Title:	**Business Continuity Plan**
Version:	**2.0**
Date:	**April 2025**
Reviewed:	**June 2024**
To be reviewed:	**June 2025**
Classification:	**Public**

1. Introduction

The purpose of the business continuity plan is to ensure the safety of all employees and other affected stakeholders and maintain key functions in the event of an emergency.

We will educate all staff and trustees - new and existing - about the importance of continuity planning and ensure the plan is available and accessible to all who need to see it. Review of our emergency operations and planning will take place annually as well as any time the plan is significantly modified or there are significant changes within our organisation.

We pledge to do the following for our staff, trustees and advisers:

- Provide a safe working environment
- Implement emergency alerts in the event of a disaster
- Conduct a damage assessment to decide the best response and recovery plans possible
- If a shutdown occurs, provide employees, trustees and advisors with help and resources to support them
- Build upon agreed strategies to restore operations
- Provide backup storage for data
- Communicate all procedures in event of shutdown

2. Scope

This plan covers 3 types of emergency:

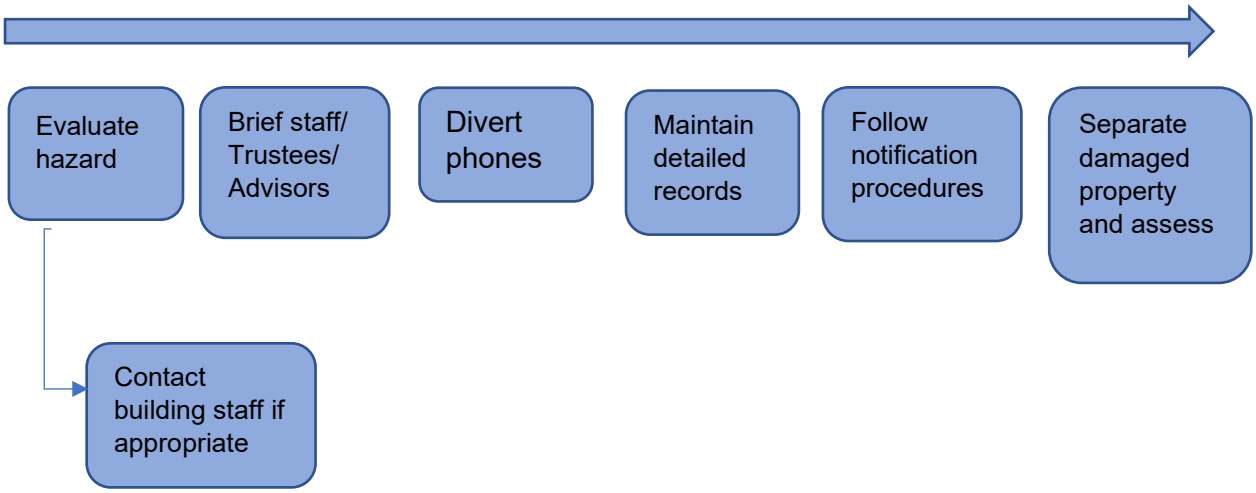
1. Inability to access central London owing to terrorist or similarly perilous action
2. Inability to access the building or other emergency which renders it unfit to work in
3. Catastrophic failure of business-critical IT systems

3. Emergency Response Workflow

In the event of an emergency, the Chief Executive (or in her absence, the Head of Communities and Governance) will be responsible for declaring emergencies, evacuating or shutting down the office as necessary and contacting employees, trustees and advisors.

The Chief Executive (or delegate) has the authority to identify critical business functions impacted by the emergency and initiate the process for recovering each function.

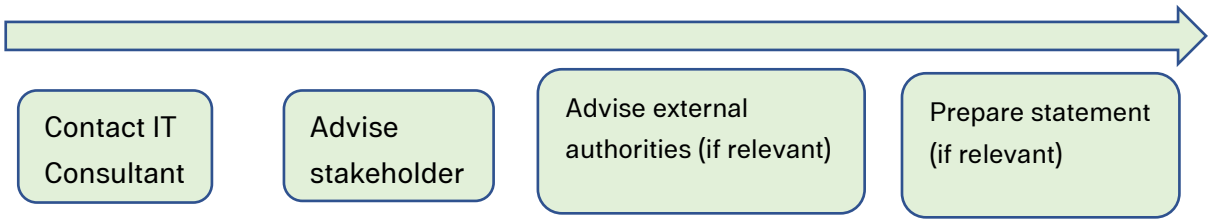
Types 1 and 2
In the aftermath of an emergency, follow these steps, as appropriate:



- Ensure the safety of personnel by evaluating hazards and, in the case of a type 2 emergency, contacting the building staff at the earliest opportunity and follow their advice on procedures to be followed
- Conduct an employee and Trustee/advisor briefing
- Divert telephones by contacting the building staff (for phones not already on divert).
- Maintain detailed records. (Record all decision making and video or photograph any damage)
- Follow notification procedures. Notify trustees, employees' designated contacts about on-duty personnel, notify off-duty personnel and alert insurers and appropriate agencies as required
- Separate damaged property from undamaged property and retain damaged goods until an insurance adjuster can view them. Protect undamaged property as much as possible
- Perform an assessment of any damaged property (with an adjuster, if possible)

Type 3

The Foundation's IT systems are all hosted through cloud technology. In the event of failure, follow the Cyber Security Incident response plan:



- Contact IT Consultant and initiate emergency back-up and restoration procedures
- Ascertain nature of failure and any implications for stakeholders (e.g. data theft)
- Advise affected stakeholders (and any necessary external authorities such as Information Commissioner)
- If nature of failure is likely to have reputational impact, prepare statement to include actions taken for future prevention and issue with approval of Chair of the Foundation.

Arrangements for working from home

Arrangements have been made to ensure that the work of the Foundation can be carried out as far as possible from the homes of the Foundation staff, using remote access and electronic means of communication. At the present time staff are working flexibly, with some days working from home and some days in the office.

In the event of an emergency situation arising, staff should all work at home and keep in contact via telephone (and email, if available).

Foundation staff have laptops for use at home which are configured to mirror office equipment and have access to all shared files remotely. (In the case of a type 3 emergency, office systems should only be accessed once the Chief Executive has obtained assurance from the Foundation's IT consultant that it is safe to do so).

Access and retrieve remotely any messages left on the voicemail system:

Dial 020 7871 5404 and once it goes to voicemail enter 0

Then enter the voicemail pin 92038

Arrangements for payments

In the event of an emergency situation where access to the London office is not possible, arrangements may need to be made with C Hoare & Co to issue new security tokens so that

urgent payments can be created and authorised via the on-line system if signatories do not have access to their tokens.

Collection of post
Dependent on the circumstances of the emergency, the offices should be checked once or twice per week for mail. If the emergency situation is likely to be prolonged temporary arrangements should be made with the post office for all post to be diverted to an agreed address, e.g. to a member of the Foundation's staff.

Alternative Meeting Room Venues and offices
In the case of a Type 2 emergency and where essential meetings need to go ahead, alternative meeting room venues should be arranged. Lenta Services (our office provider) have buildings throughout London and should be approached for a potential temporary office as well as alternative meeting rooms.

4. Related policies

Data Protection Policy
Information Security Policy
Mobile Computing and Remote Working Policy and Procedure