OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

Business Continuity Policy and Incident Management Plan

~~Feb 2020~~

~~Feb 2021 Ver 1.02~~

Nov 2024 Ver 1.03

Trust Mission Statement

We are a partnership of Catholic schools, and our aim is to provide the very best Catholic education for all in our community and so improve life chances through spiritual, academic and social development.

We will achieve this by:

- Placing the life and teachings of Jesus Christ at the centre of all that we do
- Following the example of Our Lady of Lourdes by nurturing everyone so that we can all make the most of our God given talents
- Working together so that we can all achieve our full potential, deepen our faith and know that God loves us
- Being an example of healing, compassion and support for the most vulnerable in our society

Matthew 7: 24-25 GNT v 24

24. "So then, anyone who hears these words of mine and obeys them is like a wise man who built his house on rock. 25 The rain poured down, the rivers flooded over, and the wind blew hard against that house. But it did not fall, because it was built on rock.

This Policy was approved and adopted by the Academy Trust Company on:	11.12.2024
Policy Review date:	5.12.2025
Reviewer:	Dave Burrough / OLOL Audit & Risk Committee / OLOL Trust Board

Contents

Appendices

Background

This policy provides the necessary tools, processes and procedures to ensure that major incidents are managed effectively and that disruption to normal operations is minimised. Business Continuity Planning is the process of giving some thought in advance to how we would maintain key services and recover from damage to, or loss of, a particular element of the Trust's business and developing those thoughts into positive plans of action.

Objectives

- To identify the types of incident which will be escalated to 'Business Continuity Incident' status and managed under this Incident Management plan and the types of incident which will be managed under an academy's emergency plan;
- To assist the incident management team (IMT) in managing an incident;
- To provide, via checklists, an orderly process for managing incidents;
- To assist in prioritisation of the recovery of critical functions;
- Provide a response framework to an emergency situation;
- To provide information on how to recover critical functions; and,
- To provide contact details to assist in the management of an incident

Successful incident management

The key to success in successfully managing major incidents is having an appropriately skilled and practised team in place to enable all incidents that might detrimentally affect the business are dealt with in a quick and efficient manner.

Strategy

The Trust will:

Create an incident management team which has the appropriate skill sets and experience to deal with unexpected incidents;

- Allocate duties to each of the team (either in advance or at the time of the incident);
- Practice disruptive scenarios.

The Planning Process

1. Identify the six critical business elements: People; premises; machinery/equipment/utilities; data; communications and suppliers
2. Determine how we will continue to carry out the Trust's business if any of these elements was interrupted for a period of time.

The effects will differ depending on the location and duration of the interruption so we will consider a range of time periods. We will establish the time period in which we would need to recover the particular aspect before the business starts to suffer. We will determine what measures we need to put in place to prevent the business being adversely affected. These measures are in the form of:

- 'recovery plans' (post-event); and
- additional protection/mitigation measures (pre-event);
- when to invoke the incident management team and how to contact the team members;
- where the incident management team might meet should the main premises become unavailable as a result of the incident;
- whom we might need to contact to inform them of the incident and/or to seek assistance; and,
- what information and equipment we might need to assist recovery in the event of an incident.

Invocation

The incident management plan may be invoked by any member of the incident management team (please refer to Table 2) in response to an incident that they feel may have an adverse effect on the normal day-to-day operations of the Trust.

The principal aims of declaring a business continuity incident are to:

- Preserve life

- Preserve buildings and facilities
- Return to operational 'normality' as soon as reasonably practicable
- Communicate effectively with stake holders

Definitions

Emergencies fall into 2 categories. These are:

1. **Business Continuity Incident:** An event that has the capacity to lead to loss of, or a disruption to, the Trust's operations, services or normal operation, typically, for typically for longer 24 hours and are outside of the provisions of an academy's emergency plan and which, if not managed, could escalate into an incident potentially having severe consequences to the longer term operations, services or normal operation. Typically, such incidents would require a high-level specialised response. A business continuity incident need not be physical. It may be one that could lead to reputational damage without any associated material loss.

2. **Emergency Plan Incident:** An event causing a disruption in duration of, typically, 24 hours or less. Each academy's emergency plan contains the following information (also refer to appendix C.):

- Evacuation / Shelter / Lockdown: Definitions and Principles
- Closing the Academy
- Extreme Weather
- Infectious Diseases
- Deaths / Major Injuries
- Gas Emergency
- Left Child / Missing Child Procedure
- Flooding
- Power Cuts
- Asbestos Release
- Academy site information
- Suspicious Packages and Bomb Threats
- Malicious Intruders

The Trust Director of Estates and Facilities and the Trust Director of Performance and Standards for each school is a permanent member of the Emergency management Team (EMT) at each academy and will invoke the Business Continuity Plan if the level of disruption initially meets, or subsequently escalates to meet, the criteria set out in definition 1.

Escalation

The incident management team (IMT) will be assembled by the person invoking the plan using the contact numbers in Table 2. The person invoking will direct the team to one of the incident control rooms listed in Table 1. The incident commander may, alternatively, convene meetings and manage an incident via Microsoft Teams rather than arranging face-to-face meetings in the event of an infectious disease or pandemic. The incident commander will contact the Board to make them aware that the Business Continuity management plan has been invoked. An extraordinary meeting may be convened if required.

Should any further staff be required to populate the Incident Management Team they will be contacted individually by the IMT via phone or email.

Initial contact with staff to explain the situation will be made via phone, email or text messaging, as appropriate, to the permanent members of the Incident Management Team (IMT) (please refer to Table 2).

The IMT can only be stood down on the instruction of the incident commander.

Incident Control Room

The location of the meeting place where the Incident management team will convene.

Table 1. Incident control room location

Location	Contact details	Resources available
Preferred: OLOL Head Office, Loxley House, First Floor West, Tottle Road, Riverside Business Park, Nottingham NG2 1RT	Tel: 0115 851 54 54	Secure facility; IT and infrastructure; Telecommunications
Backup: The Becket School, Becket Way, Wilford Ln, West Bridgford, Nottingham NG2 7QY	Tel: 0115 982 4280 Site Manager Tel: 07775 022 601	Secure facility; IT and infrastructure; Telecommunications

Incident Management Team (IMT)

The group of individuals responsible for implementing a plan in response to an incident. The team consists of a core group of specialist decision-makers prepared to respond to any situation and is led by the incident commander.

Table 2. Permanent members of the Incident Management Team (IMT)

Role	Responsibilities	Person responsible
Incident commander	▪ Take overall control of the incident ▪ Allocate roles and responsibilities ▪ Establish the strategic objectives of the response to the incident ▪ Determine recovery policy and long- term strategy ▪ Second other staff to the team as required ▪ Take strategic decisions and authorise expenditure ▪ Provide regular team briefings and updates	CEO
Deputy Incident commander(s)	<u>In the absence of the Incident Commander:</u> ▪ Take overall control of the incident ▪ Allocate roles and responsibilities ▪ Establish the strategic objectives of the response to the incident ▪ Determine recovery policy and long- term strategy ▪ Second other staff to the team as required ▪ Take strategic decisions and authorise expenditure ▪ Provide regular team briefings and updates	Deputy CEO Directors of Performance & Standards
Record keeper	▪ To record all actions taken and decisions made ▪ To record all expenditure ▪ To record all other relevant information ▪ To present the information in the post-exercise debrief	Executive Assistant
Media liaison	▪ Agree and issue media statements ▪ Monitor the media channels for latest developments	Executive Assistant

	▪ Liaise with Madeleine Strezynski, Diocesan Communications Officer madeleine.strezynski@dioceseofnottingham.uk to ensure clarity and consistency of message	
Director of IT	▪ Ensure that the IT disaster recovery plan is expedited effectively ▪ Comms reinstatement	Director of IT
Director of Estates and Facilities	▪ Damage assessment ▪ Securing of the site ▪ Utility isolation and/or provision ▪ Emergency services liaison ▪ Co-ordinate relocation to alternate premises	Director of Estates
Director of Finance	▪ Providing financial resources to enable key staff to carry out their responsibilities	COO
HR Manager	▪ Identifying people who have key skills and knowledge ▪ Training individuals to acquire additional skills and knowledge ▪ Keeping a list of retired or ex-employees with key skills and knowledge that can be called up when required ▪ Outsourcing a portion of the work requiring key skills and knowledge to a third party that has the capability of taking over more of the work at short notice	HR Manager

Financial Authority

Table 3. Pre-approved financial authorities following invocation

Role	Person	Pre-approved financial authority (£K's)
Incident commander	CEO	£200,000
Deputy Incident commander(s)	Deputy CEO	£200,000
Deputy Incident commander(s)	COO	£200,000

Appendix A – Incident Management Checklist

Table 4. Incident management checklist

	Task	Owner	Completed
1	Start action log	Executive Assistant	
2	Account for staff (whereabouts and well-being)	Incident commander (Headteacher if a school site)	

3	Identify skill gaps (if any)	Incident commander	
4	Dispatch team members to site	Incident commander	
5	Liaise with emergency services and identify salvage priorities	Director of Estates	
6	Identify and assess damage	Director of Estates	
7	Identify disrupted activities	Incident commander (Headteacher if a school site)	
8	Secure damaged asset/building	Director of Estates	
9	Review critical functions priority list	Incident commander	
10	Identify appropriate recovery strategy and strategic response	Incident commander	
11	Decide on a course of action and allocate duties	Incident commander	
12	Convene operational recovery teams	Incident commander	
13	Communicate details to staff and stakeholders	Incident commander (Headteacher if a school site)	
14	Prepare media statement and communication strategy (refer to appendix H - CMAT Crisis Communications Strategy)	Incident commander	
15	Inform Insurance company/broker/loss adjuster	Director of Estates	
16	Set up helpline and update the website(s)	Executive Assistant; Director IT	
17	Ensure adequate resources to man phone lines and communicate with all stakeholders	Director of IT	
18	Contact stakeholders and suppliers	Incident commander	
19	Update the board and other stakeholders	Incident commander	
20	Arrange a debrief	Incident commander	

21	Review incident management plan and reassess priorities	Incident commander	

Appendix B - Recovery Plans

Table 5. Incident management plan - People

People		
Optimum timescale for recovery	2 days	
Recovery plan(s)	**Person responsible**	**Status**
▪ Identifying and documenting details of which people have key skills and knowledge	**HR Manager**	**In progress**
▪ Training individuals to acquire additional skills and knowledge	**HR Manager**	**In progress**
▪ Documenting key processes to allow staff to undertake roles with which they are unfamiliar	**HR Manager**	**In progress**
▪ Keeping a list of retired or ex-employees with key skills and knowledge that can be called up when required	**HR Manager**	**In progress**
▪ Using people with the relevant skills and knowledge from a third party (either through a contractual arrangement or keeping a list of suitable third parties)	**HR Manager**	**In progress**
▪ Geographical separation of individuals or groups with key skills and knowledge	**HR Manager**	**In progress**
▪ Outsourcing a portion of the work requiring key skills and knowledge to a third party that has the capability of taking over more of the work at short notice	**HR Manager**	**In progress**
▪ Ensure all job descriptions are up-to-date	**HR Manager**	**In progress**

Table 6. Incident management plan - Premises

Premises		
Optimum timescale for recovery	Head office loss – short term 2 days to relocate Full school block loss - 2 weeks to delivery of temporary accommodation	
Recovery plan(s)	**Person responsible**	**Status**
▪ Using available space at another of the Trust's sites, where possible (this might include meeting rooms, training space, canteens, etc)	**Incident commander**	**In place**
▪ Increasing staff density at another of the Trust's sites (sometimes referred to as 'budge-up')	**HR Manager**	**TBC**
▪ Displacing staff undertaking less urgent activities from another of the Trust's sites and using the space made available (care must be taken when using this option that backlogs of the less urgent work suspended do not become unmanageable)	**HR Manager**	**TBC**
▪ Remote working includes the concept of 'working from home', and working from other non-corporate locations like hotels. Working from home can be a very effective solution but care must be taken to ensure health and safety issues are addressed, suitable IT equipment with properly licensed software is provided and sufficient networking capacity/technical support is available	**HR Manager / Support/Director of IT**	**In place**
▪ List of available premises or potential suppliers of premises to find alternative premises after the disruption - suitable for activities with relatively long optimum timescale for recovery	Director of Estates	**In place**
▪ Mobile accommodation –brought into use rapidly.	Director of Estates	**In place**

Table 7. Incident management plan - Premises

Data (electronic and paper)		
Optimum timescale for recovery	Business Critical Systems (MIS, Authentication) – 1 day, All systems – 3 days	
Recovery plan(s)	**Person responsible**	**Status**
▪ **Backups** – backing up the information held in the computer systems and storing the backups in a safe and secure location that is geographically separated from the computer systems on which the original information is held and where possible Cloud based for business critical systems. Restores may rely on reinstatement of Managed Network Services	**Academy IT Support/Dir. IT**	**In place**
▪ **Virtualised Systems –** Systems are virtual servers allowing a range of physical hardware to be used and easily replaced	**Academy IT Support**	**In place**
▪ **Ad-hoc** – As virtual servers, physical servers/equipment can be purchased from available stock to suit requirements of the situation	**Director of IT**	**In place**
▪ **Standby equipment** – Sites or Trust may hold retired equipment, where suitable, or new equipment, to be used as a temporary system for initial restoration of critical systems from backups whilst awaiting replacement equipment	**Academy IT Support/Dir. IT**	**In place**
<u>Paper</u>		
▪ Do nothing – accept the loss.		
▪ Copy the paper records and store the copies at a site geographically separated from where the original records are held	**Academy IT Support/Dir. IT** **Academy IT / Academy**	**In progress** **In progress**
▪ Scan the paper records and store the images electronically (the electronic records can be held either at the same site, with backups held elsewhere, or at a geographically separated site).	**Admin** **Academy IT / Academy Admin**	**Upon invocation/ need**
▪ Recreate the paper records as best as possible from information supplied by staff, customers, suppliers, and other stakeholders		

Table 8. Incident management plan - Communications

Communications		
Optimum timescale for recovery	2 days	
Recovery plan(s)	**Person responsible**	**Status**
▪ Manual call diversion – calls diverted through provider portal or call to provider, to Trust provided number	**Academy IT Support/Dir. IT**	**In place**
▪ Broadcast notification to staff and other stakeholders of alternative numbers to call	**Academy Admin Staff**	**In place**
▪ Managed network services – restore of managed network service including physical infrastructure, router etc	**Dir. IT/Academy IT Support/Network Supplier**	**In place**
▪ Use of mobile telephones – although this cannot be relied upon as mobile telephone communications may be switched off, or become over-loaded, following a major incident	**Director of IT**	**In place**

Table 9. Incident management plan - Machinery/equipment/utilities

Machinery/equipment/utilities		
Optimum timescale for recovery	1-2 days temporary plant; 5-7 days direct replacement (portable equipment); 5-14 days (fixed plant)	
Recovery plan(s)	**Person responsible**	**Status**
General equipment used day to day in normal business processes.		
▪ Support agreements with third party suppliers to replace equipment in a pre-defined time period.	Director of Estates	**In place**
▪ Mechanical plant has redundancy built-in	Director of Estates	**In place**
▪ Portable heaters held across the Trust which can be transported to sites	Director of Estates	**In place**
▪ Catering equipment – full replacement (modular) kitchen as required.	Director of Estates	**In place**
▪ On-site maintenance or maintenance contracts with guaranteed service levels	Director of Estates	**In place**
▪ Changing equipment from bespoke to generic – Estates / IT joint procurement strategy	Director of Estates **/ Director of IT**	**In place**
▪ Uninterruptible power supply (UPS) – to cover short power outages and enable the safe shut down of equipment (particularly computers).	Director of Estates **/ Director of IT**	**In place**
▪ Portable generators – shipped in when required. Standby back-up generator point available at CTK for domain controller replication.		

Table 10. Incident management plan - Suppliers

Suppliers		
Optimum timescale for recovery	2 days	
Recovery plan(s)	**Person responsible**	**Status**
▪ Dual-sourcing of supplies	Director of Estates **/**	**In place**
▪ Identification and pre-acceptance of alternative suppliers	**Director of IT**	**In place**
▪ Asset Inventories up to date	**Head of Finance**	**Policy in progress**

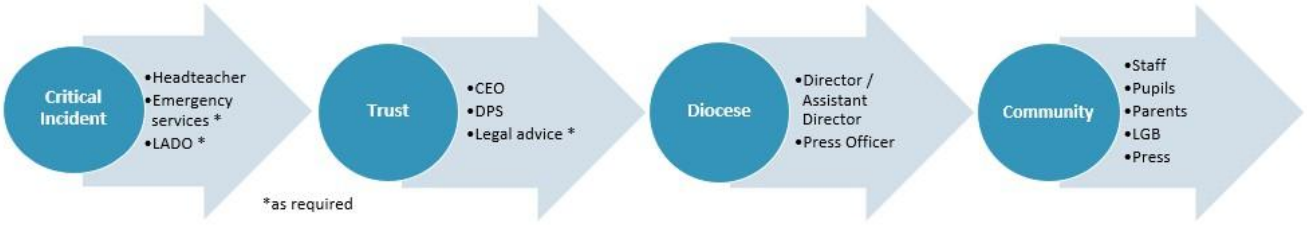
Appendix C - CMAT Crisis Communications Strategy

CMAT Crisis Communications Strategy

This document provides advice on how to respond to a crisis in terms of communication with key stakeholders. It should be considered in conjunction with other relevant policies, dependent on the type of incident (e.g. safeguarding, disciplinary, disaster recovery, critical incident, bereavement etc).

As ever, the first priority should be the safety, health and well-being of pupils, staff and the wider community. Once this is established, the following communications protocol should be followed:

- Emergency services should be called if required
- Headteacher (or deputy) should be informed immediately
- The Headteacher should contact the CEO and/or DPS (CEO to inform Trust Board as required)
- Senior Trust staff should contact the Director NRCDES (or deputy) – Director to inform the Diocesan Bishop as required
- Diocesan Press Officer should be contacted - no comments should be made to the press (front office made aware). Agreed statement prepared.
- Decision made between HT and CEO / DPS about communication with other school stakeholders (pupils, parents, governors).
- It may be necessary and important to share information with stakeholders to avoid rumours / additional panic or worry. The content of this communication should be decided by CEO/DPS and HT in liaison with the press officer. This communication is likely to be used by the press.



Key Contact details:

Name	Role	Contact details
James McGeachie	Incident commander	07805 631202 / 0115 8515454
Moira Dales	Deputy Incident commander	07852 133114 / 0115 8515454
Peter Giorgio	Director NRCDES	01332 293833
Eva Callaghan (County) Eve Hailwood (City)	LADO LADO	0115 8041498 0115 8764148
Madeleine Strezynski	Diocesan Communications Officer	madeleine.strezynski@dioceseofnottingham.uk / 07988 789507

Appendix D - Academy Emergency Plan Format

1. Evacuation / Shelter / Lockdown: Definitions and Principles
    a) Evacuation (standard): Remain on the academy site
    b) Evacuation (off-site): To a pre-arranged place of safety
    c) Shelter: (or internal/inwards evacuation: “invacuation”)
    d) Lockdown
2. Closing the Academy
    a) Background
    b) Safety of Pupils
    c) Home to Academy Transport
    d) Closure due to a funeral
    e) Water supply disruption
    f) Heating disruption
    g) Exam disruption
3. Extreme Weather
    a) Staff Considerations
    b) Plant Room Considerations
4. Infectious Diseases
    a) Role of Public Health England (Institute of Population Health)
5. Deaths / Major Injuries
6. Gas Emergency
    a) Procedure
    b) Engineer Call
    c) Indoor Gas Leaks
    d) Next Steps
    e) Carbon Monoxide
7. Left Child / Missing Child Procedure
8. Flooding
9. Power Cuts
    a) What to do during a power cut
    b) Fallen power lines
    c) Contacting the Distribution Company
10. Asbestos Release
11. Academy site information
12. Suspicious Packages and Bomb Threats
    a) Suspect Packages
    b) Bomb Threat via Phone Call, E-mail or Social Media
    c) Media and Communication
13. Malicious Intruders
    a) Contacting the Police
    b) Alerting Staff
    c) Emergency Procedure to Follow
    d) Armed police response
14. Emergency contacts list including key holders
15. Communications
    a) Media Handling
    d) Communication Response Protocol
16. Emergency arrangements for other services using the academy site
17. Training and exercising