reputation of the Trust. Examples are a disruption to the services, and/or performance of our mission functions. proprietary or confidential information has been compromised, a virus or worm has become widespread, and is affecting over 1% of employees, critical systems are unavailable.
3	Incident where the impact is catastrophic. Examples are a shutdown of all network services. Proprietary or confidential information has been compromised and published on a public site. Critical systems are unavailable. Executive management must make a public statement.

3. Responding to an incident

There are generally six stages of response:

1. Preparation—one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident **BEFORE** it occurs can save valuable time and effort in the long run.
2. Identification—identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions based on the severity.
3. Containment—involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.
4. Eradication—removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.
5. Recovery—restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.
6. Follow-up—some incidents require considerable time and effort. Often once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

Organization

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute. Figure 1 depicts the Cyber Incident Response organization.

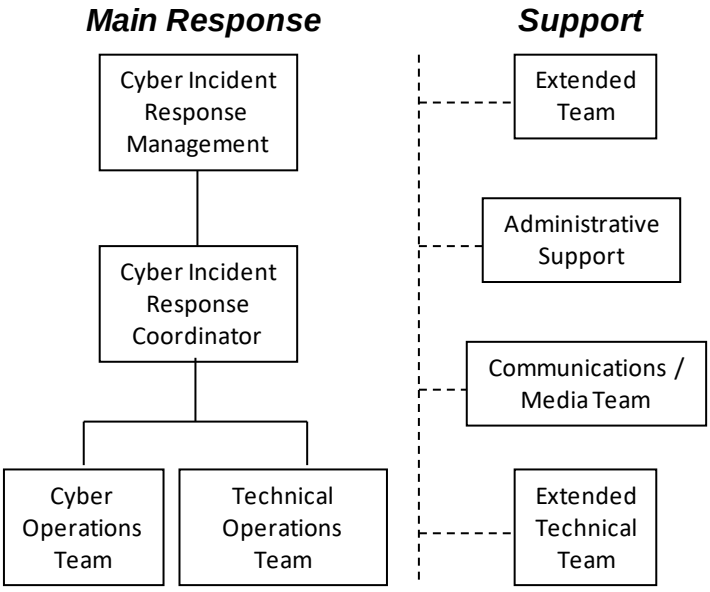

Figure 1: Cyber Incident Response Organization

3.1 Cyber Incident Response Team

Role	Responsibilities
Cyber Incident Response Management	Will have overall responsibility for directing activities regarding the incident at Severity Level 2 and above. Will serve in advisory capacity for incidents at Severity Level 1.
Cyber Incident Response Coordinator	Provides oversight to incident response. Requests resources as required to effectively contain and manage an incident response. Documents incident for purposes of law enforcement, lessons learned, and insurance.
Technical Operations Team	Provide technical aspects of incident response.
Communications Team	Responsible for internal, external and media communications. Staff Media Contact.
Extended Technical Team	Provides additional technical skill and capability to the Technical Operations team as required (i.e. outside vendor or agency)
Admin Support	Provides requested administrative support.
Extended Team	Provide additional visibility and support to incident response as required. Provide specific HR, legal, finance, etc. skills as required.

Table 1: Roles and Responsibilities

3.2 Escalation Levels

	Main Response			Support			
Severity Level	**Technical Operations Team**	**Cyber Incident Response Coordinator**	**Cyber Incident Response Mgmt.**	**Extended Technical Team**	**Comms Team**	**Admin Support**	**Extended Team**
0	X						
1	X	X	X				
2	X	X	X	X	X		
3	X	X	X	X	X	X	X

Table 2: Severity Level Matrix

The escalation process will be invoked to involve appropriate resources as the incident has more impact (severity level increases). Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. Table 3 defines the escalation levels with the associated team involvement.

Escalation Level	Affected Team(s)	Description
0	• Technical Operations Team	Normal Operations. Technical and cyber groups monitoring for alerts from various sources.
1	• Technical Operations Team • Cyber Incident Response Coordinator • Cyber Incident Response Management	Richard Huish Trust has become aware of a potential or actual threat. Determine defensive action to take. Message employees of required actions if necessary.
2	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Technical Operations Team • Extended Technical Team • Communications Team	A threat has manifested itself. Determine course of action for containment and eradication. Message employees of required actions if necessary.
3	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Extended Team • Technical Operations Team • Extended Technical Team • Communications Team • Administrative Support Team	Threat is widespread or impact is significant. Determine course of action for containment, mitigation, and eradication. Message employees. Prepare to take legal action. Prepare to make public statement.

Table 3: Escalation Levels

3.3 Escalation Considerations

Cyber Incident Response Management will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact?
- Will this affect our image negatively?

3.4 The Cyber Incident Response Process

The Cyber Incident Response Process is an escalation process whereas the impact of the incident becomes more significant or widespread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if, and when they are needed.

Section 3.5 outlines the roles and responsibilities of individual teams. Team membership is contained in Appendix A.

3.5 Cyber Incident Response Escalation Plan

3.5.1 Escalation Severity Level 0

Technical Operations Team

1. Monitors all known sources for alerts or notification of a threat.
2. Take appropriate defensive actions per known issues.
3. Escalate to Cyber Incident Coordinator if determined that Severity level may be greater than Severity Level 0.

3.5.2 Escalation Severity Level 1

Richard Huish Trust has become aware of a potential or actual threat.

Technical Operations Team

1. Determine initial defensive action required.
    a. IT staff should isolate affected devices from the network, e.g., unplug the network cable, or disable edge switches.
    b. 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.
2. Notify the Cyber Incident Coordinator.
3. Determine appropriate course of action.

Cyber Incident Coordinator

1. Receive and track all reported potential threats.
2. Verify the initial incident report as genuine.
3. Start a chronological log of events.
4. Escalate Cyber Incident Response to Severity Level 2 if a report is received indicating that the threat has manifested itself.
5. Determine relevant membership of the Technical Operations and Extended Technical teams.
6. Alert other IT personnel and applicable support organizations of the potential threat and any defensive action required.
7. Alert Cyber Incident Response Management of the potential threat. Seek advisory inputs as appropriate.

Cyber Incident Response Management

1. Provide advisory inputs as appropriate.

3.5.3 Escalation Severity Level 2

The threat has manifested itself.

Technical Operations Team

1. Determine best course of action for immediate containment of the incident,
2. Notify the Technical Support Team of any action that is required,
3. Report actions taken and status to the Cyber Incident Response Coordinator.

Cyber Incident Coordinator

1. Notify Cyber Incident Response Management of the manifestation of the threat,
2. Receive status from the Technical Operations Team and report to Cyber Incident Response Management,
3. Record on the Incident Recovery Event Recording Form at Appendix D.
4. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix C to identify which key functions are operational / which are affected. Record on the Incident Recovery Event Recording Form at Appendix D.
5. Continue with chronological log.

   Note: The chronological log will be used to support possible follow-on legal action as determined by Richard Huish Trust's Executive Directors.

Cyber Incident Response Management

1. Assume responsibility for directing activities regarding the incident,
2. Coordinate discussion and analysis to determine best course of resolution,
3. Contact Cyber Insurance Provider
4. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the ICO.
5. Alert the Extended Technical Team as applicable,
6. Alert the Administrative Support Team of the incident,
7. Alert the Executive Management,
8. Determine whether Severity Level 2 is appropriate or escalate to level 3,
9. Determine when the risk has been mitigated to an acceptable level.

Extended Technical Team

1. Take whatever action as determined by the Technical Operations Team
2. Report actions taken; number of personnel involved etc. to Incident Coordinator for the chronological log.

Communications Team

1. Message school/college staff/students/parents informing them of the incident if deemed appropriate by Cyber Incident Response Management,
2. Message school/college staff/students employee population of any action they need to take as determined by the Technical Operations Team and directed by Cyber Incident Response Management.

*3.5.4 Escalation Severity **Level 3***

Threat is widespread or impact is significant.

Technical Operations Team

1. Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat,
2. Continue reporting status to the Cyber Incident Response Coordinator for the chronological log of events,
3. Monitor effectiveness of actions taken and modify them as necessary,

4. Provide status to Cyber Incident Response Coordinator and Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat.

Cyber Incident Response Coordinator

1. Continue maintaining the Chronological Log of Event,
2. Continue to manage incident response per direction of Cyber Incident Response Management.
3. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix E and review the Cyber Recovery Plan accordingly.

Cyber Incident Response Management

1. Direct the response team to:
    a. Set up communications channels between all teams.
2. Organize scheduled team meetings. Define specific status update schedule.
3. Alert the Extended Team of the incident notifying them of the Severity Level.
4. Update Executive Management as appropriate.
    a. Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
    b. Contact the local police via Action Fraud website or call 0300 123 2040
    c. DPO should consider whether reporting to the ICO is necessary at www.ico.org.uk 0303 123 11
    d. Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk
5. Decide with the Executive Management as to the safety of the school / college remaining open,
6. Determine when the risk has been mitigated to an acceptable level.
7. Educate employees on avoiding similar incidents / implement lessons learned.

Communications Team

1. Message school/college staff/students/parents and external media as directed by Cyber Incident Response Management.

Extended Technical Team

1. Continue actions to eradicate the threat as directed by the Cyber Incident Coordinator and Cyber Incident Response Management and the Technical Operations team.
2. Continue to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

Administrative Support Team

1. Provide administrative support to all persons and teams involved in incident

Extended Team

1. Contact local authorities if deemed appropriate,
2. If local authorities are called in, make arrangements for them to be allowed into the building,
3. Ensure that all needed information is being collected to support legal action or financial restitution.

3.6 Special Circumstances

i. Email Communications are compromised or otherwise unavailable.

1. There could be a cyber security incident that compromises the ability to communicate via email. In this case, the backup will be communications via desk phone or mobile phone. A phone directory of key persons on the response teams is given in Appendix A.

ii. Personal Identification Information / or other Confidential Information is leaked via Internal Source

1. The process defined above can also apply to the circumstance where information is leaked via an internal source by accident or maliciously. In this case, the steps in the response process would be very similar to the above process but would also include early determination of the type and quantity of data leaked, the source of the leak and the potential impact of the leak to the Trust or to the public at large.

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

Ensure the key contacts (Appendix A) and data assets (Appendix B) is kept up to date with new suppliers, new contact details, and changes to policy.

4. Further Key Roles and Responsibilities

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 / Site Supervisor / Caretaker

- Ensures site access for external IT staff.
- Liaises with the headteacher / principal to ensure access is limited to essential personnel.

School Admin Assistant / Principal PA

- Convenes and/or informs staff, advising them to follow the 'script' when discussing the incident.
- Ensures office staff understand the standard response and knows who the media contact within school / college is.
- Manages the communications, website / texts to parents / school emails.

Data Protection Officer (DPO)

- Supports the school / college, using the school / college data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Principal / 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 / CEO / CFO / CPO

- Supports the Principal / 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.

Teaching Staff and Teaching Assistants

- Reassures pupils / students, staying within agreed pupil standard response.
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed.

5. Staff Media Contact

Assigned staff will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications.

The staff media contact should only provide verified facts. It is likely that verifying details will take some time and stating, “I don’t know at this stage”, is a perfectly acceptable response.

It is likely the following basic questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications **should not respond** to requests for information and should refer callers or media representatives to assigned staff.

Appendix A. Cyber Incident Response Team Contact Details

See Key Contacts.xlsx

Appendix B. Data Asset information.

Held in IT Team Site within O365. Copies on USB drive in the fire safe located at Richard Huish College room W105 and synced to IT workstations for offline access.

Appendix C: 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 D: 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:	
Operational Assessment:	
Informational Assessment:	
Restoration Assessment:	
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.					

Appendix E: 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 minimization		
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:		

Appendix F: Communication Templates

1. College/School Open

Dear Parent/Carer,

I am writing to inform you that it appears the [college/school] has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the 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 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 [college/school] will be working with the Trust 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, we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. The [college/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 [college/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 / school system]

Yours sincerely,

2. School Closure

Dear Parent/Carer,

I am writing to inform you that it appears the [college/school] has been a victim of [a cyber-attack / serious system outage]. This has taken down the [college/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 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, 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 [college/school] to students on [XXXXXXXXXX]. We are currently planning that the [college/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 [college/school] will be working with the Trust 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 / school system]

Yours sincerely,

3. Staff Statement Open

The [college/school] detected a cyber-attack on [date] which has affected the following [college/school] IT systems: (Provide a description of the services affected)

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

(Detail any workarounds / changes)

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

(Provide a description of the services affected)

Following liaison with the Trust, the [college/school] will close to students [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 [college/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 [college/school] IT systems. Following liaison with the Trust the [college/school] [will remain open / is currently closed] to pupils.

The [college/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 [college/school] has taken immediate remedial action to limit data loss and restore systems.

Standard Response

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.

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 / Students

For staff responding to pupil requests for information, responses should reassure concerned students 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 G: Playbooks

See Playbooks.docx