Hawthorn Learning

Contingency and disaster recovery policy

Date created:	September 2024
Last update:	September 2025
Revised:	Annually
Author:	Maz Wilberforce

Contents

Introduction

Aim: To provide a flexible framework to manage the response to any disruption or emergency and to maintain critical activities and recover from the incident quickly and efficiently.

Incidents may occur during the pod day or out of hours. The Disaster Recovery Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.

The plan will ensure that communications can be quickly established whilst activating disaster recovery. It is also important that the plan is well communicated and readily available.

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

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

Scope

This Plan will be activated to manage the response to any incident causing significant disruption to normal service delivery, particularly the delivery of key/time critical activities. Plan activation triggers may include:

- Loss of key people or skills e.g. above normal levels of absenteeism due to illness/injury or other scenarios such as severe weather, changes in service structures, major transport disruption, emergency response duties, or people leaving the organisation.
- Loss of critical systems e.g. ICT network disruption, telephony outage, power outage, utilities disruption or third party supplier disruption.
- Denial of access, or damage to, facilities e.g. loss of a building through fire or flood, an external emergency where emergency service cordon would prevent access for a period of time, utilities failure. You may also require the activation of continuity arrangements in the event of an office move.
- Loss of a key resource such as an external supplier or partner vital to the delivery of a key service or activity.
- To ensure that in the event of an IT disaster such as fire, flood, acts of vandalism, terrorism, malicious cyber-attack, or hardware / software failure, staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

Aims

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

Objectives

- To enable prompt internal reporting and recording of incidents.
- To maintain the welfare of pupils and staff.
- To identify the nature of any threat and assess whether there is a safeguarding concern / immediate threat to individuals.
- To promptly assess whether there is a criminal aspect to the incident, and if so, to report to the police.
- To have immediate access to all relevant contact details (including backup services and IT technical support staff).
- To ensure immediate and appropriate action is taken in the event of an IT incident, or a disaster affecting the IT system.
- To ensure that the pod 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 pod which are unaffected.
- To acknowledge the additional demands placed upon staff members, and where appropriate and applicable, to offer support during incident handling and subsequent recovery.

Incident Management

Purpose:

- Protect the safety and welfare of staff, visitors and the public
- Protect vital assets e.g. equipment, data, reputation
- Ensure urgent and necessary communication takes place
- Support the Business Continuity phase
- Support the Recovery and Resumption phase

Actions:

- Make a quick initial assessment:
    - Survey the scene/situation
    - Assess the impact on pupils and staff (i.e. scale/severity, duration & impact)
    - Disseminate information (to others)
    - Call the Emergency Services if needed
    - Evacuate the building if necessary
    - Gather and share information to facilitate decision-making and enhance the response.
- Nominate individuals to carry out Incident Management roles, as appropriate
- Ensure a log of key decisions and actions is started and maintained throughout the incident.
- Record names and details of any staff or pupils that may have been injured or affected by the incident as part of your incident record keeping. This information should be held securely as it may be required by Emergency Services or other agencies during or following the incident.
- Log details of all items lost by pupils, staff, visitors etc as a result of the incident, if appropriate.
- Assess the key priorities for the remainder of the working day and take relevant action. Consider actions to ensure the health, safety and well-being of pupils, staff and the wider community at all times. Consider your business continuity strategies, i.e. alternative ways of working, re-location to your recovery site etc to ensure the impact of the disruption is minimised.
- Log all expenditure incurred as a result of the incident and seek advice/inform Insurance Company. Record all costs incurred as a result of responding to the incident.
- Consider your communications strategy to ensure staff and pupils are kept informed about what is required of them. If the incident is taking place outside of normal working hours, staff may need to be contacted to advise of any alterations to normal working arrangements for the next day.
- All staff member’s emergency contact details should be held securely electronically as well as in a hard copy as part of your plan. Ensure parents/carers contact details are also available.
- Ensure recording processes are in place for staff/pupils leaving the site. Ensure the safety of staff and pupils before they leave the site and identify suitable risk control measures as required.

Hawthorn Learning Continuity

Purpose:

- To ensure that ‘critical activities’ are resumed as quickly as possible and/or continue to be delivered during the disruption
- To activate one or more of your business continuity strategies to enable alternative ways of working
- To make best use of potentially limited resources by suspending ‘non critical’ activities

Whatever the cause of disruption, the impacts will generally be one or more of the below categories:

- Loss of key people or skills e.g. above normal levels of absenteeism due to illness/injury
- Scenarios such as severe weather, changes in service structures, major
- transport disruption, emergency response duties, people leaving the organisation etc
- Loss of critical systems e.g. ICT network disruption, power outage, utilities disruption, third party supplier disruption etc
- Denial of access, or damage to, facilities e.g. loss of a building through fire or flood, an external emergency where emergency service cordon would prevent access for a period
- of time, utilities failure etc. You may also require the activation of continuity arrangements in the event of an office move
- Loss of a key resource such as an external supplier or partner vital to the delivery of a key activity

Loss of Premises

- Short term work area recovery site is St Anne’s Neighbourhood Centre in Hythe.
- Google classroom in place for virtual learning environment opportunities
- Offsite activities available if premises loss is short term in nature. E.g. Gang Warily, Golden Geckos, Calshot Activities, Lepe, New Forest activities etc.

Tactical options to mitigate against a loss of critical IT systems

- Flexible lesson plans
- Use of secure external network (cloud based which can be accessed via the internet to allow extra back up and protection for files)
- Manual workarounds: pre-printed first aid, safeguarding etc forms.
- Options for WFH for non-child facing staff

Tacitcal options to mitigate against loss of staff or skills

- Use of temporary bank staff

- Multiskilling/cross training to support staff undertaking different roles and responsibilities
- Different ways of working to allow for temporary reduction in staff. E.g. pre prepared educational materials, virtual lea/rning environment opportunities
- Suspend non-critical activities to focus on core priorities
- Ensure business continuity aspects of management are considered (see recruitment policy)

Tactical options to mitigate against loss of key suppliers

- Pre identify alternative suppliers
- Insurance cover
- Alternative ways of working to mitigate the loss

Recovery and Resumption

Purpose:

- To return to ‘business as usual’ as quickly as possible
- To ensure any non critical activities suspended as part of your business continuity response are recovered within appropriate timescales
- Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building on a longer term basis.

Actions:

- Agree and plan the actions required to enable recovery and resumption of normal working practises
- Continue to record all expenditure incurred as a result of the incident
- Respond to any ongoing and long term support needs of Staff and Pupils.
- Once recovery and resumption actions are complete, communicate the return to ‘business as usual’.
- Carry out a ‘debrief’ of the incident with Staff and Suppliers/Partners if appropriate.
- Complete a post incident report to document opportunities for improvement and any lessons identified.
- Review this Business Continuity Plan in light of lessons learned from the incident and the consequent response to it.

Preparation

Preventative Strategies

- Regularly review relevant policies e.g. IT Security Policy, Data Protection Policy, Health and Safety.
- Assess the current security measures (including IT)
- Routinely install security and system updates.
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

IT Acceptable Use

Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for devices.

Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

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

Testing and Review

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

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

IT Disaster Recovery Team and Access Rights

In the event of this plan having to be initiated, Maz Wilberforce will lead the recovery team.

Server and systems admin Access

Please detail all the people with administrative access to the server. Maz Wilberforce, Tomlin Wilding

In the event of an incident access to backup files are available for the following:

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

Backup Strategy

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

Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Provider	Smarty broadband	447897521680
Website Host	Hostinger	tomlin.wilding@icloud.com
Electricity Supplier	EDF	A-92F5D03E
Burglar Alarm	Landlord contact	Heather Hill
Water	Landlord contact	Heather Hill
Text Messaging System	ID Mobile	07765251107
Site / Premises	Landlord contact	Heather Hill

Disaster Recovery Plan

1. Verify the initial incident report as genuine and accurate.
2. Assess and document the scope of the incident.
    - *Which key functions are operational / which are affected?*
3. Start the Actions Log to record recovery steps and monitor progress.
4. Convene the Disaster Recovery Team (DRT).
5. Liaise with IT staff to estimate the recovery time and likely impact.
6. Make a decision as to the safety of the pod remaining open.
    - *This will be in liaison with relevant Local Authority Support Services / Trust*
7. Identify legal obligations and any required statutory reporting e.g. criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the Data Protection Officer and the police*
8. Execute the communication strategy which should include a media / press release if applicable.
    - *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*
9. Identify what can be salvaged (physical and virtual assets) and where there are crucial gaps that take priority.
10. Implement contingency plans e.g. possible workarounds such as remote learning / combining office spaces.
11. IT support staff to continue restoring and facilitating alternative services as required.
12. Document any losses and damages.
13. Contact insurers and file insurance claims, as necessary.
14. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
15. Upon completion of the process, evaluate the effectiveness of the response and review the Disaster Recovery Plan accordingly.
16. Educate employees on avoiding similar incidents / implement lessons learned.

Key Roles and Responsibilities

Directors

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

DSL

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

Onsite Director

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

- 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 pod is.
- Contacts relevant external agencies – IT services / technical support staff / insurers.
- Manages the communications, website / texts to parents / pod emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Recovery

In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not:**

- Turn off electrical power to any computer.

- Try to run any hard drive, back up disc or tape to try to retrieve data.
- Tamper with or move damaged computers, discs or tapes.

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

Data Protection Officer (DPO)

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

Community director

- Supports the Disaster recovery lead throughout the process and ensures 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 policy.

Disaster recovery lead

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

Teaching Staff and Teaching Assistants

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

Insurance

As part of the company’s disaster recovery and business continuity strategies, contact with the insurers is essential.
There may be omissions, liability clauses and other requirements which, if not met, could invalidate any cover.

Insurance contacts

Location of policy: *pod email*

Policy Name	**Coverage Type**	**Coverage Period**	**Amount Of Coverage**
Y149201QBE0123A	Employers Liability	21st Oct 2024 to 20th Oct 2025	£10,000,000
Y149201QBE0123A	Public Liability	21st Oct 2024 to 20th Oct 2025	£5,000,000
Y149201QBE0123A	Professional indemnity	21st Oct 2024 to 20th Oct 2025	£1,000,000

Staff Media Contact

Assigned staff will coordinate with the media, working to guidelines that have been previously approved (for example as detailed in your Critical Incident Plan) for dealing with post-disaster communications.

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

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

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

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

Assigned Media Liaison(s):
Name: Tomlin Wilding Role:Director

Critical Activities - Data Assets

Data assets which are critical and how long would we be able to function without each one.

Leadership and Management:
Access to Headteacher's email address - 1 day
Minutes of SLT meetings and agendas - 1 month

Safeguarding / Welfare:
Access to systems which report and record safeguarding concerns - 4 hours
Referral information / outside agency - 1 day

Child protection records :
Looked After Children records / PEPs - 1 day
Pupil Premium pupils and funding allocations - 1 week
Pastoral records and welfare information - 1 week
Medical - 1 week
Access to medical conditions information - 1 day
Administration of Medicines Record - 1 day
First Aid / Accident Logs - 1 week

Teaching:
Schemes of work, lesson plans and objectives - 1 week
Teaching resources, such as worksheets - 1 week
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 - 1 week
SEND List and records of provision - 1 week
Access arrangements and adjustments - date dependent
EHCPs - 1 week
Behavioural observations / staff notes and incident records - 1 week

Assessment and Exams:
Exam entries and controlled assessments - date dependent
Targets, assessment and tracking data - 1 week
Baseline and prior attainment records - 1 week
Exam timetables and cover provision - date dependent
Exam results - date dependent

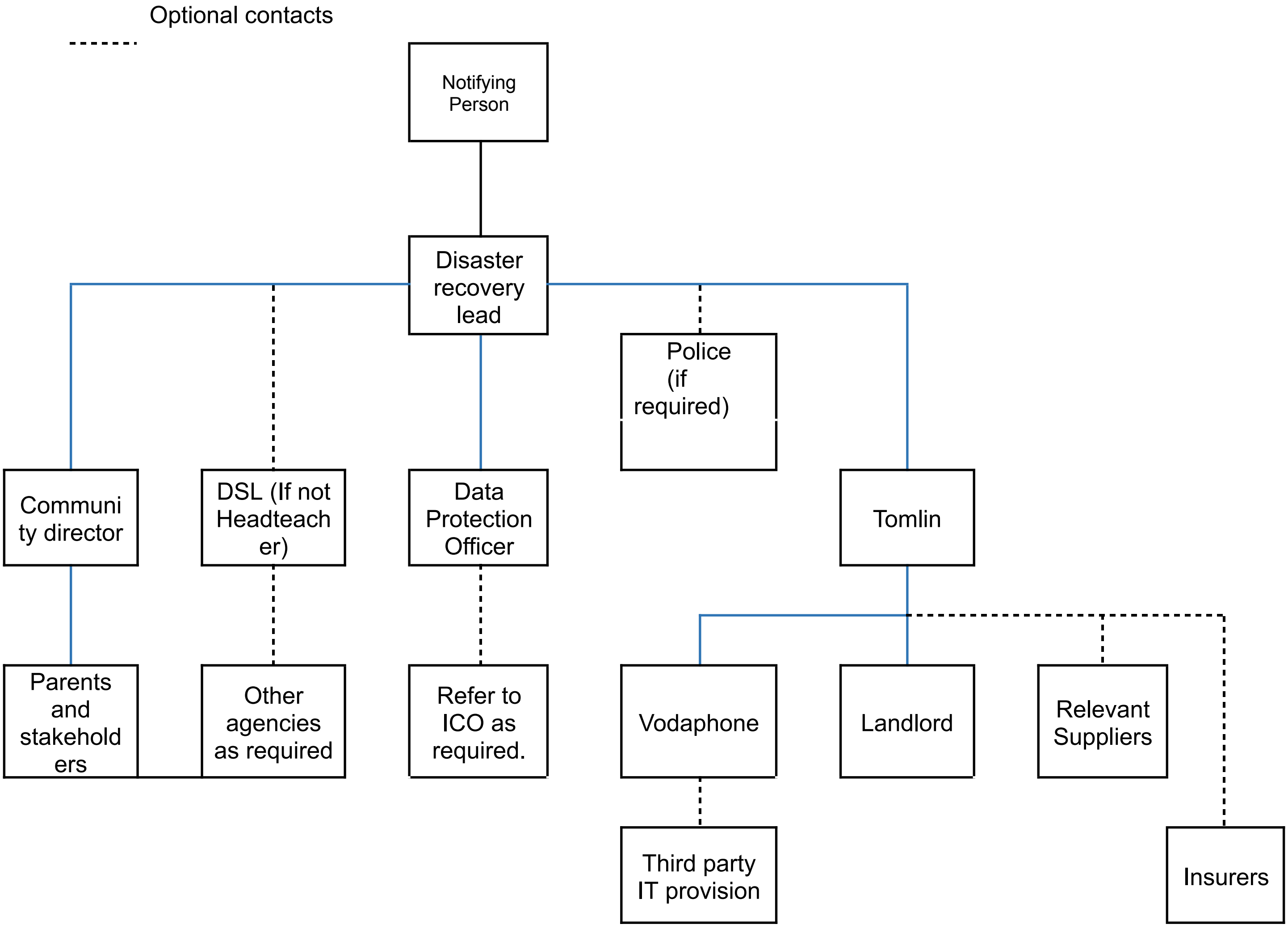
Administration:
Admissions information - 1 week
School to pod transfers - 1 week
Transition information - 1 week
Contact details of pupils and parents - 4 hours
Access to absence reporting systems - 1 day

Diary of appointments / meetings - 1 day
Letters to parents / newsletters - 1 week
Extra-curricular activity timetable and contacts for providers - 1 week

Human Resources:
Disciplinary / grievance records - 1 week
Contact details of staff- N/A

Office Management:
Photocopying / printing provision - 1 week
Telecoms - phones and access to answerphone messages - 72 hours
Email - access to email systems - 72 hours
website and any website chat functions / contact forms - 72 hours
Social media accounts (Facebook / Twitter) - 1 week

Contact List and Notification Calling Tree



Appendix 1

A.1. Incident Impact Assessment

Operational	No Impact	There is no noticeable impact on the 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 pod 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 resources.
	High Impact	The pod can no longer provide any critical services to users. It is likely the pod 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 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 pod.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.

Appendix 2

A.2. Risk Management

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

Appendix 3

A.3. Communication Templates

A.3.1 Pod Open

Dear Parent/Carer,

I am writing to inform you that it appears the pod has been a victim of [a cyber-attack / fire / flood / serious system outage]. This has taken down [some / all] of the pod 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 pod 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 pod will be working with the [Local Authority], IT providers and other relevant third-parties [Health and Safety / NCSC / Derbyshire Constabulary] to restore functionality and normal working as soon as possible.

In consultation with the [Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. The pod 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 pod communications and apologise for any inconvenience.

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

Yours sincerely,

A.3.2 Pod Closure

Dear Parent/Carer,

I am writing to inform you that it appears the pod has been a victim of [a cyber-attack / fire / flood / serious system outage]. This has taken down the pod 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 [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 pod to students on [XXXXXXXXXX]. We are currently planning that the pod 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 pod will be working with the [Local Authority], IT providers and other relevant third-parties [Health and Safety / NCSC / Police] to restore functionality and re-open as soon as possible.

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

Yours sincerely,

A.3.3 Staff Statement Open

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

(Provide a description of the services affected)

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

(Detail any workarounds / changes)

The pod 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 pod has taken immediate action to mitigate data loss, limit severity, and restore systems.

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

A.3.4 Staff Statement Closed

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

(Provide a description of the services affected)

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

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

The pod 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 pod has taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].

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

A.3.5 Media Statement

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

The pod 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 pod 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 pod in initial media responses.

A.3.6 Standard Response - Parents

The information provided should be factual and include:

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

Staff should not speculate how long systems will take to be restored, but can provide an estimate if this has been agreed.

If no restoration date has been advised, staff should merely state that work is on-going and that services will resume as soon as practically possible.

Staff should direct further enquiries to an assigned contact / website / other pre-determined communication route.

A.3.7 Standard Response - pupils

For staff responding to pupil requests for information, responses should reassure concerned pupils that incidents are well prepared for, alternative arrangements are in place and that systems will be back online shortly.

Staff should address any outlandish or suggested versions of events by reiterating the facts and advising pupils that this has been confirmed in letters / emails to parents / carers.

Staff should not speculate or provide pupils with any timescales for recovery, unless the sharing of timescales has been authorised by senior staff.

Appendix 4

A.4 Disaster Recovery Event Recording Form

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

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

1.18.1 Relevant Referrals

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

1.18.2 Actions Log

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

Appendix 5

A.5 Post Incident Evaluation

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

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