

Business Continuity Policy

Status: Statutory

Date Approved: September 2026

Review Date: September 2027

Team Responsible: DSL Team/ SLT

Policies are approved and ratified by the Senior Leadership Team and the approval of policies are recorded within the minutes of the meetings.

Contents

No	Section	Page
1	Aim and scope of the Business Continuity Policy	1
2	Objectives of the Plan and those responsible	2
3	Critical Function Checklist	4
4	Critical Function Analysis and Recovery Process	5
5	Emergency Response Checklist	8
6	Contact Lists	9
7	Local Emergency Services	9
7	Insurance and Finance Companies	9
8	Emergency Pack Contents	10
9	Actions and Expenses Log	11

1. Aim and scope of the plan

This risk assessment has been designed to prepare *Be My Tutor* to cope with the effects of an emergency. It is intended that this document will provide the basis for a relatively quick and painless return to “business as usual” regardless of the cause. This policy sets out the framework for preventing, preparing for, responding to, and recovering from incidents that could impact service continuity.

This policy applies to all staff, tutors, mentors, contractors, systems, and services involved in the delivery of:

- Online 1:1 or small group tutoring
- Online mentoring sessions
- Associated administrative, safeguarding, and support functions

It covers disruptions including (but not limited to):

- Technology failures

- Loss of key personnel
- Cybersecurity incidents
- Safeguarding incidents
- Data breaches
- Widespread illness or unavailability of staff
- Internet outages
- Natural disasters or other emergencies

2. Objectives of the plan and those responsible for it

To provide a flexible response so that *Be My Tutor* can:

- Respond to a disruptive incident (incident management)
- Maintain delivery of critical activities/services during an incident (business continuity)
- Return to 'business as usual' (resumption and recovery)

Director: Overall responsibility for implementing and reviewing the policy, approving recovery plans, and communicating with commissioners.

Designated Safeguarding Lead (DSL): Ensure safeguarding remains active and effective during incidents.

Operations Manager: Coordinate the continuity response, reallocate resources, and arrange cover staff where necessary.

IT Lead and Head of Admin: Manage system recovery, cyber incident response, and technical continuity solutions.

All Staff: Follow incident reporting and response procedures

3. Be My Tutor Business Priorities: Risks and Critical Function Checklist

Key risks identified include:

- **IT & Platform Failure:** Disruption to online learning platforms (e.g., Zoom, Teams, bespoke LMS).
- **Cybersecurity Breach:** Data loss or unauthorised access to pupil/staff information.
- **Staff Unavailability:** Illness, unexpected leave, or resignation of key tutors/mentors.
- **Infrastructure Issues:** Localised power or internet failure impacting tutors or pupils.
- **Safeguarding Risks:** Increased vulnerability during service disruptions

Priority	Critical function	Timeframe	Page
1	<i>Provision of Tutors- tutor takes absence with short notice due to unforeseen circumstances</i>	<i>Restore with supply cover from teacher team (always leave teachers free).</i>	4
2	Delivery of Online platforms- internet goes down/ not available. Loss of learning management and delivery system	Restore internet connection within 4-5 hours	5
3	LessonSpace Lessons links fail for all students	Teachers to contact students via contact list on tutorcruncher and use other secure means of delivering lessons- Google Meet/ Teams/ Pencil Spaces	
4	Tutorcruncher goes down	Keep a secure list of contacts.	

4. Prevention and Critical Function Analysis and Recovery Process

Prevention & Preparedness

Technical Resilience:

Use of secure, cloud-based platforms with data backup.

Multiple platform readiness (e.g., Zoom, Microsoft Teams, Google Meet) to switch if one fails.

Staff Resilience:

Maintain a pool of approved relief tutors/mentors.

Cross-training in administrative and operational processes.

Safeguarding Continuity:

Ensure DSL and Deputy DSL are always contactable.

Data Security:

Regular backups, multi-factor authentication, and encrypted storage.

Incident Training:

Annual training for staff on emergency procedures and safeguarding in disruption scenarios.

In the event of a disruption Be MY Tutor will:

1. **Assess the situation** – identify the type, scale, and expected duration of disruption.
2. **Activate the Business Continuity Plan** – led by the Managing Director or delegate.
3. **Communicate promptly** – inform staff, pupils, parents/carers, and commissioners of the issue and alternative arrangements.
4. **Implement alternative delivery:**
 - Switch to backup platform.
 - Reschedule or reassign tutors.
 - Provide asynchronous learning resources if live delivery is not possible.

5. **Maintain safeguarding oversight** – ensure all sessions (live or asynchronous) follow safeguarding protocols.

6. **Document all actions** taken during the incident.

4.3 Safeguarding and Wellbeing Continuity

1. **Session Abandonment Protocol:** In the event of a platform failure that disrupts a live session, the tutor must immediately notify the parent/carer and the school contact to ensure the student is safe and to communicate the interruption.
2. **Wellbeing Check-in:** If a session is cancelled or significantly delayed due to technical issues, a designated staff member must send a pre-approved wellbeing check-in message to the student/carer to maintain engagement and support.
3. **Real-time Session Log:** In compliance with service specifications, the Operations team must maintain a 'Real-time Session Log' (via Tutor Cruncher or similar) identifying all staff and learners currently in active sessions to ensure accurate reporting during an emergency.

Recovery and communication

- Restore normal operations as soon as feasible.
- Review and address any safeguarding concerns arising during disruption.
- Conduct a **post-incident review** to identify improvements.
- Report to commissioners and regulatory bodies if required (e.g., serious safeguarding breaches, data breaches to ICO within 72 hours).
- Maintain up-to-date contact lists for staff, pupils, parents/carers, and commissioners.
- Use email, phone, and text alerts to communicate urgent updates.
- All official updates must be approved by the Director

Priority:	1	Critical function:	Tutor not able to attend lessons
Responsibility: (role responsible for leading on this activity, plus deputies)			Adam Haffner Director
Potential impact on organisation if interrupted:			Online lessons missed by students critical to their education
Likelihood of interruption to			Medium

organisation:	
Recovery timeframe: <i>(how quickly must this function be recovered to avoid lasting damage)</i>	12-24 hours
Resources required for recovery:	
Staff <i>(numbers, skills, knowledge, alternative sources)</i>	Adam Haffner- Director and DSL Leena Cark- Head of Operations Carol Cato- Head of Groups
Data / systems <i>(backup and recovery processes, staff and equipment required)</i>	Tutor Cruncher secure learning management software- used to store secure bank of lesson times and teachers available (use timetabling function) Teachers follow code of conduct to ensure 48 hours notification of any absences (see code of conduct). All teachers are also made aware of this on contracts. Notify office if absent- senior leadership team arrange supply teacher.
Premises <i>(potential relocation or work-from-home options)</i>	Online
Communications <i>(methods of contacting staff, suppliers, customers, etc)</i>	Via Be My Tutor secure email; in the event of email failure, use pre-agreed encrypted messaging channels (e.g., WhatsApp or Signal) for urgent staff communication. Also see Section 6 Contact Lists.
Equipment <i>(key equipment recovery or replacement processes; alternative sources; mutual aid)</i>	N/A
Supplies <i>(processes to replace stock and key supplies required; provision in emergency pack)</i>	N/A

4. Critical Function Analysis and Recovery Process (continued)

Priority:	2	Critical function:	Loss of internet
Responsibility: <i>(role responsible for leading on this activity, plus deputies)</i>			Adam Haffner- Director
Potential impact on organisation if interrupted:			All learning management systems and lesson delivery systems go

	down
Likelihood of interruption to organisation:	small
Recovery timeframe: <i>(how quickly must this function be recovered to avoid lasting damage)</i>	4-6 hours
Resources required for recovery:	
Staff <i>(numbers, skills, knowledge, alternative sources)</i>	Adam Haffner- Director Nish Thenuwara at Fotowork-consultant on technology for Be My Tutor
Data / systems <i>(backup and recovery processes, staff and equipment required)</i>	All systems securely backed up daily on cloud
Premises <i>(potential relocation or work-from-home options)</i>	online
Communications <i>(methods of contacting staff, suppliers, customers, etc)</i>	Also see Section 6 Contact Lists.
Equipment <i>(key equipment recovery or replacement processes; alternative sources; mutual aid)</i>	Use of new computers
Supplies <i>(processes to replace stock and key supplies required; provision in emergency pack)</i>	computers

5. Emergency Response Checklist

This page should be used as a checklist during the emergency.

Task	Completed (date, time, by)
Actions within 24 hours:	
Start of log of actions and expenses undertaken (see section 9 Action and Expenses Log)	

Liaise with emergency services (see section 6E Contact List – Emergency Services)	
Identify and quantify any damage to the organisation, including staff, premises, equipment, data, records, etc	
Assess the key priorities for the remainder of the working day and take relevant action. Consider sending staff home, to recovery site etc	
Inform staff what is required of them.	
Identify which critical functions have been disrupted (use section 3 Critical Function Checklist)	
Convene those responsible for recovering identified critical functions, and decide upon the actions to be taken, and in what time-frames (use section 4 Critical Function Analysis and Recovery Process)	
Provide information to: ● Staff ● Suppliers and customers ● Insurance company	
Publicise the interim arrangements for delivery of critical activities. Ensure all stakeholders are kept informed of contingency arrangements as appropriate	
Recover vital assets/equipment to enable delivery of critical activities. The essential equipment/resources/information that need to be recovered where possible are:	
Daily actions during the recovery process:	
Convene those responsible for recovery to understand progress made, obstacles encountered, and decide continuing recovery process	
Provide information to: ● Staff ● Suppliers and customers ● Insurance company	
Provide public information to maintain the reputation of the organisation and keep relevant authorities informed	
Following the recovery process:	
Arrange a debrief of all staff and identify any additional staff welfare needs (e.g. counselling) or rewards	
Use information gained from the debrief to review and update this business continuity management plan	

6. Contact List

Staff

This section contains the contact details that are essential for continuing the operation of the organisation.

Name	Job Title	Office Contact	Mobile Contact	Home Contact
Adam Haffner	Manager	07901916286	07901916286	07901916286

7 Local Emergency Services

Service	Location	Telephone
Ambulance	Emergencies	999
Fire Service	Emergencies	999
Floodline	Information service	0845 988 1188
NHS Direct		0845 46 47
Police	Emergencies	999
	Non-emergency matters	101

Insurance and Finance Companies

Service	Company	Telephone	E-mail
Banking	Starling	02079304450	help@starlingbank.com
Insurance	Policy Bee	03455610320	contactus@policybee.co.uk

8. Emergency Pack Contents

As part of the recovery plan for the organisation, key documents, records and equipment are held off-site at *Rickmansworth Office* in an emergency pack. This pack may be retrieved in an emergency to aid in the recovery process.

The contents of the emergency pack comprise the following:

Documents:

- A copy of this plan, including key contact details
- Insurance policy

Records:

- Computer backup tapes and / or disks
- Financial records

Equipment:

- Spare keys
- Torch and batteries

9. Actions and Expenses Log

This form should be used to record decisions, actions and expenses incurred in the recovery process. This will provide information for the post-recovery debriefing, and help to provide evidence of costs incurred for any claim under an insurance policy.

Date/time	Decision / action taken	By whom	Costs incurred

[illegible]