



# Business Continuity Plan (BCP)

Organisation: Autism Mentors

Date: 5/9/25

Review Date: September 2026

Approved by: Directors of Autism Mentors

## 1. Purpose

The purpose of this Business Continuity Plan is to ensure Autism Mentors can continue to provide essential educational and care services to children and young people with neurodiverse needs in the event of an emergency, disruption, or crisis.

## 2. Objectives

- Safeguard children, young people, and staff.
- Minimise disruption to service delivery.
- Maintain compliance with safeguarding, contractual, and data protection obligations.
- Establish a framework for rapid response, recovery, and communication.

## 3. Scope

### **This plan applies to:**

- All Autism Mentors staff, consultants, and contractors.
- All services delivered in schools, homes, and community settings.
- All business operations, including administrative, IT, and communication systems.

## 4. Risk Assessment

### **Key Risks Identified:**

1. Staff Shortages – due to illness, resignation, industrial action, or safeguarding suspension.
2. IT/Systems Failure – loss of access to client data, communication systems, or scheduling platforms.
3. Safeguarding Incident – requiring immediate investigation or suspension of service delivery.
4. Venue/Location Unavailability – schools or community settings closed due to emergencies.
5. Transport Disruption – inability to travel to sessions due to extreme weather, accidents, or fuel shortages.
6. Health Emergency/Pandemic – outbreaks of contagious diseases limiting face-to-face work.
7. Reputational or Legal Crisis – adverse publicity, regulatory investigation, or litigation.

## 5. Roles and Responsibilities

- Directors – Overall responsibility for BCP activation, decision-making, and external communication.
  - Michelle Wray
  - Elizabeth Carter
  - Tracy Hinton
- Consultants/Mentors – Responsible for safeguarding continuity of care, following emergency protocols, and reporting incidents.
- Admin Team; Michelle Wray, Elizabeth Carter and Tracy Hinton – Ensure client communication, rescheduling, payroll, and documentation are maintained.
- Safeguarding Leads – Coordinates safeguarding response, liaises with local authorities, and ensures compliance.
  - Michelle Wray
  - Elizabeth Carter

## 6. Continuity Strategies

### 6.1 Staff Shortages

- Maintain a list of vetted reserve consultants.
- Introduce two mentors during initial visits where possible.
- Cross-train staff to provide cover in essential areas.
- Prioritise high-need clients where full coverage is not possible.

### 6.2 IT/Systems Failure

- Daily backups of client and business data.
- Secure cloud-based system for storing sensitive information.
- Emergency contact tree stored offline.

### 6.3 Data Recovery Plan

In the event of a data breach, loss, or system failure, Autism Mentors will take immediate action to recover and protect critical information.

#### Objectives:

- Restore access to essential client and business data within 24–48 hours.
- Ensure data integrity, confidentiality, and compliance with UK GDPR.
- Minimise operational downtime and disruption to client services.

#### Key Procedures:

##### 1. Incident Identification

- Report all suspected data loss or breach incidents immediately to the Directors and Data Protection Lead.
- Identify the nature and scope of the loss (accidental deletion, cyberattack, system crash, etc.).

## 2. Containment & Isolation

- Disconnect affected systems or devices from the network to prevent further loss or corruption.
- Preserve unaffected backups and systems.

## 3. Data Restoration

- Retrieve the most recent secure backup from encrypted cloud storage (Google Workspace/SharePoint/Dropbox Business – depending on service).
- Restore critical files in priority order:
  1. Safeguarding and client records
  2. Staff and HR documentation
  3. Scheduling and financial systems

## 4. Verification

- Confirm restored data is complete and accurate.
- Log all actions and changes for audit and accountability.

## 5. Reporting & Compliance

- Notify the Information Commissioner's Office (ICO) within 72 hours if data loss meets the GDPR reporting threshold.
- Inform affected individuals where there is a potential risk to privacy or safety.

## 6. Post-Incident Review

- Review causes and prevention measures.
- Update IT and data policies, security software, and staff training.
- Record incident in the Data Breach Log.

### **Data Recovery Contacts:**

- Data Protection Lead:

- Michelle Wray
-  [dsl@autismmentors.co.uk](mailto:dsl@autismmentors.co.uk)
-  07707 764876
- Deputy Lead:
  - Elizabeth Carter
  -  [beth@autismmentors.co.uk](mailto:beth@autismmentors.co.uk)
  -  07979 692297

#### **6.4 Safeguarding Incident**

- Immediate referral to Safeguarding Lead.
  - Michelle Wray
  - Tel: 07707 764876
  - Email: [dsl@autismmentors.co.uk](mailto:dsl@autismmentors.co.uk)
- Temporary suspension of staff if required.
- Maintain continuity of service with alternative staff.
- Full documentation and reporting in line with safeguarding policy.

#### **6.5 Venue/Location Unavailability**

- Switch sessions to online delivery (where suitable).
- Relocate to alternative agreed venues.
- Communicate promptly with clients and families.

#### **6.6 Transport Disruption**

- Prioritise local staff for local cases.
- Use remote/online sessions where appropriate.
- Agree contingency travel arrangements in advance.

#### **6.7 Health Emergency/Pandemic**

- Follow Public Health England guidance.
- Switch to online/remote support where appropriate.
- Provide PPE and hygiene training to staff.

## **6.8 Reputational/Legal Crisis**

- Appoint a spokesperson (Director).
  - Elizabeth Carter
  - Tel: 07979 692297
  - Email: beth@autismmentors.co.uk
- Prepare holding statements for press or stakeholders.
- Seek immediate legal advice.

## **7. Communication Plan**

- Internal: WhatsApp groups, email, emergency phone tree.
- External: Parents/carers notified via phone/email, schools via official contact channels.
- Regulatory bodies: Local authority and safeguarding boards notified where required.
- IT downtime: Backup communication plan (personal mobiles, offline emergency contact list).

## **8. Recovery Plan**

- Assess situation and implement continuity measures.
- Restore services to normal operation as soon as possible.
- Conduct post-incident review to identify lessons learned.
- Update BCP accordingly.

## **9. Testing and Review**

- BCP to be reviewed annually by Directors.
  - Michelle Wray

- Elizabeth Carter
- Tracy Hinton
- Tabletop exercises conducted twice per year.
- Updates made following any major incident or organisational change.

## 10. Approval and Sign-off

Signed:



Director: Michelle Wray



Director: Elizabeth Carter

Date: 05/09/25