BUSINESS CONTINUITY & EMERGENCY PLANNING STRATEGY

Section 1: Incident Management Plan

Section 2: Key Contact Information

Section 3: Threat Response Plans

Section 4: Key Documents

Document Owner	Chief Operating Officer
Reviewed, updated and Approved by Trustees	September 2025
Scheduled for Next Review	September 2027
Contact details to be updated:	As needed, at least annually

Contents

SECTION I Incident Management Plan

1.1 Purpose & Scope of this document

The purpose of this document is to assist Endeavour MAT (EMAT) and its constituent schools to define an incident/ emergency response structure that would be required in the event of an incident/ emergency occurring or looking likely to occur. In doing so it outlines the key roles and responsibilities in responding to and recovering from an incident/ emergency and preparations to mitigate the impact of such.

The Business Continuity Standard –

"In any incident situation there should be a simple and quickly-formed structure that will enable the organisation to:

- *Confirm the nature and extent of the incident*
- *Take control of the situation,*
- *Contain the incident, and*
- *Communicate with stakeholders"*

This document is not intended to be a prescriptive list of actions to take to manage an incident but a guide to support an effective approach in practice.

In considering the needs of the Trust and its schools it is meaningful to distinguish between the school specific and the Endeavour Central Team or Trust-wide. As a result this strategy is in two parts:

- An overarching approach to be taken across the Trust via the use of templates to be completed by each EMAT school for school specific information and issues.
- The detailed approach to be taken in relation to the Central Team or Trust-wide issues.

In order to complement and complete the coverage of the organisation in respect of business continuity and emergency planning each EMAT school will have its own document following this format (template provided by the Central Team alongside this document) and dovetailing the approach across the Trust.

1.2 Incident Management Team (IMT)

IMT structure

The Central Team as well as each EMAT school will identify the core members of its IMT (made up of the Headteacher (HT) and Senior Leadership Team (SLT)) and other key staff and those co-opted as required. The team needs to form and react as soon as possible to the incident/ threat. 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 IMT are to:

- Provide strategic direction at the appropriate level
- Hold responsibility for the actions to be taken
- Represent the public face of the School/ Trust
- 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 Central Team/ Trust-wide IMT

Role	Deputy
Chief Executive Officer (CEO)	Deputy CEO – for Education & Safeguarding matters Chief Operating Officer – for all other matters
Chief Operating Officer (COO)	Head of Business Management or Finance (as appropriate)
Head of Governance & Compliance (also DPO)	Head of Student Records, Data & Systems
Head of IT	Deputy Head of IT
Head of Premises	Deputy Head of Premises
Head of HR	HR Manager

It is noted that any the BCEP arrangements for any individual EMAT school and those of the Central Team/ Trust-wide are complementary and interleaving, with keyCentral Team staff available and necessary to supplement any school based IMT as indicated by their role and expertise.

It may also be necessary for an issue which first emerges at an individual school level to become a Trust-wide issue, ultimately managed by the Central Team IMT. Similarly Trust-wide issues may require school based IMT action.

1.3 The Central Team/ Trust-Wide IMT Meeting Room/ Virtual Venue Option

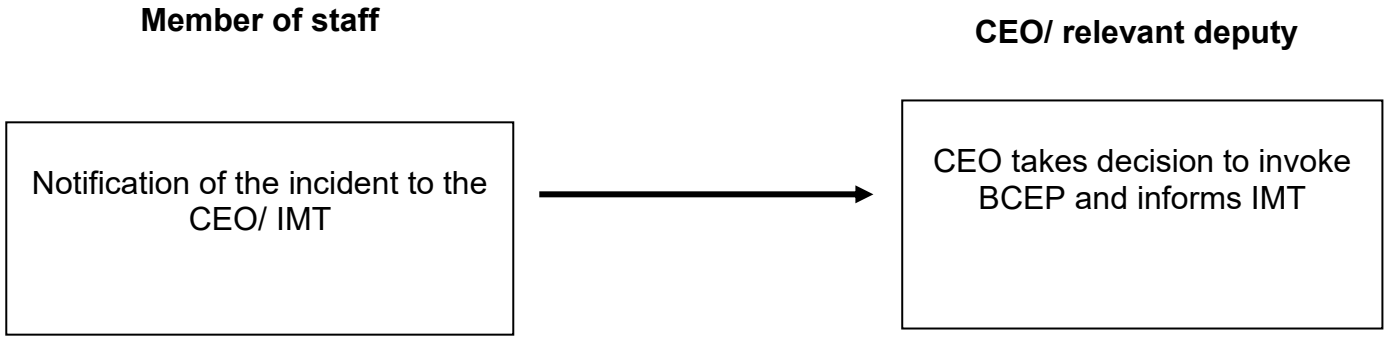
	First Choice	Second Choice	Third Choice	Virtual Venue Option (Teams)
Nominated Meeting Rooms	CEO's Office	The Grange meeting room	Classroom to be requisitioned as needed	This may be utilised by necessity or choice
Capacity	6	12	32	300
Computer Equipment Held in Room	Yes	No	Yes	A pre-requisite for participation
IT Network Point(s) in Room	Yes & Wi-Fi	Yes & Wi-Fi	Yes & Wi-Fi	See above
Other Specialist Equipment Held if Necessary (e.g. Digital TV & Radio, fax)	Full office facilities	None	None	Screen sharing and virtual collaboration

1.4 Incident escalation and invocation of the Business Continuity & Emergency Planning Strategy (BCEP)

Incident escalation process – the Central Team/ Trust Wide

It is vital that there is a clear and simple method by which a business continuity threat can be recognised and acted upon. 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.



The CEO/ relevant deputy has the authority to compel any member of staff as relevant to meet, as soon as is reasonable, to discuss an incident/ emergency, or the threat of an incident/ emergency, which could force the BCEP to be invoked.

1.5 Example actions for the IMT – the Central Team/ Trust-wide

No	Action	Completed Yes / No
1.	Determine nature of incident and extent of impact on the Central Team/ Trust (see Appendix A – Incident Assessment Form and Appendix C – Information Gathering Log).	
2.	Ensure priorities have been identified including assessing the continuing risk and ensuring safety and welfare of staff, students and others	
3.	Decision taken to invoke BCEP.	
4.	Decide on location of meeting room. Contact other members of IMT as relevant and get them to come to the meeting room.	
5.	Open an incident log (see Appendix B) to record key actions and decisions taken.	
6	Contact the Chair of Trustees (if unavailable, contact the Vice-Chair)	
7.	Identify resources required to deal with incident	
8.	Consider implementation of a communications strategy (internal and external) and whether necessary to refer to the Local Authority, DFE or other relevant body/ bodies	
9.	Agree a time for next meeting and follow on meetings and briefing and reporting into incident log. Agree monitoring process for plan implementation and frequency of reports to CEO.	
10.	Consider the plan for recovery – (focussed on Mission Critical Activities – see Appendix D, and non-critical activities).	
11	On conclusion of incident stand down Team and instigate a lessons learnt review.	

Appendix A – Incident Assessment Form – the Central Team/ Trust-wide

This table is to be used by the IMT for completing an initial assessment of which Mission Critical Activities have been impacted and the likely duration of the impact (to be completed immediately after incident).

Priority Order	Mission Critical Activity	Accountability for Mission Critical Activity	Nature of Impact	Duration	Recovery Time Objective
1	Leadership Team	CEO			Within 4 hours
3	Telecoms	Head of IT			Within 24 -48 hours
4	ICT support –email	Head of IT			Within 24 -48 hours
5	ICT support –Internet	Head of IT			Within 24 -48 hours
5	ICT support –Network	Head of IT			Within 24 -48 hours

Appendix B – Incident Log

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

Appendix C – Information Gathering Log

Information to be gathered	
Nature of Incident	
Location of Incident	
Time of Incident	
Does the incident still present a danger/action to be taken.	
If the incident is off site (away from the Central Team main office in Parsons Lane), what help is required.	

Information to be gathered – contd.	
Number of persons injured, extent of injuries & names	No. Names:
Current location of those injured and contact details of adult present (Hospital Details if required).	
The location of students who were involved but not injured, plus the name and contact number of an adult present.	
The name and contact number of an adult at the incident site (if off-site)	
The name and contact number of police and emergency services	

Appendix D – the Central Team/ Trust-wide Business Impact Analysis (On scale of 1 – 5, where 5 represents Maximum Impact)

Mission Critical Activity	Description of Impact if the activity cannot continue	Key Resources Required	4 hrs	24 hrs	24 – 48 hrs	1 wk	2 wk	1 mth
IMT	- Unable to co-ordinate management of incident / lack of clear direction - Ineffective response - Possible delays - Incident escalates / takes longer to recover - Reputation undermined	Minimum 2 members of IMT (one of either CEO/ COO physically or virtually present) Laptops/ similar Mobile Phones	**5**	**5**	**5**	**5**	**5**	**5**
Comms	- Unable to provide information to stakeholders e.g. staff/ colleagues, media - Impact on ability to respond effectively to the incident - Rumours and misinformation spread - Incident escalates / takes longer to recover	VoiP or mobile phones Outlook web access as minimum	**3**	**4**	**5**	**5**	**5**	**5**
Site access / management (including health & hygiene)	- Unable to access the Central Team designated office(s), utilities, toilets, etc effectively - Risk to safety of staff	Key holder/ Premises Team member required.	**5**	**5**	**5**	**5**	**5**	**5**

Mission Critical Activity	Description of Impact if the activity cannot continue	Key Resources Required	4 hrs	24 hrs	24 – 48 hrs	1 wk	2 wks	1 mth
HR support	- Unable to pay staff - Criticism from staff - Loss of goodwill in responding to the incident - Impact on reputation	Payroll system & Lloyds software Contact details Lloyds (iTrent) Key staff dependency, Head of Finance/ COO	**3**	**4**	**5**	**5**	**5**	**5**
Creditors (payments)	- Unable to make payments - Difficult to obtain resources - Potential financial penalties - Impact on reputation	IT / IRIS/ Lloyds systems Key staff dependency, Head of Finance & COO	**2**	**2**	**2**	**3**	**4**	**5**
Financial management	- Impact on ability to manage finances - Impact on day to day operations and ability to do longer term planning - Potential long term financial implications	IT / IRIS/ Lloyds systems Key staff dependency, Head of Finance & COO	**2**	**2**	**3**	**4**	**5**	**5**

SECTION 2 KEY CONTACT INFORMATION

2.1 Public Section

The Central Team/ Trust-wide (May be shared with third parties assisting with the incident without express permission)	
Role	**Work No.**
Chief Executive Officer (CEO)	01322 250285 x 901
Deputy CEO	01322 250285 x 933
COO	01322 250285 x 902
Head of Governance & Compliance (inc. DPO)	01322 250285 x 912
Head of IT	01322 250285 x 906
Deputy Head of IT	01322 250285 x 927
Head of Premises	01322 250285 x 909
Deputy Head of Premises	01322 250285 x 930
Head of HR	01322 250285 x 914
HR Manager	01322 250285 x 925
Head of Finance	01322 250285 x 904
Head of Business Management	01322 250285 x 905
Head of Student Records, Data & Systems	01322 250285 x 928

2.3 External Communication

Organisation	Contact Name & Address	Title	Contact Telephone Number(s)
Key External Stakeholders			
Media Radio Local Companies	BBC Kent Radio Newshopper Kentish Times		01892 675607 01689 885702 01322 303110
Broadband andtelecoms suppliers	Broadband4 Nimvelo	Customer service (24hrs) Customer service (with out of hours option)	01202 472997 0330 120 1200
Other nearby schools	Wilmington Academy Wilmington Primary Dartford GS Girls Dartford GS Boys Oakfield Lane		01322 272111 01322 274080 01322 223123 01322 223039 01322 220831
Local Authority	Kent County Council	Out of hours Office hours	03000 41 81 81 03000 41 41 41
Emergency Services			
Fire / Police / Ambulance	Local number		101 or 999
PCSO – Neighbourhood Policing	PCSO		101 or 07989181144
Staff Welfare			
Trauma /Counselling Agencies	Health Assured		0800 0305182

Local Hotels	Hilton (Dartford Bridge) Holiday Inn Express, Dartford		01322 284 444 0871 902 1606

SECTION 3 THREAT RESPONSE PLANS

3.1 Loss of site (the Central Team main office - Manor)

3.1.1 Plan Owner

Owner:	Deputy Owner / Plan Maintainer:
Head of Premises	**Deputy Head of Premises**

3.1. 2 Risk Description

Risk	Potential Triggers of the Risk	Risk width (i.e. critical activities that will be affected)	Current Mitigation
Loss of site	Fire, explosion, flood, terrorism, power failure	Key the Central Team operations including CEOs office & central finance function	Examples: Complying with Health & Safety policy / legislation • Planned maintenance programme • Flood / Fire risk assessment plan • Regular walk of the building – list of defects noted • Good communications on site

3.1.3 Response Plan

No	Action	Timing / Priority	Responsible	Completed By
1. Actions required in the event of the incident occurring out of hours				
1.1	Security and fire alarm would trigger key holders contacted, Premises Manager/ Premises Assistant for WGSG site are contacts.	Immediate	WGSG Premises Manager	
1.2	Premises Manager/ Premises Assistant to attend site immediately to manage incident at site and liaison with emergency services	Immediate	Premises Manager	
1.3	Fire & Rescue service will be alerted by Site staff	Immediate	Premises Manager	
1.4	Premises Manager/ Premises Assistant informs Head of Premises, COO & CEO	Immediate	Premises Manager	
1.5	Incident team meets and decide what parts of the plan require implementing	Immediate	CEO	
1.6	Telephone staff per cascade system and tell them what actions they are to take	Immediate	IMT per cascade	
1.7	Notify Chair of Trustees	Immediate	CEO	
1.8	Relocate to alternative facility on site e.g. vacant space at a school site	By 8.30am	Head of Premises	
1.9	COO will contact RPA	First few hours	COO	
1.10	Premises Manager to provide regular updates to incident team	Ongoing	Premises Manager	
1.11	Review situation and wider site implications	Ongoing	IMT	
1.12	Investigate more permanent use of: - Portakabins - Other Schools facilities	Ongoing	Head of Premises	

2. Actions required in the event of the incident occurring in normal working hours				
2.1	Alarm triggers evacuation (in line with fire drill / evacuation policy)	Immediate		
2.2	Investigate whether the alarm is genuine and contact emergency services	Immediate	WGSG Premises Manager	
2.3	Senior staff to manage assembly points. WGSG Premises Manager and School Business Manager to manage incident at site and liaison with emergency services and senior management If utility failure: WGSG Premises Manager to contact utility company	Immediate	Premises Manager & senior staff	
2.4	IMT meet to decide steps to be taken and use BCEP to plan and allocate actions	Immediate	IMT	
2.5	Contact Chair of Trustees	Immediate	CEO	
2.6	Use alternative site e.g. other vacant facilities in an EMAT school	First few hours	IMT	
2.7	COO will contact RPA	First few hours	COO	
2.8	WGSG Premises Manager to provide regular updates to Incident team – incident team brief colleagues	Ongoing	WGSG Premises Manager	
2.9	Regularly review situation and wider implications	Ongoing	IMT	

3.2 Response Plan for: Significant loss of key staff

3.2.1 Plan Owner

Owner:	Deputy Owner / Plan Maintainer:
CEO	COO

3.2.2 Risk Description

Risk	Potential Triggers of the Risk	Risk width (i.e. critical activities that will be affected)	Current Mitigation
Significant loss of key staff	Flu pandemic, strike, weather, transport	All activities	• Encouraging work life balance • Agency arrangements • Early detection of possible severe weather / transport problems

Cover in place for key staff:

CEO Nominated Deputy is: COO in general matters and Deputy CEO on matters of education & safeguarding.

COO
Roles and Responsibilities picked up in short term by: Head of Finance, Head of Premises, Head of IT, Head of HR, Head of Business Management, Head of Governance & Compliance. Payroll BACS authorising role to be performed by other signatories in the short term.

In the event of an unplanned absence of more than five working days and likely to be on-going the CEO will liaise with the Chair of the Finance & Audit Committee to consider appointing interim/agency cover.

Head of Student Records, Data & Systems
A Data manager from one of the EMAT schools would be invited to act up short term..

Head of Governance & Compliance
COO to assume responsibilities in short term to medium term.

Head of Premises
Deputy Head of Premises**.**

Head of IT
Deputy Head of IT.

Head of Finance or Head of Business Management
COO to assume responsibilities in short term (with the assistance of the other post holder). In the event of an unplanned absence of more than five working days and likely to be on-going on the part of the Head of Finance interim/agency cover will be appointed.

1. Actions required in the event of a significant loss of key staff

1.1	Need to know which staff are missing –staff report absence to line manager by 8.30am.	Immediate	All the Central Team staff	
1.2	Line managers assess which roles/ commitments/ meetings need covering – find alternative cover from within the Central Team or reschedule	Immediate	the Central Team	

1.3	CEO/ COO to inform Chair of Trustees if/ as necessary	Immediate	CEO/ COO	
1.4	Regularly review and monitor situation and absence levels (every 2 – 3 days) and keep all stakeholders involved	Ongoing	IMT	

Response Plan for: Loss of ICT (NOTE: there is a separate Cyber Response Plan)

3.3.1 Plan Owner

Owner:	Deputy Owner / Plan Maintainer:
Head of IT	**Deputy Head of IT**

3.3.2 Risk Description

Risk	Potential Triggers of the Risk	Risk width (i.e. critical activities that will be affected)	Current Mitigation
Loss of IT / Loss of phones	Virus, hacking, sabotage, theft, fire, flood, water leak, loss of power, defective hardware	Operation of all the Central Team activities including central finance processing and payroll.	• All data is backed up and a copy is taken off site or cloud hosted • All program licences will allow re-use of corrupted programs • RPA cover at levels adequate to replace all hardware if lost • Firewalls and secure log ins

3.3.3: Response Plan

No	Action	Timing / Priority	Responsible	Completed By
Critical systems for the Central Team: • SIMS (24 hrs) • User areas (48 – 72 hrs) • Email (48 hours) • Internet (24 hours) • Finance (48 hours)				
1. Actions required in the event of a loss of IT services				
1.1	If staff have IT related issues they contact the IT Manager at WGSG	Immediate	IT Managers	
1.2	Try to resolve issue internally (4 hour response)	Immediate	IT Managers	
1.3	If relevant arrange to implement external support provided under maintenance and collaboration contracts	Immediate	IT Managers	
1.4	Progress tracked through the help desk	Immediate	IT Managers	
1.5	For major breakdowns and escalation of minor problems the ICT Technicians will advise the Head of IT of the scale of the issue and the time and cost required to resolve	Immediate	IT Managers	
Contingency plan for loss of User Areas				

1.6	Head of IT - Disseminate information to all staff including details of time required to resolve – alternative procedures in place etc - If server down – access backups – restore data from backups to a working server - Once restored – test data – disseminate information to everyone	Immediate	IT Managers	

SECTION 4 KEY DOCUMENTS

Summary of key documents and location

Should a significant incident occur there are a number of key documents which may need to be referred to in order to effectively manage the emergency.

Below are a few questions which may assist in identifying and accessing key documentation.

- What key documents would be required or prove useful should a significant incident occur?
- How accessible are these documents?
- What format are the documents in e.g. electronic, paper?
- Who is the owner of the document(s)?
- Are the documents the most up to date versions?

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

4.1 Table summarising key documents and location

Document or File Name	Location	Format	Document Owner
BCEP	All members of IMT,	All members of IMT – hard copies & electronic	COO
Key contract documents	Trust Finance Office – hard copy electronic copy available	Hard copy and electronic	COO
Key legal and financial documents	RPA documents – COO's office	Hard / electronic	COO