CONTINGENCY AND BUSINESS CONTINUITY POLICY
OCTOBER 2024

Approved: Trust Board
Version 1.3

Contingency and Business Continuity Policy

Date Policy Reviewed / Developed:	**June 2021** **March 2023 (review)** **July 2024 (review)** **September 2024 (review)**	
Title:	**Contingency and Business Continuity Policy**	
Summary of Policy:	**This policy sets out the Esteem Multi-Academy Trust's approach to planning and responding to major incidents which affect the continuity of its business and the safety of its staff, pupils and stakeholders. The Academies Financial Handbook states that Trust's must recognise and manage present and future risks, including contingency and business continuity planning, to ensure continued and effective operations.** **The Trust will ensure that business continuity management is embedded within its culture and that all those connected with the delivery of services, including partners and key suppliers are fully aware of their roles and responsibilities in ensuring business continuity.**	
Policy Authors:	Mandy Lee – Dep CEO	
Policy Agreed By: Trust Board/CEO/Committee	Agreed By: Trust Board	Date: June 2021 (First Approval) October 2024 (Latest Approval)
Additional documents/references related to this policy:	Academy Emergency Plans Central Team Emergency Plan Trust and Academy Cyber Response Plans Academy Trust Handbook 2024 Esteem MAT Schools Emergency Plan Template Esteem MAT Schools Business Continuity Plan Template DfE Emergency planning and response for education, childcare, and children's social care settings October 2022 DfE Protective security and preparedness for education settings April 2024	
Academy Specific / MAT wide	MAT wide policy	
Review Period:	1 year	
Date Review Due:	July 2025	

EMAT Contingency and Business Continuity Policy

1. Introduction

1.1 This policy sets out the Trust's approach to planning and responding to major incidents which affect the continuity of its business and the safety of its staff, pupils and stakeholders. The Academies Financial Handbook states that Trust's must recognise and manage present and future risks, including contingency and business continuity planning, to ensure continued and effective operations.

1.2 The flowchart detailed at the end of this document sets out the contingency and business continuity process and required action in the case of a trigger event and emergency response activation. This should be considered in conjunction with this policy and will help determine action to be taken in the event of an incident.

1.3 This policy should be read in conjunction with the following for each of the academies and central team within the EMAT:

- Emergency Plan (see EMAT Schools Emergency Plan Template)
- Academy Business Continuity Plan
- Cyber Response Plan
- Fire Evacuation Plans
- Fire risk assessment
- Snow Procedure
- Emergency Contact Information

An emergency information pack is kept securely at the main/reception office at each academy site within the EMAT and includes:

- Copies of this document
- All associated documents (listed above)
- Class Lists (including emergency contact telephone numbers)
- Site Plans

Access to staff and student data with home phone numbers can be accessed on-line by the Headteacher or School Business Manager.

1.4 The Trust will ensure that business continuity management is embedded within its culture and that all those connected with the delivery of services, including partners and key suppliers are fully aware of their roles and responsibilities in ensuring business continuity.

1.5 Whilst no amount of planning can totally prevent accidents and problems occurring, it is recognised that some can be prevented and the effects of others minimised by taking sensible precautionary measures. The Trust expects that all staff will be familiar with the routines and procedures for dealing with emergencies. It is not

possible, or desirable, to write a plan for every possible disruption. No matter what the cause of the incident, the effect can generally be summarised as:

- An inability to carry out daily and/or critical activities
- Loss of life or serious injury to Trust staff and students/pupils or members of the public
- Loss of buildings, or part of or access to them
- Loss or failure of ICT systems and essential data
- Loss/shortage of staff
- Loss of critical suppliers or partners
- Severe financial loss
- Adverse publicity and/or reputational impact

1.6 In the event of a critical incident the priorities of those in charge of the academy or trip will be to:

- Preserve life
- Minimise personal injury
- Safeguard the interests of all pupils and staff
- Minimise any loss to property and to return to normal working as quickly as possible
- Minimise the impact of loss of, or inability to access, essential / confidential data

2. Planning for and Managing Emergencies or Critical Incidents

2.1 Each academy and central team will maintain their own Emergency Plan and the central MAT will maintain the EMAT Contingency and Business Continuity Policy to address and respond to the key risks identified.

2.2 These plans will be activated in the event of a critical incident or an emergency i.e. when an incident occurs that impacts on the delivery of our critical activities or the safety and well-being of our pupils, staff and other stakeholders; and when normal responses, procedures and coping strategies are deemed insufficient to deal with the circumstances.

2.3 Planning should be based on the principle that in the first instance and where possible other staff, sites and premises within the Trust should be utilised to support immediate responses and the return to normal operations.

2.4 Academies should use / follow the Esteem MAT Schools Emergency Plan and Business Continuity Plan templates. As a minimum all plans will include:

- Stakeholder information and key contact details
- Emergency and security plan management team membership and their responsibilities
- Communications plan
- Emergency evacuation, invacuation and lock down procedures
- Contingency plans and strategies for possible risk scenarios such as closure or loss of site or loss of staff – including remote learning / working planning
- Alternative premises plans if access to the school site is prevented, focused on both the short and medium term
- Incident management plan for off-site incident
- Any documents that will assist in dealing with the situation, such as media advice, IT recovery and security plans, site plans and location of emergency shut-off valves, potential hazards etc.
- Record-keeping logs to record all decisions and actions (to protect against litigation post-incident).
- Details on training and testing of plans and procedures

2.5 A paper copy of the respective plans for each academy should be maintained by the Headteacher and School Business Manager to allow access out of normal working hours. The latest version of each plan should be forwarded to the Dep CE at the Central MAT team who will ensure the secure storage and maintenance of a central record of all plans.

3. Cyber Response Plan (previously ICT Disaster Recovery Plan)

3.1 Each Headteacher (or designated lead as determined by the Headteacher) in each academy, and the Dep CE for the central team, supported by the Trust ICT Manager, will be responsible for establishing a Cyber Response Plan. A template cyber response plan will be provided for all academies to follow.

3.2 This will identify measures to take to mitigate the risk of an ICT related critical event and also identify actions to take in the event of loss of ICT hardware, software, infrastructure or connectivity; the loss of key ICT related staff; loss of critical data; and/or the impact of cyber-attacks.

Trust Level Roles and Responsibilities

Role	Responsibility
CEO	The implementation and co-ordination of the CBCP, including: • Contacting the police / other emergency services if the disaster relates to the built environment or the ICT infrastructure, to establish if the building can be re-occupied and/or service delivery reinstated. • Co-ordination of crisis status reports/communication for the benefit of all audiences (including staff, pupils, parents, LA, Academies Team at DFE, press). • If academy building is inaccessible the CEO will determine which of the other academies could provide temporary accommodation • Setting up and notifying members of the IMT immediately following decision to implement • Notifying the EMAT Chair of Trust Board of the implementation of the CBCP and nature of incident. • Maintaining communications with the EMAT Chair of Trust Board until incident has been de-escalated or normal conditions have been restored. • Maintaining communications with the EMAT Trust Board (via the Chair of Trust Board) • Trust level risk management and reporting • When applicable, providing direction on required system of controls and quality assurance • When applicable, ensuring provision of single point of contact for media enquiries • When applicable contacting the DfE, ESFA, RSC, LA and other trusts or schools local to the incident • Maintaining the CBCP in an up-to-date format
Incident Management Team (IMT) – may include: Dep CE Finance Director CEdO Headteachers Head of HR Estates Manager ICT Manager Governance Manager Head of Safeguarding and FASST	• Restoration of normal conditions as soon as possible (IMT) • Implementation and monitoring of agreed system of controls (Key leads) • Ongoing monitoring and assessment of risks (Dep CE) • Provision of timely and approved communications to all those affected by the incident i.e. staff, pupils, parents/carers, stakeholders and service providers, LA, governing boards (Dep CE, Head of HR, Governance Manager) • Implementation of Cyber recovery plan and off-site data/systems management (ICT Manager) • Statutory safeguarding requirements, and support to families of those pupils who are vulnerable (Head of Safeguarding and FASST) • GDPR and data protection advice and reporting (Governance Manager)

4. Testing and Review

4.1 It is the responsibility of each academy's Headteacher, and the Dep CE for central team, to ensure that plans are reviewed on a regular basis and always reviewed and appraised upon the conclusion of an incident. As a minimum all plans must be subject to some form of testing at least once in every 12-month period.

Contingency & Business Continuity