BUSINESS CONTINUITY PLAN

Issued: December 2019

Document History

All members of the Incident Management team should receive the latest version of this document when it is updated.

Version	Date	Author	Status	Comment/Description of change
1.00	20.11.19	Fern Holmes	DRAFT	Created plan

Test Record

The following table describes tests that have taken place to validate the plan.

Date	Description of test exercise	Parties involved in test	Other notes
No tests have been recorded.			

1 Introduction

1.1 Background

Business Continuity Management is an ongoing planning process to enable continued provision of core activities throughout any kind of disruptive incident. This may loss of access to premises, loss of key staff, IT outage, power cut etc.

1.2 Purpose

The purpose of this plan is to facilitate the maintenance and rapid recovery of the Trust's most critical activities and to enable efficient incident management. The plan does not endeavour to cover every imaginable contingency but should be used as a flexible guide to assist management decision making. All procedures should be followed with a common sense approach, with regard at all times for the welfare of staff, students and the wider community.

1.3 Plan Owner

Fern Holmes (Trust Finance & Operations Director) is the owner of this plan and is responsible for updating it on a regular basis to reflect any significant business change. The plan will be completely reviewed and updated once every 12 months.

1.4 Contents

A business continuity plan is a collection of four important documents:

- **Incident Management Plan**
  How to escalate serious incidents and decide whether to invoke the business continuity plan.
- **Key Contact Details**
  Getting hold of persons and organisations that you need
- **Incident Response Plans**
  The planned response to key threats
- **Key Supporting Documents**
  Documents to support the business continuity response

2 Incident Management Plan

2.1 Purpose

The purpose of this section is to define an incident response structure that would be required in the event of an incident occurring at the Trust. In doing so it outlines the key roles and responsibilities in responding to and recovering from an incident.

In accordance with BS ISO22301 there is a need for an incident management team to:

- *Have a process for activating the response*
- *Details to manage the immediate consequences of a disruptive incident*
- *Details on how and under what circumstances the organization will communicate with employees and their relatives, key interested parties and emergency contacts*
- *Details of the organization's media response following an incident*
- *A process for standing down once the incident is over*

This section is not intended to be a prescriptive list of actions to take to manage an incident but should be used as a flexible guide to assist management decision making.

Key sections include:

- The Incident Management Structure e.g. key people responsible for overseeing the co-ordination of a response and where they would meet
- The process for escalating an incident and for invoking the plan
- A checklist of actions for senior managers
- An incident assessment form template
- An incident log template

2.2 Incident Management Team structure

The incident management team is made up of the Chief Executive Officer, Finance & Operations Director, Finance Officer and Trustees, as available. The team needs to form and react as soon as possible to the incident. On forming, those present can take decisions to apply appropriate resources to deal with an event as it occurs (ideally to prevent it becoming a crisis).

The key roles of the Incident Management Team are to:

- Provide strategic direction, especially at a local level
- Hold ultimate responsibility
- Represent the public face of the School
- Assume responsibility for co-ordinating incident management
- Provide direction / support as required to staff and students and outside agencies to effectively manage the incident at an operational level.

The table below shows the members of the Incident Management Team

Name	Role	Deputy
Damian Chubb	CEO	Fern Holmes
Fern Holmes	Finance & Operations Director	Claire Holmes
Claire Holmes	Finance Officer	
Trustees	Trustees	

2.3 Incident Management Team Meeting Room

In the event of an incident, the Incident Management Team will meet in a nominated venue. The first choice of venue is as follows:

	First Choice
Nominated meeting room	Trust Finance Office, Thornaby CofE Primary School
Capacity	8
Equipment Held in Room	ICT, phones, paper records
Status *	Operational

** This is a measure of the readiness of the room at the time this plan was created.*

In the event that the first choice is unavailable, the incident management will meet in the second choice venue below:

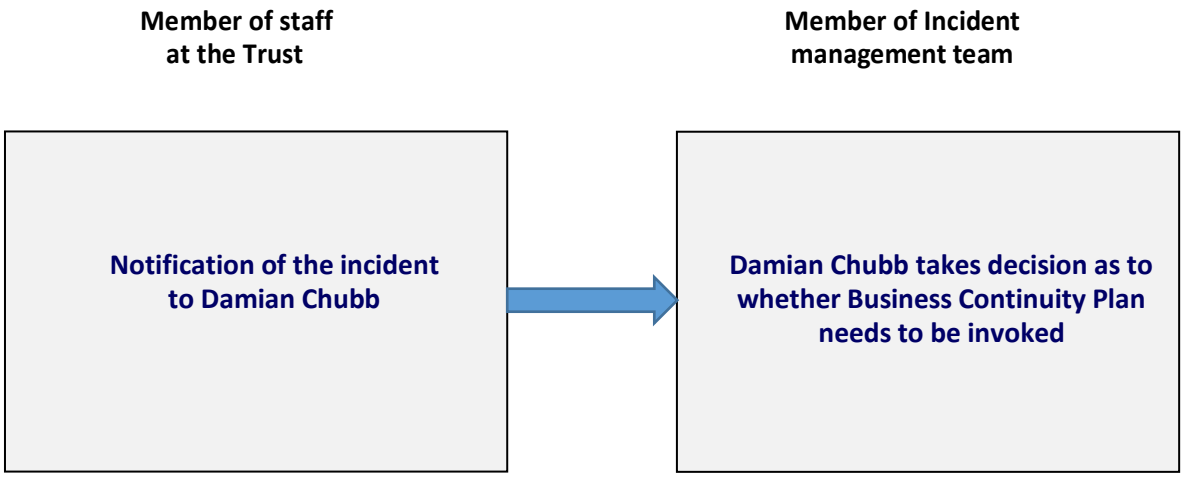
	Second Choice
Nominated meeting room	Senior Assistant Headteacher's Office, All Saints CE Academy
Capacity	6
Equipment Held in Room	ICT, phones
Status *	Operational

The CEO has the authority to compel all members of the Incident Management Team to meet as soon as is reasonable (regardless of the time of year) to discuss an incident (or the threat of an incident) which could force the Business Continuity Plan to be invoked.

2.4 Incident escalation and invocation of the BCM Plan

The Trust has a clear and simple method by which it can quickly recognise a business continuity threat and act accordingly. It is better to over-react to serious incidents and then stand down members of staff than to under-react.

The agreed escalation and invocation framework (to be adopted and understood by all) is set out below.



If Damian Chubb is unavailable the following person(s) can act as a deputy:

- Fern Holmes

If Damian Chubb is unavailable the following person(s) can act as a deputy:

- Fern Holmes

2.5 Checklist of actions for the Incident Management Team

In the event of a business continuity threat complete the following checklist of actions to ensure that all of the important steps to manage the incident have been considered.

No	Action	Completed by
1	Decide to invoke the business continuity plan	
2	Open an incident log (ref: Ref: Section 1 Appendix B) to record key actions and decisions taken	
3	Determine the nature of the incident, the extent of impact on the Trust and assess priorities. (Ref: Section 1 Appendix A - Incident Assessment Form)	
4	Identify which threat response plan(s) would be invoked (ref: Section 3 of the BCM plan)	
5	Call team together	
6	Inform Trust Board members	

2.6 Incident record

The following table describes incidents that have taken place and how the plan performed

Date	Description	How the plan performed	Other notes
No previous incidents have been recorded			

Appendix A - Incident Assessment Form

This table is to be used by the Incident Management Team for completing an initial assessment of which Mission Critical Activities have been impacted and the likely duration of the impact.

Priority Order	Mission Critical Activity	Recovery Requirements	Nature of Impact	Duration
1	Provision of leadership	Ensure robust leadership in crisis		
2	ICT support	Ensure ICT support for communications and information		
3	External communications with key stakeholders	Require phones and ICT		
4	Internal communications with Staff and Trustees	Require phones and ICT		
5	Ensuring safety of staff and Trustees (Duty of Care)	Ensure central staff safe and secure		
6	Running of MAT	IT; phones; files; workspace		
7	Loss of Offices	IT, phones, files, workspace		

Appendix B - Incident Log

This table is to be used by the Incident Management Team during the incident to record any action taken or decisions made.

Entry No.	Date	Time	Description of action taken / decision made	Costs incurred	Completed by

3 Key Contact Information

3.1 Purpose

The purpose of this section is to facilitate contact of key business continuity management stakeholders.

3.2 Contents

A business continuity plan contains a collection of information:

- Public Section
- Confidential Section
- External Communication Welfare
  - ◊ Key External Stakeholders
  - ◊ Emergency Services
  - ◊ Staff Welfare
  - ◊ Disaster Recovery

3.3 Public section

The public section does not contain home telephone numbers.

Business continuity contacts for:
DALES ACADEMIES TRUST

Name	Role	Work main number	Work alternative/Mobile
Damian Chubb	CEO	03301242618	07876 684655
Fern Holmes	Finance & Operations Director	03301242618	07908 545248
Claire Holmes	Finance Officer	03301242618	N/A

3.5 External communication

Organisation	Contact details	Policy/Account Number/Other Information
Travellers Insurance	Contract Tracey Smith at Towergate below Alternately contact Towergate; 0800 5878388	Insurance policy UC CMK 5560614
Towergate	Tracey Smith – 0113 2368561; 07702 367079 Out of hours; 0203 394 1620	
Dales Board	See contacts list	N/A
Dioceses	See contact list	N/A
Academies	See contacts list	N/A
Health & Safety (North Yorkshire)	Terry Bland 07813007289 Out of hours: 0845 0349437	N/A
IT (OneIT)	01642 635570	

4 Threat Response Plans

4.1 Purpose

The section contains the planned response to key threats.
Each threat response plan is detailed on separate pages (below).

4.2 Threat Response Plan for: Loss of Site

Plan Owner *This person owns the threat response plan and has confidence in it.*	Fern Holmes
Deputy Plan Owner *This person also has confidence in the plan and is responsible for maintenance of the plan.*	Claire Holmes

Possible Triggers:	Fire Theft Power failure Flood Explosion

Risk Assessment:	**Likelihood:** Low **Impact:** High **Risk Rating:** Medium

Risk Width *(i.e. critical activities that could be affected)*	• ICT support • External communications with key stakeholders • Internal communications with staff • Ensuring safety of staff (Duty of Care)
Current Mitigating Actions:	Fire precautions, regular alarm tests, PAT testing.
Future Mitigating Actions:	

No.	Threat response action for Loss of Site	Who is responsible	Action completed?
1	Contact Towergate Assist - Loss Assessor - 0203 3941620	Fern Holmes	
2	Seek alternative premises	Fern Holmes	
3	Short term relocation e.g. to All Saints	Claire Holmes	

4.3 Threat Response Plan for: Loss of Staff

Plan Owner *This person owns the threat response plan and has confidence in it.*	Damian Chubb
Deputy Plan Owner *This person also has confidence in the plan and is responsible for maintenance of the plan.*	Fern Holmes

Possible Triggers:	• Fire • Flu pandemic • Weather • Transport problems • Train crash • Virus • Bus crash • Stabbing or fatal incident • Terrorism incident • Car crash involving individual/multiple staff • Murder/suicide

Risk Assessment:	**Likelihood:** Low **Impact:** Medium **Risk Rating:** Medium

Risk Width *(i.e. critical activities that could be affected)*	• Provision of leadership • External communications with key stakeholders • Internal communications with staff • Ensuring safety of staff (Duty of Care)

Current Mitigating Actions:	Overlap in some job roles, well briefed staff, contact with Trustees, ongoing partnership with BDAT
Future Mitigating Actions:	

No.	Threat response action for Loss of Staff	Who is responsible	Action completed?
1	Reallocate tasks	Damian Chubb	
2	Contact with Trustees	Damian Chubb	

4.4 Threat Response Plan for: Loss of IT/Phones

Plan Owner *This person owns the threat response plan and has confidence in it.*	Fern Holmes
Deputy Plan Owner *This person also has confidence in the plan and is responsible for maintenance of the plan.*	Claire Holmes

Possible Triggers:	Fire Flood/sprinkler leakage/burst pipes Power failure Theft Explosion

Risk Assessment:	**Likelihood:** Medium **Impact:** High **Risk Rating:** High

Risk Width *(i.e. critical activities that could be affected)*	• ICT support • External communications with key stakeholders • Internal communications with staff

Current Mitigating Actions:	Resilient network, remote working, cloud storage, off-site backup, anti-virus, managed services
Future Mitigating Actions:	Cloud-based applications

No.	Threat response action for Loss of IT/Phones	Who is responsible	Action completed?
1	Decide on alternate ways of working	Fern Holmes	
2	Contact Towergate Assist - Loss Assessor – 0203 3941620	Fern Holmes	
3	Contact OneIT	Fern Holmes	

4.5 Threat Response Plan for: Health incident

Plan Owner *This person owns the threat response plan and has confidence in it.*	Damian Chubb
Deputy Plan Owner *This person also has confidence in the plan and is responsible for maintenance of the plan.*	Fern Holmes

Possible Triggers:	• Virus • Health incident • Accident

Risk Assessment:	**Likelihood:** Low **Impact:** Medium **Risk Rating:** Low

Risk Width *(i.e. critical activities that could be affected)*	• Running of MAT

Current Mitigating Actions:	Routine vaccinations, health awareness, regular cleaning and sanitising
Future Mitigating Actions:	If warning signs of virus take additional precautions, increase cleaning routines, personal hygiene etc.

No.	Threat response action for Health incident	Who is responsible	Action completed?
1	Reallocation of tasks	Damian Chubb	

5 Key Documents

5.1 Purpose

In the event of a disruptive incident there are a number of key documents which may need to be referred to in order to effectively manage the emergency.

5.2 Summary of key documents and location

The table below identifies possible example documents that may be required should an incident occur:

Document or File	Location	Format	Owner
Paper records	MAT office, Thornaby Primary	Soft and Hard copies	Fern Holmes
Contracts	MAT office, Thornaby Primary	Soft and Hard copies	Fern Holmes
Personal files	Bishop of Whitby's Office	Soft and Hard copies	Damian Chubb