Disaster Recovery & Business Continuity Plan

PURPOSE AND SCOPE

Step Ahead has a fully comprehensives range of insurances in the event that the unexpected occurs and we will be pleased to provide specific details of our policies if required.

This Disaster Recovery and Business Continuity Plan outlines how the business will maintain critical operations in the event of disruption, including IT failure, cyber incidents, environmental disruption or loss of key personnel.

The main risk to the business remains IT and systems-based disruption, given the organisation's reliance on cloud platforms and digital infrastructure.

DISASTER RECOVERY

Core IT Infrastructure

The company utilises a fully cloud-based system and, as all staff are remote workers, the business is not reliant on power or WiFi in one geographic area to ensure that operations can continue.

At Step Ahead, all staff have access to our fully integrated database and email systems, via secure password-protected accounts with appropriate access controls, ensuring optimum resources are available at all times. In the event that one member of staff is unexpectedly unavailable, another Consultant, Manager or Director is able to step in to provide continuity of service across the organisation.

System Dependence and Recovery

Should any issues occur with Sharepoint, Microsoft Office 365, online phone system or other shared systems, the company's IT provider or specific system providers will be able to work immediately to resolve.

As all information is held in the cloud, there is no issue with local data being lost should there be issues with individual's equipment.

IT Security and Equipment

All company equipment runs anti-virus and malware detection software to minimise the chance of systems getting infected. These are monitored by our IT provider.

All IT equipment used within the business is the property of the business and is maintained by the IT provider. In the case of failure, replacements can be sent and set up by the following day. Replacement equipment is stored at the IT provider's site as well as two members of staff having a full set of spare equipment to be able to send out if needed.

ENVIRONMENTAL DISASTERS

The following plans are in place in case of environmental disasters or events.

On an individual basis, staff have access to co working spaces (Regus and WeWork Offices) so can go to their local venue to work should their usual place of work not be viable for example power outages, WiFi not working, flooding.

If individuals WiFi goes down for any length of time, staff can use mobile hot spot access for any necessary access to cloud based information.

As staff are geographically dispersed, environmental issues in a local area will have a lesser impact as staff in other locations have access to all files, company databases etc. via the cloud.

Staff locations are monitored to take into account likely weather based issues such as storms leading to power or internet access issues or flooding. No role in the business can be done solely by one person and critical business processes such as payment of temporary workers weekly payroll can be done by a minimum of two people to allow for localised issues.

In case of wider spread issues that impact on a greater number of staff, all critical business processes that need to be done to ensure business continuity can be picked up by the Managing Director who has a back up generator to enable continuity of power for the processing of any business critical processes.

Critical business processes are:

- Processing of temporary workers payroll weekly
- Processing of staff payroll monthly
- Uploading of financial data to external sites to specific deadlines as required

These can all be done by a minimum of 2 people in the business and should there be any issues with the processing of any more complex processes, plans are in place to be able to easily do simple bank payments with adjustments made at a later date. Uploading of other financial data, although business critical, has lead times of several weeks so it is highly unlikely that this would be compromised.

Any other business activity can either be picked up by other staff or carried on after any issues had been resolved.

BUSINESS CONTINUITY

As all staff are remote workers, no plans are required for business issues relating to locations not being accessible.

Leadership Team (LT) meetings include discussions on current business activity and all members of the LT are able to caretake other areas if required and suppliers such as the Accountant and IT provider can provide additional support or input as needed.

Business Continuity Action Plans are in place for all departments of the business.

The key roles that need to be covered are:

- **Director of Compliance & Claims** - This role is also the Ofsted nominee, and in the event of absence for any significant period, the Head of Compliance is able to fulfil this role.

- **Head of Compliance** – all urgent compliance tasks can be undertaken by a member of the compliance team.
- **Finance** – Urgent finance tasks such as payment of monthly and weekly payroll can be undertaken by the Corporate Admin Assistant. The Chief Executive can, in addition deal with any finance tasks as needed including making bank payments.
- **Chief Executive** – Day to day business matters can be managed by the Director of Business Improvement and Quality with support from the company Accountants and legal adviser if needed.

All information relating to contracts and other service provision is stored in the cloud based CRM system and Sharepoint file system which is accessible to all users so picking up on any aspect of individuals work can be done effectively.

CYBER INCIDENT REPORTING AND EXTERNAL IT ESCALATION

All staff are required to report any suspected cyber incident immediately upon discovery. Cyber incidents include, but are not limited to, phishing emails, suspected credential compromise, malware or ransomware infections, unauthorised access to systems or accounts, data loss or corruption, or any unusual system behaviour which may indicate a security breach.

In the event of a suspected incident, staff must report it immediately to the external IT support provider, manager and a member of the Leadership Team. Prompt reporting is essential to limit potential damage and ensure a rapid response.

Staff must immediately cease using any affected system or device and must not attempt to investigate or resolve the issue themselves unless instructed to do so. Emails, files or system alerts should not be deleted, as they may be required for investigation purposes. Where advised, devices should be disconnected from the internet to prevent further risk.

The external IT support provider will take responsibility for assessing the incident, containing any affected systems and initiating appropriate recovery actions. This may include system isolation, account recovery, malware removal or restoration of services.

Where personal data is involved, the incident will be assessed in line with UK GDPR requirements, and where necessary, notifications will be made to the Information Commissioner's Office (ICO), or any other relevant regulatory body where applicable, within statutory timeframes. This will typically be within 72 hours of becoming aware of the breach where there is a risk to individuals' rights and freedoms.

Where there is likely to be a high risk to affected individuals, those individuals will also be informed without undue delay and provided with appropriate information about the nature of the breach and any steps they should take.

All cyber incidents will be recorded, including details of detection, systems affected, actions taken and resolution steps. Following resolution, a review will be conducted by the Leadership Team in conjunction with the IT provider to identify root causes and any improvements required.

COMMUNICATIONS PLAN

Effective communication is essential to maintaining continuity of service during any disruption affecting systems, staff availability or business operations.

Internal communication will primarily take place via Microsoft Teams and email. In the event that these systems are unavailable, communication will continue via mobile phone and SMS to ensure staff remain contactable.

The Managing Director or nominated Leadership Team member will coordinate internal communications, including confirmation of incidents, allocation of tasks and ongoing operational updates. Staff are expected to acknowledge communications promptly and escalate any inability to access systems.

Externally, communication will be maintained with clients, candidates, contractors and suppliers where appropriate. Clients will be informed where service delivery may be delayed, candidates will be updated on interviews, onboarding or placement activity, and contractors will be informed of any impact on payroll processes.

Where systems are unavailable, communication will continue using alternative methods such as email, telephone or SMS. All external communication during an incident will be approved by the Leadership Team to ensure consistency and accuracy.

During any disruption, the business will aim to acknowledge incidents within two hours where possible and provide regular updates depending on severity. Clear communication regarding expected resolution times will be provided where known, with confirmation issued once normal operations resume.

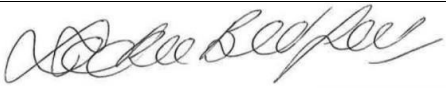
PLAN ACTIVATION, TESTING AND REVIEW

This plan will be activated in the event of any incident that significantly disrupts normal business operations, including but not limited to IT system failure, cyber incident, loss of critical systems, environmental disruption affecting multiple staff, or any event that prevents the delivery of core business services.

The decision to activate this Business Continuity Plan will be made by the Managing Director or, in their absence, a nominated member of the Leadership Team. Once activated, the business will prioritise the continuation of critical services, communication with stakeholders, and the restoration of normal operations as quickly as reasonably possible.

This Business Continuity and Disaster Recovery Plan will be reviewed at least annually, or sooner if there are significant changes to the business, its systems, or operating model. Following any activation of the plan or significant disruption, a review will be carried out to assess effectiveness and identify any required improvements.

Disaster Recovery & Business Continuity Plan

Document Control	
Document Title: Disaster Recovery & Business Continuity Plan	
Version Number: 1.2	Document Owner: Corporate Support
Date Approved: 16 June 2025	Approved By: Jackie Bedford, CEO
Effective Date: 16 June 2025	
Superseded Version: 1	
Date of Last Review: 2 June 2026	Date of Next Review: 1 July 2027