Title of Document	**Business Continuity Management**
Name of Department	**Executive Team**

What type of document is this?	Policy	This sets out instructions for how a particular procedure in Helping Hands is to be routinely carried out	
Which Helping Hands POL/SOP/W.I does this document relate to?		**Reference number of POL/SOP/W.I**	

Which Operational Priority/Priorities does this document link to?	Governance Framework	Superior Client Care	People, Performance & Culture	Business Growth
	Maximising Efficiency & Cost Management	Facilities & Sustainability	Internal & External Communications	Information Management & Technology

Custodian of document	Chief Executive Officer	**Committee/Group responsible for this document**	Executive Team
Approval date and committee chairperson signature	25.03.25	**When is its next scheduled review?**	25.03.26

Who does it apply to?	All Helping Hands employees with the organisation				
	Does it apply to bank workers?	Yes	**Does it apply to agency staff?**	Yes	**Does it apply to third party contractors?**	Yes

Purpose of the Policy	Business Continuity Management (BCM) establishes a strategic framework in order to proactively implement the businesses continuity plan in the case of disruption, interruption or loss in supplying its products and services while protecting customers and employees, safety and care. Helping Hands needs to be able to plan for, and respond to, a wide range of incidents and events that have the potential to disrupt normal and safe processes to the business and customer care. The policy identifies potential business threats. It provides a framework that safeguards the interests of Helping Hands and provides a facility for operations to be “business as usual” with minimum of harm or loss.

	The aim of the policy is to provide a consistent business continuity plan response. It can be used at a branch level, for example in the instance of flood or fire that renders the branch inaccessible, through to organisation wide business continuity issues such as a cyber breach. All Helping Hands employees are required to adhere to the roles and responsibilities set out within this policy. A local incident response plan (as part of the overall business continuity plan) must be developed at all Helping Hands Sites, with the relevant card systems in place.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Executive Team, Senior Leaders and Managers	To ensure that the Business Continuity Plan (BCP) is embedded within the organisation and across all the teams and locations.
All Staff	To ensure that they understand the policy and the necessary actions that may be required.

1.0 Business Continuity Management Planning

Business continuity management plans have been completed by each branch and by the teams within the support office in the last 12 months.

All sites maintain a set of “relevant” action cards taking into account the local environment and relevant suppliers.

All branches are required to localise their Incident Response Plans (aligned to the Business Continuity Plan), including local suppliers and providers where applicable.

Below are the potential business threats

- ‘Short notice’ of a regulatory inspection
- A concerned CQC/CIW inspection, call immediately after verbal feedback of the inspection outcome
- Cyber breach
- Data breach / loss – customer / employee
- Loss of any/all office staff which will affect our ability to deliver the service/operate the service
- Loss of premises
- Loss of internet, telephony, corporate systems, website
- Loss of medical data
- Loss of mains water
- Loss of Security systems, Fire Alarm
- Forced Branch / Branches closure
- Serious Risks, Injuries, Deaths

- Serious PR risks (website)
- Neglect or Abuse
- Fraudulent activity
- Adverse weather conditions
- Flood; Fire; Power Failure, Sewage, Drainage, septic tank
- Criminal Incident eg Assault
- Bomb threat and suspicious packages / terrorism
- Serious Complaints
- Pandemic/Out-Break of Infection

2.0 Planning Arrangements

The business will, on an annual basis, refresh the Business Continuity Plan to clearly identify:

- What functions are critical activities:
- What level of service is acceptable in an emergency?
- That the action cards have been localised and edited and be kept in a Battle Box.
- What the trigger is to place the action cards in place including alert and standby procedures;

- The specific roles and actions (including where the action plan is located) that are taken when the action cards need to be placed into action;
- The stand down procedures, including the lessons learnt and the debriefing process and the returning to normal process.
- The contact details of the key personnel, relevant partners, agencies, local suppliers, landlords and key people contact list is kept up to date.

3.0 Be Prepared

- A staff communication is issued every six months;
- A desktop exercise led by the IT Director and Group Managing Director is carried out once a year, for each branch / department within the Support Office to ensure currency of the Incident Response Plans.
- A live exercise is carried out every 3 years
- (a live incident can be covered through a real incident when BCP is involved)

4.0 Business Continuity Management Process

Identification

Decide whether a Business Continuity Incident has occurred. If the incident is, or has the potential to be organisation wide, this decision should be immediately escalated to a member of the Executive Team. If it is a single Branch, this can be with the Regional Care Director or with the Group Managing Director. Then:

- Identify who the Incident Response Lead will be
- Identify who the Scribe will be

- Identify if there is a Local Coordinator required (either by function or by branch)

Where will the incident be managed from? E.g. Support Office or another location?

If the Incident is organisation wide, if possible, use the Teams Channel established for this purpose, as coordinated by one of the Executive Team, Incident Response Lead or the nominated Scribe.

Establish how communications will be managed – centrally or locally, or combination of both – dependent on the type of incident. To be defined by the Incident Response Lead.

Begin scribing an Incident Log Sheet as early as possible at identification stage, so as to have a working timeline document from start to close down.

5.0 Action

Immediate Action – this should be aimed at preventing harm to people, property and key business systems. Activating the use of the appropriate action card. This may involve evacuation, calling the emergency services or locking down of key systems (to be approved by CFO, CEO or IT Director only);

Interim Action – this is to provide as many services as possible in a safe manner and to protect the safety of our employees, customers and of the business

The coordination of the incident will include;

- Cascading of information to employees – cadence should be agreed as regular
- Keeping stakeholders including the Board and any key suppliers informed
- Establishing an Incident Response Team with shift cover if the incident is likely to go on for more than a few hours - make up of the team and location to be defined
- Providing the Action Cards and relevant documents to the incident.
- Deciding whether to source and deploy additional resources, internally or via partners and suppliers
- Consideration of PR, Regulatory and Insurance third parties
- Planning of timescales and intensity of actions and communications required.
- Completion of the detailed incident log sheet for lessons learnt

6.0 Incident Response Team

Will ensure the health and safety of customers, employees and third parties and account for all personnel. Will proactively seek to minimise damage, including data losses or reputational;
Will conduct a detailed and ongoing damage assessment

- Document all communications with external agencies
- Agree action plan and timescales
- Implement all telephone response plans, including with customers and employees
- Implement IT response plans in conjunction with IT
- Notify affected suppliers and if necessary any landlord
- Document decisions and situation with timestamp
- Reallocate and/or provide additional resources;
- Manage the return to “business as normal” process;

- Maintain a strict standard during the recovery period on financial security, information security, anti-fraud.
- Maintain records for insurance purposes and ensure insurers are notified appropriately
- All of the above should be documented on the incident log sheet

7.0 Recording and Reporting

This a vital process to enable further review and audit of actions taken to improve the process and outcomes.

- **Recording** – all decisions must be documented / Accurate minutes of the team meeting held on the incident log sheet(s).
- **Reporting** – Reports must be submitted to a senior management team member via the incident log sheet(s).

8.0 Improvements

As a result of an actual incident or an exercise the action cards if required should be updated to reflect the following;

- Any lessons learned/identified from an incident, emergency or exercise.
- Any restructuring and changes required
- Any employee, policy or process changes relating to business continuity
- Root cause of the incident and confidence that measures implemented to prevent a reoccurrence.
- Any change in systems or security
- Any change in guidance and policy

9.0 Learning

A debrief should be sent to the relevant senior managers and the Executive team and wider stakeholders as necessary.

TRAINING

Is training required?	Yes
Details of training	Local induction procedures should enforce individual and collective responsibility for business continuity. Guidance can be accessed through the Compliance Co-ordinator for Health & Safety. Annual desktop exercise to ensure readiness of key team members

COMPLIANCE

How is compliance with the POL going to be monitored	Reviewed as part of the internal Audit programme, unannounced basis and through support office desktop exercises.

EQUALITY IMPACT ASSESSMENT AND PROCEDURAL INFORMATION

	Positive / Negative / N/A	Comments
Does the document have a positive or negative impact on one group of people over another on the basis of their:		
• age?	N/A	
• disability?	N/A	
• gender reassignment?	N/A	
• pregnancy and maternity (which includes breastfeeding)?	N/A	
• race (including nationality, ethnic or national origins or colour)?	N/A	
• marriage and civil partnership?	N/A	
• religion or belief?	N/A	
• sex?	N/A	
• sexual orientation?	N/A	
If you have identified any potential impact (including any positive impact which may result in more favourable treatment for one particular group of people over another), are any exceptions valid, legal and/or justifiable?	N/A	
If the impact on one of the above groups is likely to be negative:		
• Can the impact be avoided?	N/A	
• What alternatives are there to achieving the document's aim without the impact?	N/A	
• Can the impact be reduced by taking different action?	N/A	
• Is there an impact on staff, client or someone else's privacy?	N/A	*If yes, privacy impact assessment required*

What was the previous version number of this document?	Version 01	
Changes since previous version	This document has been fully reviewed in line with review of incident response and recovery plans.	
Who was involved in developing/reviewing /amending the POL?	Chief Executive Officer IT Director Quality Development Lead	
How confidential is this document?	Public	Can be shared freely within Helping Hands and externally with strategic partners relevant to this policy

References	NA
Associated Documents	