Emergency Preparedness, Response, Resilience and Recovery (EPRRR) Policy

PRN-182: Emergency Preparedness, Response, Resilience and Recovery (EPRRR) Policy

CAREHOPES™
A subsidiary of AI Auto Tech Ltd
Company Number: 15556946
Website: www.carehopes.com
Email: admin@carehopes.com

---

1. Policy Statement

CAREHOPES™ is committed to maintaining effective arrangements for Emergency Preparedness, Response, Resilience and Recovery (EPRRR) to protect service users, employees, volunteers, contractors, visitors, third-party providers, and organisational assets.

CAREHOPES™ recognises that emergencies, incidents, disruptions, disasters, cyber incidents, public health emergencies, extreme weather events, infrastructure failures, and major incidents can affect the safety, wellbeing, and continuity of its services.

This policy establishes a structured framework for preparing for, responding to, recovering from, and learning from incidents that may affect the organisation.

---

2. Purpose

The purpose of this policy is to:

- Protect life, safety, and wellbeing.
- Promote business continuity.
- Minimise disruption to services.
- Maintain service user support during emergencies.
- Ensure coordinated incident response.
- Strengthen organisational resilience.
- Support rapid recovery following incidents.

- Meet legal, regulatory, and governance obligations.

---

3. Scope

This policy applies to:

- Employees
- Managers
- Supervisors
- Volunteers
- Contractors
- Third-party providers
- Agency workers
- Students and trainees

It applies across:

- Home-based services
- Community settings
- Travel assignments
- Airport companionship services
- Training environments
- Office locations
- Digital service delivery environments

---

4. Definitions

Emergency

A situation requiring immediate action to protect life, safety, health, service delivery, property, or reputation.

Major Incident

An event that seriously disrupts service delivery and requires coordinated action beyond normal operational arrangements.

Resilience

The ability of CAREHOPES™ to anticipate, withstand, adapt to, and recover from disruption.

Recovery

Activities undertaken to return services to normal operation following an incident.

---

5. EPRRR Framework

CAREHOPES™ adopts the four pillars of:

Emergency Preparedness

Being ready before an incident occurs.

Emergency Response

Managing the immediate effects of an incident.

Resilience

Maintaining critical operations during disruption.

Recovery

Restoring services and learning from incidents.

---

6. Emergency Preparedness

CAREHOPES™ will:

- Conduct risk assessments.
- Develop emergency response plans.
- Maintain business continuity arrangements.
- Ensure critical contact lists remain current.
- Train employees in emergency awareness.
- Conduct emergency exercises where appropriate.
- Maintain suitable communication arrangements.
- Ensure safeguarding arrangements remain operational during emergencies.

Employees must:

- Familiarise themselves with emergency procedures.

- Understand reporting requirements.
- Keep emergency contact information up to date.
- Participate in training when required.

---

7. Emergency Response

During an emergency, employees must:

- Prioritise life and safety.
- Remain calm and professional.
- Follow emergency instructions.
- Contact emergency services where necessary.
- Notify management immediately.
- Document incidents as soon as practicable.
- Follow safeguarding procedures.

Employees must never:

- Place themselves unnecessarily at risk.
- Ignore emergency instructions.
- Provide services beyond their level of competence unless specifically trained and authorised to do so.

---

8. Service User Safety During Emergencies

CAREHOPES™ employees must:

- Consider the immediate safety of service users.
- Follow emergency evacuation instructions where applicable.
- Provide reassurance and emotional support.
- Assist individuals to access emergency services where required.
- Contact designated family members or emergency contacts where appropriate.
- Escalate safeguarding concerns immediately.

Employees must maintain professional boundaries during emergencies.

---

9. Business Continuity and Service Continuation

CAREHOPES™ will seek to maintain critical services during:

- Severe weather
- Flooding
- Fire incidents
- Transport disruption
- Industrial action
- Technology failures
- Cyber incidents
- Utility failures
- Public health emergencies
- National emergencies

Business continuity arrangements may include:

- Alternative staffing arrangements
- Remote working
- Rescheduling services
- Alternative communication methods
- Temporary service prioritisation

---

10. Public Health Emergencies

During public health incidents, employees must:

- Follow public health guidance.
- Follow infection prevention and control measures.
- Use PPE where required.
- Report symptoms of infectious illness.
- Protect themselves and service users.

CAREHOPES™ may temporarily modify operational arrangements to ensure safety.

---

11. Cyber and Information Security Incidents

In the event of a cyber security incident, employees must:

- Report suspected breaches immediately.
- Report phishing attempts.
- Report lost or stolen devices.
- Report unauthorised access concerns.
- Follow cyber incident response procedures.

Employees must never:

- Attempt to investigate cyber incidents independently.
- Conceal suspected breaches.
- Circumvent security controls.

---

12. Safeguarding During Emergencies

Safeguarding responsibilities remain in effect during all emergencies.

Employees must:

- Continue to report safeguarding concerns.
- Escalate urgent risks immediately.
- Maintain accurate records.
- Follow safeguarding procedures.
- Protect vulnerable adults and children.

Emergencies do not remove safeguarding responsibilities.

---

13. Recovery and Restoration

Following an incident, CAREHOPES™ will:

- Assess impact.
- Restore services safely.
- Support affected service users.

- Support affected employees.
- Review safeguarding implications.
- Identify lessons learned.
- Implement improvement actions.

Managers may conduct post-incident reviews to strengthen future preparedness.

---

14. Supervisor Responsibilities

Supervisors must:

- Coordinate emergency communications.
- Support employees during incidents.
- Escalate major incidents.
- Monitor service delivery impact.
- Support recovery efforts.
- Maintain situational awareness.
- Review incident documentation.

---

15. Third-Party Provider Responsibilities

Third-party providers must:

- Comply with emergency procedures.
- Report incidents immediately.
- Cooperate with emergency response arrangements.
- Maintain their own business continuity arrangements where applicable.
- Support safeguarding requirements.

---

16. Training Requirements

Employees may receive training in:

- Emergency awareness
- Fire safety

- First aid
- Business continuity
- Safeguarding during emergencies
- Incident reporting
- Cyber security incident response
- Infection prevention and control

Additional role-specific training may be required where appropriate.

---

17. Monitoring and Compliance

CAREHOPES™ will monitor compliance through:

- Supervision
- Audits
- Incident reviews
- Training records
- Business continuity testing
- Quality assurance activities

---

18. Breach of Policy

Failure to comply with this policy may result in:

- Additional training
- Corrective action plans
- Disciplinary action
- Suspension
- Termination of engagement
- Referral to relevant authorities where appropriate

---

19. Related Policies

- Duty of Care Policy

- Business Continuity Policy
- Health and Safety Policy
- Fire Safety Policy
- First Aid Policy
- Safeguarding Adults Policy
- Safeguarding Children Policy
- Information Governance and Data Security Policy
- Cyber Security and Internet Fraud Awareness Policy
- Incident Reporting Policy
- Risk Assessment Policy

---

20. Policy Review

This policy will be reviewed:

- Annually
- Following major incidents
- Following legislative changes
- Following regulatory changes
- Following organisational restructuring
- Following emergency exercises or testing