Title:	**Business Continuity Plan**
Version:	**3.0**
Date:	**June 2026**
Reviewed:	**June 2026**
To be reviewed:	**June 2027**
Classification:	**Public**

1. Introduction

The purpose of this plan is to protect people, minimise disruption, and enable the Foundation to continue operating at a safe minimum level during unexpected events.

This plan supports our three strategic aims by ensuring continuity of our critical investment, grant-making and partnership activities.

We are a small organisation. This plan is deliberately simple and focuses on what we will prioritise if we cannot do everything.

2. Scope

The scope of this document is to ensure we minimise disruption to critical activities and ensure the Foundation can continue delivering our strategy.

This includes disruption such as:

- Loss of access to the office
- IT or cyber incidents
- Loss of key staff availability
- Disruption to banking, payments or suppliers
- Inability to run Board or committee activity

This plan focuses on maintaining essential activity rather than responding to every possible incident.

3. Critical Activities and Priorities

In a disruption, the Foundation will prioritise the following in order:

1. Communications – Ability to contact staff, trustees and key stakeholders (Same day)
2. Access to systems and data – Access to email and core files (Same day)
3. Urgent payments – Ability to approve and process priority payments [To be confirmed – requires testing with contractors and bank]
4. HR and financial operations – Payroll, staff support, and core financial processes [To be confirmed – requires testing with contractors and bank]
5. Governance – Board and committee decisions can proceed (Within 1–2 days) Investment activity – Maintaining oversight where decisions are time-sensitive (Within 1 week)
6. Grant-making and partnership activity – Maintaining contact with priority funded organisations, applicants and partners (Within 1 week)

Non-essential activity may pause.

Recovery expectations will be tested with key providers (e.g. banking, IT) and updated.

4. Roles and Responsibilities

- The Chief Executive decides whether to activate this plan
- In their absence, the Head of Governance will act as deputy

The Chief Executive (or delegate) will:

- Identify which critical activities are affected
- Agree priorities
- Coordinate communication with staff and trustees

Given the size of the organisation, responsibilities will be shared across the team.

5. Response Approach

1. Ensure people are safe
2. Decide whether to activate the plan
3. Identify affected critical activities
4. Agree priorities
5. Communicate clearly
6. Keep a simple record of decisions

6. Working Arrangements

The Foundation can operate remotely using laptops and cloud-based systems. Remote working will be the default. Meetings will be online and work will continue using shared systems.

Wellbeing:

- Line Managers will maintain regular contact
- Team check-ins will continue
- Existing guidance and training will be followed

7. IT and Cyber Incidents

The Foundation relies on external IT providers for response and recovery. We will:

- Contact IT provider
- Follow guidance
- Pause systems if required
- Assess impact
- Inform stakeholders if needed
- Resume once safe

8. Operational Continuity

- Urgent investment management e.g. liquidation and payments owed will be prioritised
- Alternative arrangements will be made for meetings, with non-essential meetings stepped down
- Other arrangements managed as needed, based on maintaining essential activity

9. Related Policies

- Data Protection Policy
- Information Security Policy
- Cyber Security Incident Response Plan
- Remote Working Policy

10. Review

This plan will be reviewed annually or following a significant disruption.