PINEAPPLE PARTNERS

Business Continuity Plan

Title of Policy Document **Issue Date and Version**	Business Continuity Plan January 2026 (Version 1)
Author / Department	Executive Management Team
Signed off by	 Director
Next review date	January 2027
Distribution	All services
First issue date	January 2026

1. Purpose

Care homes still need carers and depots still need crews when our office has a bad day. Business continuity management is how Pineapple Partners keeps its essential services running through disruption, and recovers quickly from it. This plan identifies our critical activities, the things most likely to threaten them, and what we do in each case.

2. Policy statement

We will maintain proportionate, tested arrangements so that: placed workers continue to be supported and paid; clients can always reach us; candidate and business data stays safe; and normal service resumes as fast as circumstances allow. The Director owns this plan; every member of staff knows their part in it.

3. Our critical activities

- Paying temporary workers on time, payroll is the activity we protect first.
- Being reachable: phones and email for clients, workers and candidates.
- Filling booked assignments and honouring commitments already made.
- Protecting data: candidate records, vetting evidence and business systems.

4. Staffing disruption

Sickness, weather or transport problems: our systems are cloud-based, so staff can work fully from home at no notice. Key tasks, payroll, bookings, compliance, have at least two people able to run them, and directors provide final cover. During a wider event such as an epidemic we follow government guidance, move to remote working, and prioritise the critical activities above over everything else.

5. Premises, facilities and equipment

Loss of access to the office, fire, flood, utilities failure, does not stop the business: no critical system lives only in the building. Staff relocate to home working immediately; post is redirected; and physical records, kept to a minimum by design, are stored securely and duplicated digitally wherever practicable.

6. Technology, communications and data

Core systems are cloud-hosted with provider resilience on top of our own backups (see the Data Backup Procedure: daily backups, three-month retention, tested restores). Office phone numbers can be redirected to mobiles within hours. Loss of a laptop is an inconvenience, not an incident: devices are encrypted and data lives in the cloud, and the device is remotely revoked.

7. Suppliers and transport

For critical suppliers, payroll processing, IT, job boards, we know the alternatives before we need them, and avoid arrangements that cannot be substituted at reasonable speed. Fuel or transport disruption shifts work to phone and video, and we help placed workers and clients agree practical arrangements site by site.

8. Emergencies involving people

Any emergency involving injury or danger to a member of staff, a placed worker or a third party comes first, before any business consideration: emergency services, then the people affected and their families, then clients, then everything else. Serious incidents are reported and investigated under our Health and Safety Policy.

9. Testing, learning and review

Elements of this plan, remote working, restore tests, contact cascades, are exercised at least annually. After any real disruption we review what worked and what did not, and update the plan. The Executive Management Team reviews it in full every year.