BUSINESS CONTINUITY AND EMERGENCY PLANNING POLICY

Policy Title: PRN-010: Business Continuity and Emergency Planning Policy
Company Name: AI Auto-Tech Ltd
Trading/Business Name: CAREHOPES
Company Registration Number: 15556946
SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled
Email: admin@carehopes.com
Version Number: V01 20260815
Date of Review: (August 2026)

---

1. Purpose

The purpose of this policy is to ensure that the organisation can continue to provide essential services during and after a disruption, emergency, or critical incident.

As a Non-Accommodation Companionship and Wellbeing Support Service supporting older people and adults with disabilities, the organisation recognises that emergencies can impact service users, employees, volunteers, partners, and the wider community.

This policy establishes arrangements to:

- Protect people from harm.
- Minimise service disruption.
- Maintain critical functions.
- Ensure effective communication.
- Support recovery following an incident.
- Promote organisational resilience.

---

2. Scope

This policy applies to:

- Employees
- Volunteers
- Managers
- Directors
- Trustees
- Contractors

The policy applies to all organisational activities including:

- Companionship services
- Wellbeing support
- Home visits
- Community-based activities
- Volunteer programmes
- Administrative functions
- Remote working arrangements

---

3. Policy Statement

The organisation is committed to maintaining continuity of service wherever possible during emergencies or disruptive events.

We will:

- Plan for foreseeable risks.
- Minimise disruption to service users.
- Protect staff and volunteers.
- Maintain communication arrangements.
- Restore normal operations as efficiently as possible.
- Learn from incidents and exercises.

Business continuity planning is an important part of good governance and risk management.

---

4. Objectives

The objectives of this policy are to:

- Ensure the safety and wellbeing of service users, employees, and volunteers.
- Maintain essential services.
- Protect organisational resources.
- Ensure clear lines of responsibility.
- Facilitate effective emergency response.

- Support rapid recovery.
- Promote organisational resilience.

---

5. Definition of Business Continuity

Business continuity refers to the processes and procedures that enable the organisation to continue operating during and after a disruption.

The aim is to ensure critical activities can continue or be restored within an acceptable timeframe.

---

6. Definition of an Emergency

An emergency is any event that disrupts normal operations and may threaten:

- Health and safety
- Service delivery
- Information security
- Facilities
- Organisational reputation
- Financial stability

Examples include:

- Severe weather
- Flooding
- Fire
- Pandemic illness
- IT failure
- Power outage
- Cyber incident
- Transport disruption
- Serious safeguarding incidents
- Loss of key personnel

---

7. Principles of Business Continuity

The organisation will:

Prioritise Safety

The safety of people will always take priority.

Maintain Essential Services

Critical activities will be prioritised.

Communicate Effectively

Clear communication arrangements will be maintained.

Promote Flexibility

Alternative arrangements may be used where necessary.

Learn and Improve

Incidents will be reviewed to strengthen future resilience.

---

8. Roles and Responsibilities

Directors

Responsible for:

- Strategic oversight.
- Approval of continuity arrangements.
- Supporting recovery efforts.
- Reviewing significant incidents.

Managers

Responsible for:

- Implementing continuity plans.
- Coordinating emergency responses.
- Communicating with staff and volunteers.
- Assessing risks and recovery priorities.

Employees and Volunteers

Responsible for:

- Following emergency procedures.
- Reporting incidents promptly.
- Maintaining up-to-date contact information.
- Cooperating with continuity arrangements.

---

9. Critical Services

The organisation will identify and prioritise critical functions.

Examples may include:

- Welfare and wellbeing checks.
- Support for vulnerable service users.
- Safeguarding responses.
- Communication with service users and families.
- Volunteer coordination.
- Incident management.

Critical functions should receive priority during disruption.

---

10. Business Impact Assessment

The organisation will periodically assess:

- Critical activities.
- Potential risks.
- Impact of service disruption.
- Recovery priorities.
- Resource requirements.

Assessments will support continuity planning and emergency preparedness.

---

11. Risk Assessment

Business continuity planning should be informed by risk assessments.

Potential risks may include:

- Loss of premises.
- IT system failure.
- Staff shortages.
- Volunteer shortages.
- Severe weather conditions.
- Supply chain disruption.
- Utility failures.
- Public health emergencies.

Appropriate mitigation measures should be identified wherever possible.

---

12. Emergency Communication

Effective communication is essential during emergencies.

Communication arrangements may include:

- Telephone calls.
- Mobile communications.
- Email.
- Virtual meetings.
- Emergency contact lists.

Communication may be required with:

- Employees.
- Volunteers.
- Service users.
- Families.
- Partner agencies.
- Emergency services.

Contact information should be reviewed regularly.

---

13. Staff and Volunteer Contact Information

The organisation will maintain up-to-date emergency contact information for:

- Employees.
- Volunteers.
- Key organisational contacts.

Individuals are responsible for notifying the organisation of changes to their contact details.

---

14. Service User Communication

Where disruption affects service delivery, reasonable efforts will be made to:

- Inform service users promptly.
- Explain alternative arrangements.
- Identify urgent support needs.
- Prioritise vulnerable individuals.

Clear and compassionate communication should be maintained throughout any disruption.

---

15. Remote Working Arrangements

Where appropriate, remote working may be used to support business continuity.

This may include:

- Home working.
- Virtual meetings.
- Telephone support services.
- Online communication systems.

Remote working arrangements must comply with:

- Data protection requirements.
- Confidentiality requirements.
- Health and safety responsibilities.

---

16. Loss of Premises

If organisational premises become unavailable due to fire, flooding, damage, or other disruption, alternative arrangements may include:

- Remote working.
- Temporary facilities.
- Community venues.
- Shared office arrangements.

Critical services should continue wherever reasonably practicable.

---

17. Information Technology and Cyber Incidents

Disruptions involving technology may include:

- System failures.
- Internet outages.
- Cyber attacks.
- Equipment failures.
- Loss of electronic records.

The organisation will seek to:

- Maintain secure backups.
- Protect information.
- Restore systems promptly.
- Report incidents appropriately.

Any data breaches must be managed in accordance with the Data Protection and GDPR Policy.

---

18. Severe Weather and Environmental Emergencies

The organisation will monitor risks associated with:

- Snow and ice.
- Flooding.

- Heatwaves.
- Storms.
- Travel disruption.

Managers may:

- Reschedule activities.
- Introduce alternative arrangements.
- Restrict travel where risks are unacceptable.
- Prioritise vulnerable service users.

Safety considerations will always take priority.

---

19. Public Health Emergencies

Public health emergencies may include:

- Pandemic illness.
- Infectious disease outbreaks.
- Public health restrictions.

The organisation will follow relevant public health guidance and may implement:

- Remote support arrangements.
- Infection prevention measures.
- Additional risk assessments.
- Temporary service adjustments.

---

20. Loss of Key Personnel

The unexpected absence of key personnel may disrupt service delivery.

To reduce risk, the organisation will:

- Maintain essential records.
- Ensure appropriate delegation arrangements.
- Share key operational knowledge where possible.
- Develop contingency plans.

This helps ensure continuity of leadership and decision-making.

---

21. Emergency Response Procedure

In the event of a significant incident:

Step 1

Ensure immediate safety.

Step 2

Contact emergency services where required.

Step 3

Notify management.

Step 4

Assess the impact.

Step 5

Activate business continuity arrangements.

Step 6

Communicate with relevant stakeholders.

Step 7

Implement recovery actions.

Step 8

Review lessons learned.

---

22. Recovery Planning

Following an emergency, the organisation will:

- Assess operational impact.
- Identify outstanding risks.
- Restore services in priority order.
- Support affected individuals.
- Review effectiveness of the response.

Recovery planning should focus on restoring normal operations safely and efficiently.

---

23. Testing and Exercising

The organisation may periodically test its business continuity arrangements through:

- Tabletop exercises.
- Scenario discussions.
- Emergency drills.
- Policy reviews.

Testing helps identify gaps and opportunities for improvement.

---

24. Learning from Incidents

Following significant incidents or near misses, a review may be undertaken to consider:

- What happened.
- What worked well.
- What could be improved.
- Lessons learned.
- Changes required.

Findings should inform future planning and risk management.

---

25. Case Study

Scenario: Severe Weather Disruption

Heavy snowfall results in unsafe travel conditions across the local area.

Actions Taken

- Community activities are postponed.
- Service users are contacted by telephone.
- Welfare checks are prioritised for vulnerable individuals.
- Volunteers are advised not to travel where conditions are unsafe.
- Managers monitor the situation and communicate updates.

Outcome

Service users remain supported through alternative arrangements and no injuries occur.

Learning Point

Flexible service delivery and effective communication help maintain continuity during emergencies.

---

26. Training and Awareness

Employees and volunteers will receive information appropriate to their roles regarding:

- Emergency procedures.
- Incident reporting.
- Communication arrangements.
- Health and safety responsibilities.
- Business continuity principles.

Training needs will be reviewed regularly.

---

27. Responsibilities Summary

Role	Responsibilities
Directors	Governance, oversight, recovery leadership
Managers	Emergency coordination, communication, continuity planning
Employees	Follow procedures, report concerns, support continuity
Volunteers	Follow guidance, maintain communication, support service continuity

---

28. Monitoring and Quality Assurance

The organisation will monitor:

- Emergency incidents.
- Service disruptions.
- Business continuity exercises.

- Risk assessments.
- Recovery outcomes.
- Staff and volunteer feedback.

Monitoring outcomes will be used to improve preparedness and organisational resilience.

---

29. Review Arrangements

This policy will be reviewed:

- Annually.
- Following significant incidents.
- Following emergency exercises.
- Following major organisational changes.
- Following legislative or regulatory updates.

Related Policies

- Health and Safety Policy
- Risk Assessment Policy
- Incident Reporting Policy
- Lone Working Policy
- Data Protection and GDPR Policy
- Adult Safeguarding Policy
- Employee Wellbeing Policy
- Volunteer Management Policy