Title:	Business Continuity Plan
Version:	1.1
Date:	June 2018
Reviewed:	June 2018
To be reviewed:	June 2021
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 Executive Director (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 Executive Director (or her 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 managing agents at the earliest opportunity and follow their advice on procedures to be followed
- Conduct an employee and Trustee/advisor briefing
- Divert telephones via Nomis dashboard
- 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 Trust's servers have offsite backup. In the event of a power failure the server has an uninterruptable power supply (UPS). In the event of other type of failure:

- 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 Trust.

Arrangements for working from home
Arrangements have been made to ensure that the work of the Trust can be carried out as far as possible from the homes of the Trust staff, using remote access and electronic means of communication.

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

Trust staff have laptops and printers 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 Executive Director has obtained assurance from the Trust's IT consultant that it is safe to do so).

Access and retrieve remotely any messages left on the voicemail system:
Dial 020 7871 5409 and enter *201#
Then enter VM passcode 181113#

Arrangements for payments
In the event of an emergency situation where access to the London office is not possible, arrangements will need to be made with C Hoare & Co to issue a new token so that urgent payments can be created and authorised via the on-line system.

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 Trust's staff.

Fax Messages
Fax messages would not be affected by an emergency situation arising, as these are automatically diverted and received via email.

Alternative Meeting Room Venues
In the case of a Type 2 emergency and where essential meetings need to go ahead, alternative meeting room venues should be arranged.   Potential local meeting room venues are:

> International Dispute Resolution Centre (IDRC)
> 70 Fleet Street
> Tel: 020 7936 7000

OR

> Crowne Plaza Hotel
> 19 New Bridge Street
> Tel: 0871 942 9190

4. Related policies

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

THE DUNHILL MEDICAL TRUST
Registered Charity number 1140372 A company limited by guarantee, registered in England Company number 07472301.
Registered office: 6 New Bridge Street, London EC4V 6AB

BUSINESS CONTINUITY PLAN
JUNE 2018
Page **3** of **3**