St Matthew's Catholic Primary School

Incident Response Plan (IRP)

2024 - 2025

Written: November 2024
Reviewed: September 2025

Adopted from LGfL CyberCloud®

Mr Garcia

Love, Learn and Shine Together with Jesus

LGfL CyberCloud®

IT Major Incident Response Plan

St Matthew’s Catholic Primary School

Document Control

Ownership	
Author	Mr J Garcia
Owner	Mrs C Sime

Review dates			
Version	Change History	Revised By	Date
0.1	Document created	J Garcia	22.11.24
1.0	Document signed off		

Date of next review	22.11.25

Contents

Introduction

This is an IT major incident response plan for St Matthew’s Catholic Primary School. It is to be invoked in the event of an incident that would affect the school's IT services.

Definitions

Incident Response Plan (IRP)

A documented set of procedures and information intended to deliver continuity of critical IT activities in the event of a disruption.

Incident

An event that causes disruption to the organisation.

Critical IT services could be disrupted by loss of:

key data because of a ransomware attack

key services because of a ransomware attack

communications networks (e.g. email, phones)

other key services (e.g. school MIS).

Purpose of Plan

This plan aims to minimise the impact of such losses by making contingency plans and putting measures in place for essential IT processes to be maintained.

IRP Ownership

Mrs Sime has overall responsibility for the IRP and has delegated responsibility for documenting the process to:

- Mrs Gaskell
- Mr Garcia

The IRP will be reviewed and updated every year, or when other factors dictate. Updated plans will be signed off by Mrs Sime and circulated to replace the previous versions.

Incident Response Team

In the event of a major incident, an Incident Response Team (IRT) will be formed. The key roles of the IRT are to:

- Make decisions to apply appropriate resources
- Provide strategic direction
- Provide communications to key internal and external stakeholders (staff, students, parents, public bodies)
- Assume responsibility for co-ordinating incident management
- Liaise with Third party suppliers

IRT Contact Details

Name	Contact details	Alternative contact
Mrs C Sime	c.sime@stmatthewscps.co.uk	Mrs T Gaskell
Mrs T Gaskell	t.gaskell@stmatthewscps.co.uk	Mrs D Tippey
Mr J Garcia	j.garcia@stmatthewscps.co.uk	Mr M Edwards / Mrs J Evans
Rev. Deacon. R Burke	governors@stmatthewscps.co.uk	Mrs C Sergeant
Liverpool IT Services	0151 538 1789	Liverpool Local Authority

IRT Communications

Effective communication is critical during a major IT incident to ensure timely response, coordination, and resolution. This section outlines the protocols and alternative methods for communication among the Incident Response Team (IRT) and key stakeholders when traditional systems such as email, telephones, and websites may be unavailable.

Primary Communication Channels

- **In-Person Communication:**
  - Meeting Point: Designate a central and secure location within the school, this will usually be the Head Teacher’s Office as the primary gathering point for the IRT during incidents.
  - Backup Location: In the event the primary meeting point is inaccessible, use the Staff Room as the alternative location.
- **Radio Communication:**
  - Handheld Radios: Ensure school-issued radios are available and accessible to IRT members.
  - Frequency Coordination: Use pre-assigned radio channels for clear and secure communication. This will be Channel 2 to avoid communication with All radio users on Channel 1.
- **Text Messaging (SMS):**
  - Use mobile devices to send SMS messages for concise updates and coordination. SMS may remain functional even if data services are down.
  - Ensure that all team members' mobile numbers are updated and tested regularly.
- **Landlines:**
  - Identify landline phones that operate independently of the school's main network infrastructure, if any.

Backup Communication Methods

- **Printed Contact Lists:**
    - Maintain an up-to-date printed list of IRT members, key stakeholders, and external service providers (e.g., IT contractors, local authorities). Store copies in multiple secure locations, such as the Headteacher's office and the Incident Response Kit.
- **Offline Storage of Key Information:**
    - Contact details and critical documents should be stored on offline media (e.g., USB drives, external hard drives) and kept in the Incident Response Kit.
    - Ensure these storage devices are password-protected and encrypted for security.
- **Bulletin Boards/Whiteboards:**
    - Use physical bulletin boards or portable whiteboards for posting updates in the designated meeting area.
- **Runner System:**
    - Designate team members or support staff to relay messages in person between IRT members and stakeholders if no electronic or telecommunication options are available.

Key Stakeholder Communications

- **Staff:**
    - Use staff meetings or printed memos to communicate updates if digital systems are unavailable.
    - Ensure staff know the location of emergency communication points.
- **Parents and Guardians:**
    - Utilise pre-printed emergency notification templates that can be distributed via hard copy or alternative channels.
    - Activate pre-arranged phone tree systems to disseminate critical information.
- **Local Authorities:**
    - Pre-establish contact methods and ensure landlines or alternative communication channels are listed in the Incident Response Plan.
- **External IT Support/Providers:**
    - Maintain emergency numbers for IT contractors, vendors, and regional IT support on offline storage and printed copies.

Testing and Maintenance

- **Regular Drills:**
    - Conduct communication tests quarterly to ensure all methods (e.g., radios, landlines, SMS) are operational.
    - Include scenario-based testing to simulate a loss of primary communication systems.
- **Contact Information Updates:**
    - Update contact lists monthly or whenever personnel changes occur.
    - Cross-check all backup copies to ensure consistency.
- **Radio and Device Checks:**
    - Test radios, offline devices, and emergency landlines monthly.
    - Keep spare batteries and chargers in the Incident Response Kit.
- **Incident Documentation**
    - Record all communication activities during the incident for post-event review and improvement of the response plan.

- Ensure secure storage of incident logs, whether digital (on offline storage) or physical (printed copies).
- This communications plan ensures that St Matthew's Catholic Primary School's IRT can operate effectively under various constraints and maintain coordination with all stakeholders during a major IT incident.

Key Documents and Files

Document of File Name	Location	Backup Location	Document Owner
Major Incident Response Plan	Headteacher's Office – Incident Response Pack	Front Office – Incident	Mr J Garcia
Staff contacts list	Headteacher's Office – Incident Response Pack	Front Office – Incident	Mrs D Tippey
Parents contacts list	Headteacher's Office – Incident Response Pack	Front Office – Incident	Mrs D Tippey
Third party contacts list	Headteacher's Office – Incident Response Pack	Front Office – Incident	Mrs C Sime
Insurance documents	Headteacher's Office – Incident Response Pack	Front Office – Incident	Mrs C Sime
Network documentation	Headteacher's Office – Incident Response Pack	Front Office – Incident	Liverpool IT Services
Secure password repository	Headteacher's Office – Incident Response Pack	Front Office – Incident	Liverpool IT Services
Backup disk/media recovery keys	Headteacher's Office – Incident Response Pack	Front Office – Incident	Liverpool IT Services

Recovery Priorities

This section details the order in which systems should be restored to ensure that critical functions are available as soon as possible. As different systems have different priorities throughout the year this order should be reviewed by the IRT to ensure that it is still appropriate. For instance, the restoration of the school's MIS may be a higher priority during exam results weeks.

System/Service	Pre-requisites	Priority	Notes
Backup solution			
Active Directory/User account administration	Backup solution	Very High	Required for the majority of other services
Office 365/ Google Workspace Email/OneDrive/G Drive	Active Directory (depending on configuration)	Very High	
Management Information System	Active Directory	High	
Phone system		High	Not integrated to other systems
User files	Active Directory	Medium	
Access control			Not integrated to other systems
CCTV		Medium	Not integrated to other systems
Education Apps	Active Directory	Low	
Printing	Active Directory	Low	
Cashless catering			
Safeguarding			
SEND			

Key Service Providers

This section provides a record of key service providers that form part of the school's IT services.

Name	Type /description of service	Contact details	Notes
Police – Action Fraud	National reporting centre for fraud and cybercrime	0300 123 2040	Available 24/7 for businesses
Liverpool Local Authority	Local Education Authority		
Information Commissioner's Office	Regulatory office in charge of upholding information rights.	ICO breach reporting website 0303 123 1113	Will need to be informed within 72 hours if data has been stolen during the incident.
LGfL	Internet connectivity and security product licensing	020 82 555 555 Option 5 Support site	
Sophos	Antivirus solution	Sophos Central	
Malwarebytes	Antimalware solution	Malwarebytes	
Gridstore	Cloud backup solution		
Liverpool IT Services	IT Support Service	0151 538 1789	This is a Voicemail Telephone Number. Document Owner to liaise with Liverpool IT Services to seek an emergency contact number.
Licensing provider			
CCTV provider			
Access control provider			

Incident Plan

Risk	Potential Triggers of the Risk	Current Mitigations
Loss of access to files and IT Systems	Ransomware attack Sabotage Phishing emails Fire/Flood Pandemic DDoS (Distributed denial of Server) Power failure	• Daily backups encrypted and stored offsite • Staff have remote access to email • Files and folders stored on Microsoft Office 365 systems • Antivirus software installed on all systems and checked regularly for correct configuration and automatic updates running • Security updates applied to devices as soon as possible • Administrative permissions limited to IT support staff • Sophos phish used to raise awareness of threats

Response Plan

1. Actions required in the event of a major incident				
	Action	Timing	Responsible	Complete
1.1	Verbal notification of incident / or identifies a problem through system alerts	Immediate	Mrs C Sime	
1.2	Notification to IRT	Immediate	Mrs C Sime	
1.3	Assessment of scope of incident and options for limiting impact	Within 1 Hour	Mr J Garcia / Mrs C Sime	
1.4	Review recovery priorities	Within 1 Hour	IRT	
1.5	Communicate with school staff Inform Action Fraud	Within 1 Hour	IRT	

1.6	Estimated recovery time / invoke full or partial recovery plan	Within 1 Hour	IRT	
1.7	Communicate with parents if required as part of school day	Within 2 Hours	Mrs C Sime Mr J Garcia	
1.8	Regular updates to IRT and school staff	2 Hourly	Mrs C Sime or Delegated Member of IRT	
1.9	Communicate with Public bodies as required		Mrs C Sime or Delegated Member of IRT	

Actions Log

During a Major Incident, a lot of things can happen very quickly. Good record-keeping can help save time in the future. The following table should be used to track what has been done and by whom. Following the incident this can be used to review the effectiveness of this plan and the actions that were undertaken.

Date	Time	Description of the event/action taken/decision made	Costs incurred	Completed by

Review and sign off

Headteacher	Mrs C Sime
Chair of Governors	Rev. Deacon. R. Burke
Other technical support	Liverpool IT Services
Date this plan was last reviewed and by whom	22.11.24 Mr J Garcia
Date of next review and by whom	22.11.25 Mr J Garcia