



Wealden Volunteering Business Continuity Plan

Approved by the Board: July 2026

Next Review date: July 2028

Chair Signature:

A handwritten signature in blue ink, appearing to read 'Paul P. K.', is written on a yellow rectangular background.

1. Purpose

Wealden Volunteering (WV) recognises that unexpected events may disrupt service delivery.

This plan sets out how we will:

- Respond to incidents or emergencies
- Maintain critical services
- Protect staff, volunteers and beneficiaries
- Restore operations as quickly as possible

2. Scope

This plan applies to:

- All staff, volunteers and trustees
- All services, locations and systems
- All types of disruption (minor to major)

Including:

- Loss of premises
- IT or communications failure
- Staff or volunteer shortages
- Safeguarding or serious incidents
- Public health emergencies

3. Objectives

We aim to:

- Maintain delivery of critical services
- Minimise disruption to communities and partners
- Ensure clear communication during incidents
- Restore normal operations as quickly as possible
- Learn from incidents to improve resilience

4. Governance and Responsibilities

Board of Trustees

- Provide oversight and strategic direction
- Monitor risks and ensure continuity planning is in place
- Review serious incidents

CEO (Continuity Lead)

- Leads response to incidents
- Makes operational decisions
- Activates this plan
- Liaises with trustees and stakeholders

Staff and Volunteers

- Follow instructions during incidents
- Report issues promptly
- Support service continuity

5. Business Continuity Principles

- Focus on critical functions first
- Plans must be practical and proportionate
- Use flexible working
- Protect people first, then services, then assets

6. Critical Functions

WV prioritises the following functions:

- Volunteer support and placements
- Communication with volunteers, partners and communities
- Safeguarding responsibilities
- IT systems and data access
- Governance, finance (including payroll and banking) and compliance

6.1 Financial Continuity

WV recognises that maintaining financial operations is critical.

Key Financial Functions:

- Payroll processing
- Supplier payments
- Banking access and cash flow management
- Grant management
- Financial reporting

Continuity Arrangements:

- Cloud-based accounting systems
- Two authorised banking signatories
- Secure credential storage
- Backup access procedures
- Remote payroll access

In the Event of Disruption:

- Treasurer ensures continuation of payroll
- Emergency authorisation process
- Prioritise salaries and essential payments
- Use manual processes if needed
- Liaise with bank and funders

7. Incident Response Framework

Stage 1 – Immediate Response

- Ensure safety of staff, volunteers and public
- Contact emergency services if required
- Notify CEO (or trustee if CEO unavailable)

Stage 2 – Assessment

- Identify type and severity of incident
- Assess impact on:
 - People
 - Premises
 - IT systems
 - Service delivery

Stage 3 – Activation

CEO decides whether to formally activate the continuity plan:

- Allocate roles and responsibilities
- Implement alternative arrangements

Stage 4 – Communication

- Inform staff and volunteers
- Notify key partners and stakeholders
- Provide updates as needed

Stage 5 – Recovery

- Restore services and systems
- Re-establish normal operations

Stage 6 – Review

After each incident:

- Review response effectiveness
- Identify improvements
- Update this plan accordingly

8. Key Contacts (Role-Based)

- CEO – Incident Lead
- Chair of Trustees – escalation and support
- Safeguarding Lead – safeguarding concerns
- IT Support Provider – system recovery
- Emergency services (999 / 101)

(Contact details maintained separately for security and accuracy)

9. Key Risks and Responses

9.1 Loss of Key Staff (e.g. CEO absence)

Impact: High

Response:

- Chair of Trustees assumes oversight
- Responsibilities delegated across team
- Temporary support or external expertise engaged if needed

9.2 Loss of Premises (fire, flood, vandalism)

Impact: Medium–High

Response:

- Activate remote working immediately
- Use alternative venues or partner spaces
- Inform stakeholders
- Contact insurers

9.3 Utilities Failure (power, water, internet)

Impact: Medium

Response:

- Shift to remote working where possible
- Identify alternative workspace if required
- Maintain essential communication via mobile devices

9.4 IT System Failure

Impact: High

Response:

- Use backup systems and cloud access
- Contact IT support provider
- Use alternative communication methods if needed
- Restore systems from backups

9.5 Theft or Security Incident

Impact: High

Response:

- Notify police and insurer
- Secure premises and systems
- Assess any data breach (follow Data Protection Policy)

9.6 Public Health Incident (e.g. pandemic)

Impact: High

Response:

- Follow government guidance
- Implement remote delivery where possible
- Maintain communication with volunteers and partners
- Adjust services to ensure safety

9.7 Financial Systems or Banking Failure

Impact: High

Response:

- Access backup banking
- Contact bank
- Use secondary systems
- Prioritise payroll
- Notify Chair

10. Safeguarding and Data Protection

- Safeguarding remains a priority in all incidents
- Concerns must be escalated immediately
- Data must remain secure and handled in line with Data Protection Policy

Continuity actions must not compromise:

- Safety
- Confidentiality
- Legal responsibilities

10.1 Critical External Dependencies

WV relies on:

- IT providers
- Cloud systems
- Payroll providers
- Banking services
- Telecoms
- Partners

Continuity Arrangements:

- Maintain provider contacts
- Regular backups
- Identify alternatives

11. Resources and Recovery

WV will:

- Use cloud-based systems for data resilience
- Maintain relationships with partner organisations for temporary support
- Access external expertise if required

12. Communication Plan

- Use email and phone and digital platforms
- Provide clear and consistent messaging
- Update stakeholders regularly

13. Training and Awareness

- Staff and volunteers will be made aware of this plan
- Key roles will receive additional guidance
- Continuity planning will be embedded in organisational practice

14. Monitoring and Review

- Reviewed every two years
- Updated after incidents
- Considered as part of organisational risk management

15. Continuous Improvement

After any incident:

- Lessons learned will be recorded
- Changes will be implemented
- Policies will be updated accordingly