ICT Disaster Recovery Plan

Version	Authorisation	Approval Date	Effective Date	Next Review
1	Full Governing Body			

Uphall Primary School, Uphall Road, Ilford, Essex, IG1 2JD
Telephone 02084782993 Email admin@uphallprimary.co.uk

Contents

To be filled in once ratified

Uphall Primary School, Uphall Road, Ilford, Essex, IG1 2JD
Telephone 02084782993 Email admin@uphallprimary.co.uk

Purpose and Scope

Introduction

Uphall Primary School (UPS) has a highly computerised operational environment like most schools and businesses. This includes the use of computers/laptops, servers, printers/copiers and other devices such as phones and CCTV. A school-wide network connects these various systems together and provides communications to other services including access to the internet for external services. These systems provide a critical component to the day-to-day operation of the school.

The use of the IT and Network Systems (ITNS) has increased dramatically in the past years. System failures that do occur can normally be diagnosed and repaired or exchanged promptly. The design of the school server infrastructure is around redundancy which provides the best reliability and uptime while remaining good value for money.

For the most part, the major problems that can cause ITNS to become inoperable for a length of time result from environmental problems or sophisticated cyber challenges. Various situations or incidents that can disable, partially or completely, or impair support of UPS's ITNS have been identified. A plan to deal with these situations is provided.

Almost any disaster will require special funding in order to allow the affected ITNS to be repaired or replaced. This policy assumes that these funds will be made available as needed. However, proper approval will be obtained before any funds are committed for recovery.

Objectives/Constraints

A major objective of this document is to define general procedures for a contingency plan to allow recovery from disruption of ITNS. This disruption may come from total destruction of the school site to something such as minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting Uphall Primary School's ITNS. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical running of the School, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the support given to UPS clients from academic and administrative systems within the remit of the IT and Network Systems Team. Each department at UPS should develop their own internal plans to deal with manual operations should any ITNS services be disrupted. Departments should work with the IT Manager to identify procedures they can develop to support with these plans.

Arising threats from cyber criminals makes it increasingly hard to safeguard the ITNS services and it is near to impossible to protect against all threats, such as so called "zero-day" exploits.
Further to this, it is not possible to provide a full and detailed list of every possible situation that could result in the interruption of ITNS services. The IT Manager reviews every situation individually and provides the best advice to the Senior staff where possible to ensure a quick, cost effective and methodical restoration of IT services (see Antivirus & Malware Policy).

Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. Uphall Primary School senior staff will make any special decisions (IT technical decisions will be made by the IT Manager, unless they believe the decision impacts the running of the school beyond their responsibility) for situations not covered in this plan needed at the time of an incident.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the - IT Manager for a determination of the need to declare an incident. The Head Teacher, Business Manager and Site Manager will also be notified.

The school IT Manager will assume immediate responsibility for restoring the ITNS to a functioning state. The first responsibility will be to see that people are evacuated if equipment is causing a dangerous situation. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured by the site first aiders. The UPS Business Manager and Headteacher will be notified. If the situation allows, attention will be focused on shutti ng down systems, turning off power, etc., **but** evacuation is the highest priority.

Once an incident which is affecting any Uphall Primary School ITNS service has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper School authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable ITNS services to the School has been re-established.

Incidents Requiring Action

The ICT disaster recovery plan for UPS will be invoked under any of the following circumstances:

1. An incident which has disabled or will disable, partially or completely, the School ITNS facilities for a period of 24 hours.
2. An incident which has impaired the use of computers or ITNS managed by IT Support Team due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems which the IT Support Team manages.
3. An incident, which was caused by problems with computers and/or networks, managed by the IT Support Team and has resulted in the injury of one or more persons at UPS.
4. An incident that involves virus attack, or unauthorised intrusion onto the schools network, endangering the security and integrity of the schools data (see Antivirus & Malware Policy).

Contingencies

General situations that can destroy or interrupt the IT network usually occur under the following major categories:

Power/Air Conditioning Interruption

Fire

Water

Weather and Natural Phenomenon

Sabotage, virus, unauthorised intrusion onto the network.

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

Partial recovery - operating in alternate client areas within the School.

Full recovery - operating in all client areas, possibly with a degraded level of service for a period of time.

Physical Safeguards

Lockable doors protect the UPS server room. The IT Support Team, Business Manager and Site Manager have access to the keys. The room is air conditioned and monitored by the school intruder and fire alarms. The server room windows are covered with metal grates. The school's CCTV system also covers the server room area. The server room door has a deadlock. This door has limited key holders for security.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve Uphall Primary School's ITNS facilities. Some minor hardware problems do not disrupt service; maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

Major networking problems

Incidents that cause major networking problems would require failure or damage to the server room, its equipment, fibre optic cables between this and each core network cabinet or core networking equipment.

All fibre optic cabling is installed in containment and where the route is external this is armoured cable in external containment. The school has fibre optic specialist contractors available to replace any damaged cabling.

A disaster recovery server cabinet has been set up in another building located on the school site. In the event of an incident rendering the main server room inoperable, primary or backup servers can be brought online at this location.

Uphall Primary School has several suppliers who can provide essential server room equipment quickly, to ensure essential services are restored as quickly as possible. Non-essential equipment can be sourced with a longer lead time to ensure the best value for money.

Legacy equipment is always kept on site to be brought into use in the case of emergencies.

Major telephone or Internet problems

UPS's telephone system is a cloud hosted service, the system is covered by a software support contract. In the event of a disaster resulting in total power loss across the building the service can be transferred to mobile devices immediately by the IT Manager (Mr S Cordeweener) resulting in zero downtime. The telephone service is covered by a 4 hour response time.

UPSs internet connection is on a 4-hour response 24/7 support contract. The school hosts the firewall equipment which is managed by AdEPT Education Services on behalf of the London Grid for Learning (LGFL). The firewall is on a support contract with the LGFL. The main internet fibre is managed by the LGFL in partnership with their infrastructure partner, Virgin Media Business. In the event of loss of internet, the IT and Network Systems team can easily identify the problem and contact the relevant support team to start restoration.

Environmental problems (air conditioning, electrical, fire)

An external maintenance company periodically services the air conditioning units, any faults are reported to and repaired by the maintenance company. The server room air conditioning unit is specified above capacity for the room to ensure the unit is not overworked.

Electrical

The server room has its own distribution board directly from the mains electrical cupboard located in the basement, the shunt is clearly marked to ensure it is not isolated by accident. Having a dedicated supply for the server room allows other electrical works to take place around the school without compromising the supply to the room.

In the event of an electrical outage, all servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPSs). These units will maintain electrical service to our servers long enough for them to be shut down gracefully. Once electrical power is restored the servers will remain "powered down" until the UPSs are recharged a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure. Automatic notifications are sent to the IT Manager in this event.

Fire

All server rooms are equipped with appropriate fire extinguishers, which will adequately provide manual fire suppression to the equipment from fires in the room itself. If a fire starts, the fire extinguishers should limit damage to the affected piece of equipment and the possibility of damage to equipment in the immediate vicinity. The server room is also fitted with a smoke detector that links to the main school fire alarm system.

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware.

Insurance Considerations

All major hardware is covered under UPS's insurance for the School.

Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site backups contains adequate and timely server backup's and documentation for applications systems, support packages, and operating procedures.

As part of the schools Disaster Recovery Plan it is essential that key data can be accessed under any circumstance within a suitable time period.

General Procedures

Responsibilities have been given for ensuring each of the following actions have been taken and that any updating needed is continued.
Maintaining and updating the ICT disaster recovery plan.

- Ensuring that all IT Support team members are aware of their responsibilities in case of a disaster.
- Ensuring that the periodic scheduled backup plan is being followed.
- Maintaining and periodically updating ICT disaster recovery materials, specifically documentation and systems information, stored in the school safe on an encrypted device and on off-site encrypted backup devices.
- Maintaining a current status of equipment.
- Ensuring that UPS systems are functioning properly and that they are being checked periodically.
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that proper temperatures are maintained in server areas.

Software Safeguards

Administrative software and data are secured by incremental backup's each weekday evening. The full copies of software data are backed up weekly.

Recovery Procedures

This portion of the disaster/recovery plan will be set into motion when an incident has occurred, and damage is such that operations can be restored, but only in a degraded mode at the school site in a reasonable time. It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. This decision will be made by the Head teacher/Deputy Head & Business Manager upon advice from the IT Manager.

The following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Rush order any supplies, forms, or media that may be needed.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine the priorities of the client software that need to be available and load these packages in order. These priorities are often a factor of the time window and the academic year in which the disaster occurs.
- Coordinate client activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed as per the school's backup plan. Work out plans to ensure all critical support will be phased in.
- Keep administration and users informed of the status, progress, and problems.
- Coordinate the longer range plans with the administration, the site officials, and staff for time of continuing support and ultimately restoring the overall system

Degraded Operations

In this event, it is assumed that an incident has occurred but that degraded operations can be set up. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site backups.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the administration and users informed of the status, progress and problems.

Network Communications

In the event of a disaster the cloud based VOIP phone system the school currently uses can be diverted to mobile devices to limit downtime. All incoming calls can be diverted in a short time to keep communication going.

Appendix A

Background

The IT server infrastructure is hosted on virtual hosts stored on a redundant cluster containing two high availability nodes. This enables quick and easier backup and restoration to new hardware and high redundancy in the case of a disaster.

Backup and Restore Procedures

The following paragraphs give details of procedures for the recovery of data in circumstances where a catastrophic loss of data has occurred due to server failure. There are a variety of reasons for server failure including hardware/software conflicts and failure, accidental or deliberate damage, hacking and inexplicable failures normally called ‘Act of God failures'.

At Uphall Primary School we use the 3-2-1 rule as a minimum for our backups:
The 3-2-1 rule refers to a tried and tested approach to data retention and storage:

- Keep at least three (3) copies of data.
- Store two (2) backup copies on different storage media.
- Store one (1) backup copy offsite.

By applying this rule, we ensure that data can be recovered in almost any failure scenario. We keep:

- 1 copy in production
- 2 copies on-site (online and offline)
- 1 copy offsite via the LGFL Gridstore

Onsite – Online: Backup operations are carried out daily onto a network attached storage (NAS) device. The backups are scheduled to run each night, Monday to Friday, a further "full" backup of servers is taken at the weekend. This device is set up with a raid 5 configuration for data protection and redundancy.

Onsite – Offline: Each half term an encrypted device containing a full backup is stored offline and stored for an entire academic year. At the end of each academic year a full backup is taken offline and stored on an encrypted device and stored in accordance with the data retention schedule.

Offsite - Each weekend a backup is uploaded to an offsite location hosted on the LGFL Gridstore platform.

Onsite Backups currently run at 10PM every evening. Offsite Backups occur at 6AM every Saturday.

Daily recovery tests are taken from both the on-site and off-site backups. All backup jobs are set to notify a status report to the ICT Manager upon completion. If a failure occurs remedial action will be taken at the first possible opportunity.

In the case of accidentally deleted files and other small scale restore jobs, the file/s will be recovered from the onsite backup. Recovery from the offsite backup will only be made in the case of an error or failed recovery of the file/s.

All backup and restore operations are undertaken by the IT Manager or an authorised member of the IT Department.

Disclaimer

While every effort is made to ensure the integrity and security of data held on the network, the school cannot accept responsibility for permanent loss of data arising from any cause. Users should, at all times, follow standard network usage procedures: particularly maintaining regular local copies of important files except where the data is business of the school, then this should not be taken off the school systems without the explicit permission of the IT Manager (Mr S Cordeweener) and the Business Manager (Mr S Brown).

The following sections should be completed to produce a bespoke Cyber Recovery Plan for your school:

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	Dr. Kulvarn Atwal	Headteacher	
Data Management	Steven Cordeweener	IT Manager	
IT Restore / Recover	Steven Cordeweener	IT Manager	
Site Security	Mohamed Dahmani	Site Manager	
Public Relations	Dr. Kulvarn Atwal	Headteacher	
Communications	Sharon Leavy	Strategic Learning Lead	
Resources / Supplies	Sutton Brown	Business Leader	
Facilities Management	Mohamed Dahmani	Site Manager	

This procedure should not be published with contact details included due to the risk of a data breach.

Server Access

Please detail all the people with physical and/or administrative access to the server.

Role	Name	Contact Details
Headteacher	Dr. Kulvarn Atwal (Physical)	
School Business Manager	Sutton Brown (Physical)	
IT Support Technician	Steven Cordeweener (Physical/Admin)	
Third Party IT Provider		

This procedure should not be published with contact details included due to the risk of a data breach.

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Strategic Learning Lead	Sharon Leavy	
School Business Manager	Sutton Brown	
MIS Provider	RM	
Data Manager	Wendy Cordeweener	

This procedure should not be published with contact details included due to the risk of a data breach.

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

- Registers
- Staff / Pupil contact details
- Current Child Protection Concerns

Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	Onsite/Offsite	Daily/Weekly/Termly
School MIS	Maintained by provider	Awaiting Data
Cloud Services	Maintained by provider	Daily
Third Party Applications / Software	Onsite/Offsite	Daily/Weekly/Termly
Email Server	Onsite/Offsite	Daily/Weekly/Termly
Curriculum Files	Onsite/Offsite	Daily/Weekly/Termly
Teaching Staff Devices	Onsite/Offsite	Daily/Weekly/Termly
Administration Files	Onsite/Offsite	Daily/Weekly/Termly
Finance / Purchasing	Onsite/Offsite	Daily/Weekly/Termly
HR / Personnel Records	Onsite/Offsite	Daily/Weekly/Termly
Inventory	Onsite/Offsite	Daily/Weekly/Termly
Facilities Management / Bookings	Maintained by provider	Daily/Weekly/Termly
Website	Maintained by provider	Daily
USBs / portable drives	N/A	N/A

Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection	02082555555	
Backup Provider	02082555555	
Telecom Provider	08000434241	
Website Host	02082555555	
Electricity Supplier	Type text here	
Burglar Alarm		
Text Messaging System	01612024141	
Action Fraud	03001232040	
Local Constabulary	02087212026	
Legal Representative		
LA / Trust Press Officer	pressoffice@redbridge.gov.uk	

This procedure should not be published with contact details included due to the risk of a data breach.

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.

Assigned Media Liaison(s):

Name: _____ Role:_____

Name: _____ Role:_____

Key Roles and Responsibilities

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

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

- Seeks clarification from person notifying 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 Governors.
- Liaises with the school Data Protection Officer.
- Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.
- Liaises with School Business Manager\Strategic Learning Lead to contact parents, if required, as necessary

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 / Caretaker

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

School Business Manager\Strategic Learning Lead (SBL/SLL)

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

Data Protection Officer (DPO)

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

Chair of Governors

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

IT Lead / IT Staff

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

- Verifies the most recent and successful backup.
- 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 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.

Teaching Staff and Teaching Assistants

- Reassures pupils, 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

Critical Activities - Data Assets

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

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

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

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

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address		
	Minutes of SLT meetings and agendas		
	Head's reports to governors (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns		
	Attendance registers		
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Pupil Premium pupils and funding allocations		
	Pastoral records and welfare information		
Medical	Access to medical conditions information		
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	Schemes of work, lesson plans and objectives		
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
	Pupil reports and parental communications		
SEND Data	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Assessment and Exams	Exam entries and controlled assessments		
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
	Exam results		
Governance	School development plans		
	Policies and procedures		
	Governors meeting dates / calendar		
	Governor attendance and training records		
	Governors minutes and agendas		
Administration	Admissions information		
	School to school transfers		
	Transition information		
	Contact details of pupils and parents		
	Access to absence reporting systems		
	School diary of appointments / meetings		
	Pupil timetables		
	Letters to parents / newsletters		
	Extra-curricular activity timetable and contacts for providers		
	Census records and statutory return data		
Human Resources	Payroll systems		
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision		
	Telecoms - school phones and access to answerphone messages		
	Email - access to school email systems		
	School website and any website chat functions / contact forms		
	Social media accounts (Facebook / Twitter)		
	Management Information System (MIS)		
	School text messaging system		
	School payments system (for parents)		
	Financial Management System - access for orders / purchases		
Site Management	Visitor sign in / sign out		
	CCTV access		
	Site maps		
	Maintenance logs, including legionella and fire records		
	Risk assessments and risk management systems		
	COSHH register and asbestos register		
Catering	Contact information for catering staff		
	Supplier contact details		
	Payment records for food & drink		
	Special dietary requirements / allergies		
	Stock taking and orders		

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:		