Westhouses Primary School
Technology Disaster Recovery Plan

Revision History

REVISION	DATE	NAME	DESCRIPTION
1.0	01.07.2021	Juliette Whitby/Amy Flint/Dave Holland	
1.1	01.07.2024	Juliette Whitby/Amy Flint/Dave Holland	Minor changes

Approval History

REVISION	APPROVAL DATE	APPROVED BY	SIGNED
1.0			
1.1	01.07.2024	S.Taylor	

Review date: 01.07.2027

Rationale

This document delineates Westhouses Primary School policies and procedures for an Information Technology Disaster Recovery Plan, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure.

This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

The purpose of this plan is to ensure information system operation, data integrity and availability, and business continuity.

This plan should be read in conjunction with the Critical Incident Management Plan, detailing the Action Plan in response to a disaster. The Critical Incident Management Plan includes details of key holders and contact lists.

Policy Statement

- The IT Disaster Recovery Plan shall be reviewed every 3 years.
- The IT Disaster Recovery Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key educational activities.
- Staff must be made aware of the IT Disaster Recovery Plan and their own respective roles.
- The IT Disaster Recovery Plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the IT Disaster Recovery Plan program is to develop, test and document a well-structured and easily understood plan which will help Westhouses Primary School recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and educational operations. Additional objectives include the following:

- The need to ensure that employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.

Key Personnel – Contact Information

In the event of an emergency situation, the contact details for key members of staff and associations are as follows:

NAME AND TITLE	CONTACT OPTION	CONTACT NUMBER
Headteacher – Mrs Juliette Whitby	Work	01773 832518
	Mobile	07525205130
	Email Address	Jwhitby1@westhouses.derbyshire.sch.uk
Caretaker – Ms Nicola Smith	Work	01773 832518
	Mobile	
	Email Address	-
I.T. Network & Systems Technician – Mr David Holland	Work	0115 6980996
	Mobile	07787110598
	Email Address	david@cultivateit.co.uk
School Clerk– Mrs Carole Newborough	Work	01773 832518
	Mobile	07563178308
	Email Address	cnewborough@westhouses.derbyshire.sch.uk
Chair of Governing Body – Mr Simon Taylor	Work	
	Mobile	
	Email Address	staylor@westhouses.derbyshire.sch.uk
Derbyshire County Council (Local Authority) – Call Derbyshire	Work	01629 533190
CAYA School Support Service – County Hall, Matlock	Work	01629 536789
	Email	Caya.schoolsupport@derbyshire.gov.uk

Data Protection and Information Control

The following individuals have authorised access to the School Server and associated administration rights:

Headteacher:	Mrs Juliette Whitby
Contracted I.T. Technician:	Mr David Holland

The following individuals have authorised access to the SAP Finance system and RM Integris:

Headteacher:	Mrs Juliette Whitby
School Clerk:	Mrs Carole Newborough
School admin:	Miss Amy Flint

The following individuals have authorised access to RM Integris (levels of access vary according to need):

Teacher:	Mr Cormac Smith
Teacher:	Mrs Kristy Coupe
Teacher:	Miss Katie Briggs
Teacher:	Mrs Emily Ramsdale
HLTA:	Mrs Jayne Russell

Only the above authorised personnel have access to children's and parents' data apart from authorised personnel from the Local Authority, Social Services and Education Welfare departments.

The General Data Protection Regulations (GDPR) allows disclosure of personal information to other bodies where appropriate. Policies and procedures are in place for the safe, secure sharing of information with other agencies.

The school is registered as a data controller as required by the Information Commissioner's Office.

The school server is segregated using folders – "Staff files", "PCOurWork", "Scans". The following users have access to each folder:

Office files within staff files– J Whitby, C Newborough, A Flint
Staff files excluding protected files – all staff have access
PCOurWork – all staff have access
Scans – J Whitby, C Newborough, A Flint

Particularly sensitive information (e.g. SCR document, safeguarding materials) stored on limited accessibility areas.

Staff have received training and information regarding password management and are regularly updated with information provided by the Local Authority (e.g. Data Demon, emails from audit services).

Backups and Restoration Arrangements

The RM Integris system is an online system with servers based off site. RM Integris is responsible for backups and restoration of the data stored on the Integris system. This system can be accessed remotely at any location with a stable and secure internet connection (e.g. another local school or Local Authority site). Assistance with the RM Integris system can be sought from the CAYA School Support Service at County Hall, Matlock.

Pupil and staff paper records are kept on-site in locked cupboards within the locked school office. Access to the school office is restricted by an electronic door lock to which only authorised members of staff have access. Critical documents are kept in the red box in the main office.

The ICT Technician ensures the regular backup of students work on a regular basis to enable recovery in the event of the loss of data files or system failure. Backups are stored remotely on a cloud-based system. Assurances have been received that the data is stored in an encrypted format, in a UK-based location under the terms of the GDPR Regulations. The ICT Technician is responsible for regularly testing the backups to ensure data can be restored in the event of system failure. The ICT technician is able to access and restore backups remotely in the event of an emergency.

All ICT equipment is listed on a school inventory. This inventory can be accessed in the event of an emergency.

Security Arrangements

Microsoft Security Essentials and MalwareBytes are used as anti-virus software on all staff computers and these are updated when required.

All staff have been issued with the policies related to safe and appropriate use of ICT and have signed to confirm receipt.

Regular updates are given to staff on the safe and appropriate use of ICT and on data protection issues.

Staff have access to data protection and GDPR training via the Derbyshire Learning Online system and are encouraged to refresh this training annually.

The "Data Demon" leaflet issued by Derbyshire County Council has been shared with all staff.

The "Audit Matters" newsletter is shared with the headteacher, staff with financial responsibilities and the governing body.

Plan

Updates and Review

It is necessary for the IT Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they should be reviewed and agreed by the Chair of the Governing Body. The plan is to be formally reviewed every 3 years or more frequently if changes to the ICT capabilities of the school occur.

Plan Documentation Storage

Copies of this Plan and hard copies will be stored in secure locations. A master protected copy will be stored on specific resources (the server, under the "Updated policies" folder) established for this purpose.

Emergency Response

Alert, escalation and plan invocation

Key trigger issues that would lead to activation of the IT Disaster Recovery Plan are:

- Total loss of all communications
- Total loss of power
- A disaster that causes damage or loss of part of the school buildings or its equipment (e.g. fire, flood).
- Total loss of the building

Assembly Points

When the premises need to be evacuated, please refer to the Emergency Evacuation Plan.

Plan Invocation

When an incident occurs, the IT Disaster Recovery Plan may be implemented.

Responsibilities of key employees are:

- Respond immediately to a potential disaster and call the appropriate emergency services;
- Assess the extent of the disaster and its impact on the school;
- Decide which elements of the disaster recovery plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

IT Disaster Recovery Team

The team members include Juliette Whitby (Headteacher), David Holland (ICT Technician), Nicola Smith (Caretaker), Carole Newborough (School Clerk), Amy Flint (Admin), and other staff members from the Local Authority and agencies as appropriate.

The team's responsibilities include:

- Establish facilities for an emergency level of service within 1 business day;
- Restore key services within 1 business day of the incident;
- Return to business as usual within 1 business day after the incident (depending upon incident);
- Coordinate activities with disaster recovery team, first responders, etc.

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The IT Disaster Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a successful return to normal business function.

The person discovering the incident informs their immediate supervisor. One of the tasks during the early stages of the emergency is to notify the IT Disaster Recovery Team that an emergency has occurred. The notification will request IT Disaster Recovery Team members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

If a team member designated to contact other staff members is unavailable, backup staff members will perform notification duties. Assistance may also be sought from the local cluster schools who will be able to provide an appropriate level of technical and management skills:

Blackwell Primary School (Mrs G Gardner - Headteacher): 01773 811281

Mickley Infant School (Mrs S Street - Headteacher): 01773 832707

Review

This plan will be reviewed every three years (as per audit recommendation) or sooner as changes require.