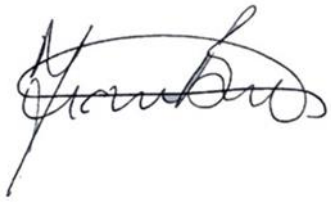
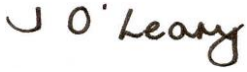
SHINE Multi Academy Trust
Business Continuity Policy

Management log

Document	Business continuity
Author	Chief Finance Officer (CFO)
Person responsible for the document	CEO
Date approved	20 June 2024
Date issued	21 June 2024
Review period	Biennially
Next review	Autumn 2026
Reviewer	Finance and business committee on behalf of the Board
Signed	**Signed**
	
Chair of the Board	**CEO**

Document history

Version	Date authored	Author	Date approved	Date issued	Comments
V1	August 2017	Helena Brooks / Sarah Brown	22 September 2017	22 September 2017	To secure SHINE business continuity plan
V2	October 2020	Helena Brooks / Sarah Brown	5 November 2020	20 November 2020	Annual review
V3	June 2024	Sarah Brown			Review

Please note that the version of this document contained at https://www.shine-mat.com/policies/ is the only version that is maintained.

Any printed copies should therefore be viewed as 'uncontrolled' and as such, may not necessarily contain the latest updates and amendments.

Contents

1. Introduction

1.1 This strategy sets out the SHINE Multi Academy (SHINE) Board of Trustees (Board) 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 Academy Trust 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 Board 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 Board 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 staff and pupils or members of the public
- loss of buildings, or part of access to them

- loss or failure of ICT systems including phone communication
- 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 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.

2. Planning for and managing emergencies or critical incidents

2.1 Each academy within SHINE 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 headteacher and will raise any concerns with the Board.

2.2 Each academy will maintain its own crisis management plan/emergency 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 will impact 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 SHINE 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 academy then the CEO and chair of the 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 academy 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)

2.6 A copy of the respective plan for each academy should be maintained by the headteacher on an encrypted USB storage device, or other secure method, to allow access out of normal working hours. The latest version of each plan must be provided to the SHINE team who will maintain a central record of all plans.

3. ICT disaster recovery

3.1 Each academy business manager in each academy with the chief finance officer will be responsible for establishing an ICT disaster recovery procedure in line with the academy'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.

4. Testing and review

4.1 It is the responsibility of each academy's headteacher and the SHINE 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.

5. Risk management

5.1 The approach to business continuity planning recognises the links with the board'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.