IT Major Incident Response Plan

Wandsworth Federation of Maintained Nursery Schools (WFMNS)

Document Control

Ownership	
Author	Rachel Rollerson
Owner	Wandsworth Federation

Review dates			
Version	Change History	By	Date
0.1	Document created	Rachel Rollerson	07.12.21
1.0	Document Review date	FGB	5.7.23
2.0	Document Review Date	FGB	19.5.2025

Date of next review 19.5.2026	

Contents

Introduction

This is an IT major incident response plan for WFMNS This plan is to be invoked in the event of an incident that would affect IT services for any of the schools.

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 one of the organisations.

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

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

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

Rachel Rollerson

The IRP will be reviewed and updated every year, or when other factors dictate. Updated plans will be signed off by Headteachers of each school within the Federation 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

If possible, it can be useful to include a Governor and a member of staff who is not technically aware in this group to get a variety of perspectives

IRT Contact Details

Name	Contact details	Alternative contact
Kellie Schrader Headteacher Somerset Natasha Crabbe Headteacher Balham Catherine McKeever Headteacher Eastwood	020 7223 5455 020 8673 4055 020 8876 3976	Rachel Rollerson
Rachel Rollerson Federation Business Leader	020 7223 5455	
Wandsworth Schools ICT Support	020 8871 8373 editsupport@richmondandwandsworth.gov.uk	Alex Purssey / Daren Marsh

Key Documents and Files

This table should be completed to detail the location of documents that may be required during a major incident

Document of File Name	Location	Backup Location	Document Owner
Major Incident Response Plan	GDPR Files Office Cupboard in all locations	Wandsworth IT/	
Staff contacts list	HR & Staff File Office Cupboards in all locations		
Parents contacts list	Office Cupboard		
Third party contacts list	GDPR file in Office Cupboard in all locations		
Insurance documents	Wall in Office		
Secure password repository	Note that passwords stored in Chrome/Edge may be inaccessible if you cannot access user accounts		
Backup disk/media recovery keys	Wandsworth IT		Wandsworth IT/Your support provider

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.

The table below provides an example using systems that are used in the majority of schools. This should be modified to meet the needs of your school.

System/Service	Pre-requisites	Priority	Notes
Backup solution			
Active Directory/User account administration	Backup solution	Very High	Required for the majority of other services
Email/ G Drive	Active Directory (depending on configuration)	Very High	Required for the majority of other services
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
Printing	Active Directory	Low	
Online Banking			Internet based
Safeguarding			
SEND			

Key Service Providers

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

This table should be updated to include details of all your school's service providers who may need to be involved in the response to a major incident.

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
LA/Borough	IT Wandsworth	020 8871 8373	Working hours
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	
BT	Phone lines	0800 800150	
Sophos	Antivirus solution	Sophos Central	
Malwarebytes	Antimalware solution	Malwarebytes	
Gridstore	Cloud backup solution	020 82 555 555 Option 3 Support site	
Hardware reseller	VeryPC Wandsworth IT	0114 321 8609 020 871 8373	
Third party organisations	Harrisons Solo	07979166021 Amanda Love 07881013512/ 01792 793021 Freddy Andrade	
Licensing provider	Microsoft Licences	0121 712 1940 Capita	
CCTV provider	Laser	Ashley 07811 264439 Steve - 07802 311466	
Access control provider	N/A	N/A	

Incident Plan

The following is included as an example. You should tailor this to your school's requirements

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 • LGfL DDoS protection provided via Janet network

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	[Alex Purssey / Daren Marsh]	
1.2	Notification to IRT	Immediate	WIT to IRT	
1.3	Assessment of scope of incident and options for limiting impact	Within 1 Hour	WIT and Headteacher	

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	Headteacher	
1.8	Regular updates to IRT and school staff	2 Hourly	Headteacher [Alex Purssey / Daren Marsh]	
1.9	Communicate with Public bodies as required		Headteacher	

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

You should schedule in regular reviews of this document to ensure it is updated at least annually

WFMNS	Headteacher / Principal	Kellie Schrader Natasha Crabbe Catherine McKeever
	WFMNS Business Manager	Rachel Rollerson
	Network manager / other technical support	[Wandsworth IT Support]
	Date this plan was last reviewed and by whom	19.5.2025
	Date of next review and by whom	19.5.2026 Rachel Rollerson