
VISION
MULTI ACADEMY TRUST

# Business Continuity Policy & Procedure

## November 2025

**Date of Review:** November 2025

**Approved by:** Trust Board

**Next Review Date:** November 2026

**1. Introduction**

1.1 This strategy sets out the Trust's policy for 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 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.

1.3 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
- Loss/shortage of staff
- Loss of critical suppliers or partners
- Adverse publicity and/or reputational impact

1.4 In the event of a critical incident the priorities of those in charge of the school 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.

1.5 The Trust will prioritise safeguarding and mental health considerations, ensuring that all emergency responses are trauma-informed and sensitive to the emotional needs of pupils and staff.

1.6 This policy complements other key Trust policies, including the Safeguarding Policy, Health and Safety Policy, and Data Protection Policy, ensuring an integrated approach to risk management and continuity planning.

1.7 This policy aligns with DfE guidance on emergency planning and response for education settings (2023) and incorporates safeguarding principles from 'Keeping Children Safe in Education'. All emergency responses will prioritise pupil welfare, staff wellbeing, and continuity of education.

**2. Planning for and Managing Emergencies or Critical Incidents**

2.1 Each school and the Central MAT team will carry out an "Assessment of Critical Activities" to identify key risks to its operations and the safety of its pupils, staff and stakeholders. This

assessment will be led by the respective Head Teacher (and CEO) and will inform the business continuity planning process.

2.2 Each school and the Central MAT team will maintain its own Crisis Management Plan to address and respond to the key risks identified.

2.3 This plan 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.

2.4 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.

2.5 As a minimum the plan will include:

- Stakeholder information and key contact details
- Business continuity response team membership and their responsibilities.
- Business impact analysis on essential services and the impact of disruption.
- Communications plan (Where an incident involves the closure of an school then the Chair of the Trust's Board should be informed as part of this response)
- Contingency plans and strategies for possible risk scenarios such as a loss of site or loss of staff.
- Alternative premises plans if access to the school site is prevented focused on both the short and medium term
- Any documents that will assist in dealing with the situation, such as media advice, IT recovery plans, location of emergency shut-off valves etc.
- Somewhere to record all decisions and actions (to protect against litigation post-incident).
- Plans must include safeguarding protocols, ensuring the Designated Safeguarding Lead (DSL) is involved in all critical incident responses. Communication strategies should cover multi-channel alerts (SMS, email, website, social media) and include templates for notifying parents, staff, and local authorities.

2.6 A copy of the respective plan for each school and the Central MAT team should be maintained by the Head Teacher (and CEO) on an encrypted USB storage device to allow access out of normal working hours. The latest version of each plan should be forwarded to the Central MAT team who will maintain a central record of all plans.

2.7 Each school will establish clear protocols for liaising with external agencies, including local authorities, emergency services, and public health bodies, to ensure coordinated responses during critical incidents.

2.8 Risk assessments will account for emerging th

2.9 reats, including cybersecurity risks and climate-related emergencies (e.g., flooding, extreme weather), with contingency measures tailored to these scenarios.

2.10 Climate-related emergencies (e.g., flooding, extreme heat) must be included in risk assessments, with mitigation measures such as alternative learning spaces and ventilation strategies.

**3. ICT Disaster Recovery**

3.1 Each Office Manager in each school and the COO for the Central MAT team will be responsible for establishing an ICT Disaster Recovery Procedure in line with the school's "Assessment of Critical Activities" for inclusion in each respective plan.

3.2 This plan will identify actions to take in the event of loss of ICT hardware, software, infrastructure or connectivity; or the loss of key ICT related staff.

3.3 Plans must comply with DfE digital and technology standards, including annual testing of backup and recovery processes, encryption of sensitive data, and cyber resilience measures such as penetration testing and staff training.

3.4 ICT Disaster Recovery plans will incorporate measures for preventing and responding to cybersecurity breaches, including data encryption, access control, and regular penetration testing.

3.5 Plans will include provisions for remote learning to ensure educational continuity for pupils in the event of prolonged site inaccessibility or staff shortages.

3.6 Remote learning protocols must ensure safeguarding compliance, including secure platforms and monitoring arrangements for pupil engagement.

**4. Testing and Review**

4.1 It is the responsibility of each school's Head Teacher and the COO for the Central MAT team to ensure that plans are reviewed on a regular basis and always reviewed and appraised upon the conclusion of an incident. Testing should include scenario-based exercises (e.g., lockdown, evacuation, cyber-attack) and involve external partners where appropriate. Post-incident reviews must capture lessons learned and update safeguarding and mental health provisions. As a minimum all plans must be subject to some form of testing at least once in every 12 month period.

4.2 Following an incident, a formal review will be conducted to document lessons learned, with updates to plans communicated to all staff and stakeholders to improve future resilience.

**5. Risk Management**

5.1 The approach to business continuity planning recognises the links with the Trust's Risk Management Strategy and the risks arising from critical incidents will be included when

developing and monitoring both the Strategic Risk Register and individual operational risk registers.

5.2 Risk registers must explicitly include safeguarding risks, ICT vulnerabilities, and climate adaptation measures, in line with DfE sustainability and climate change strategy (2025).

5.3 The Trust will integrate business continuity risks into its broader Risk Management Framework, ensuring alignment with financial planning, safeguarding considerations, and operational priorities.

5.4 This policy will be monitored in line with the Academies Financial Handbook requirements, ensuring all identified risks are adequately mitigated and appropriately funded.

6. Post-Incident Welfare

- Following any critical incident, the Trust will provide trauma-informed support for pupils and staff, including access to counselling services and wellbeing resources. This aligns with DfE guidance on supporting mental health during emergencies.