

Business Continuity Policy

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014	15, 17, 18
Care Quality Commission (Registration) Regulations 2009	18a
CQC Single Assessment Framework Topics Safe Topic Areas: Safe systems, pathways and transitions Safe environments Safe and effective staffing Effective Topic Areas How staff, teams and services work together Caring Topic Areas Responding to people's immediate needs Responsive Topic Areas: Care provision, integration and continuity Well-led Topic Areas: Governance, management and sustainability Partnerships and communities Learning, improvement and innovation	

Please see the 'Quality Statements' section for full guidance

Scope

Business continuity planning is in place within the organisation and aims to reduce interruptions to business activities and to protect critical business processes from the effects of minor or major service failures or natural/manmade disasters that may disrupt or stop services to service users.

This policy and procedure are provided for the regulated activity of personal care.

Equality Statement

Our organisation is committed to equal rights and the promotion of choice, person-centred care and the promotion of independence. This policy demonstrates our commitment to creating a positive culture of respect for all individuals. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to reflect the Human Rights Act 1998 to promote positive practice and value the diversity of all individuals.

Key Points

- The risks identified under this policy include interruptions to business activities, disasters and unavailability of staff.
- The business continuity plan will be subject to regular testing.
- Key contact details for this organisation are listed in Emergency Contact Information in this policy.
- Appendix A sets out actions to be taken in the event of particular incidents.
- The fire risk assessment is provided in the 'Fire Safety Policy.'

- Care Quality Commission (Registration) Regulations 2009: Regulation 18 notification is to be made to CQC if the business is interrupted from its normal functioning for 24 hours.
- Training will be provided to staff, especially office and out of hours staff, on this policy.
- The key priority of this policy is to keep service users as safe as possible and provide a continuity of service during incidents which may disrupt the service.
- On occasion services will be disrupted and we will only be able to deliver a limited service, e.g. during heavy snow or floods.
- At these times we will prioritise the most at risk service users who we have previously identified.
- This will be coordinated by the management team within the office who will communicate directly with staff delivering services and service users and their family.
- Staff are responsible for identifying when they are running late or there is significant disruption that the office may not be aware of.
- The office is responsible for informing the service users and modifying visit schedules.

Policy Statement

The business continuity plan will be developed based on identification of risks to service continuity, with mitigation identified to minimise disruption to the business activity and services to service users. Mitigation activities will prioritise those service users most at risk due to health and social care needs or who lack alternative support, e.g. no local family.

The business continuity plan will be tested on a regular basis (at least annually). The test will include ensuring that all staff and any other relevant persons are aware of the plan.

The test schedule for the plan will indicate how and when each element of the plan will be tested. A variety of techniques will be used in order to provide assurance that the plan will operate in real life.

The business continuity plan will be maintained by regular reviews (minimum of annually or as concerns arise, e.g. COVID-19) and updates to ensure its continuing effectiveness.

Responsibility for development and regular reviews of the plan will rest with the Registered Manager or be formally assigned to another senior manager in writing. The Plan will include contact details of the local authority, local health services, including CQC and other commissioners and where relevant out of hours contact details.

The Policy

It is important that a managed process is in place to develop and maintain business continuity for the organisation, and to as much as possible provide continuity of care for service users. The

following key areas will be part of the business continuity process:

- Identification of risks that could affect the organisation.
- Identification of the assets involved in critical business processes.
- An understanding of the impact, and consequences, should anyone or combination of events occur within the organisation.
- Ensuring that the service has suitable and adequate insurance as part of the business continuity process.
- Ensuring sufficient financial, organisational, technical and environmental resources are available to address the identified information security requirements.
- Ensuring the safety of personnel and the protection of information processing facilities and service property.
- Development and documentation of business continuity plans addressing information security requirements.
- Regular testing and updating of the plans and processes put in place.
- Allocation of responsibility for co-ordinating the business continuity management process to an appropriate person in the service
- Identification and consideration of additional preventive and mitigating controls.

Risk Assessment

The organisation will identify the key business functions and events that can cause interruptions to its day-to-day business processes, e.g. equipment failure, major pandemics, lack of staff, flood and fire. A risk assessment will then be undertaken to determine the impact of those interruptions, both in the damage scale and recovery period. This assessment will consider all business processes and will not be limited to information processing facilities.

A continuity plan will be developed, using the results from the risk assessment, which will determine the overall approach. The continuity plan will be endorsed by both the organisation and where appropriate the commissioner.

Examples of incidents that could impact on business critical activities include:

- Traffic Delays - Care and support workers and office staff
- Severe wind, rain or snow
- Severe heat
- Fuel shortage
- Pandemic
- High levels of sickness absence
- Postal strike
- Telephone systems
- Sabotage of, or break to, regulated office

- Offices are inaccessible
 - Home care roster system failure
 - Supplier or supplies unavailable
-
- Utilities
 - Broadband
 - IT
 - Personal Protective Equipment

This list is not exhaustive, and the organisation will review its business critical activities on a regular basis to identify any changes or areas which need to be updated.

Developing and Implementing a Continuity Plan

Plans will be developed to maintain, or restore, business operations in the required time scales following interruptions to, or failure of, critical business processes.

Business Continuity Planning Framework

The business continuity plan will specify the conditions for its activation, including timing, resources, and the individuals responsible for executing each component.

The plan will include:

- Conditions for activating the plan.
- How the plan will be activated.
- Emergency procedures, including effective liaison with the CCG, CQC, public authorities, e.g. the Police, fire service and local government and other business partners.
- Fall-back procedures, e.g. manual processes.
- Temporary operational procedures to follow pending completion of recovery and restoration.
- The resumption of procedures, a schedule of how and when normal working practice can be resumed.
- A schedule of when the plan will be tested and the process of maintaining the plan.
- How an effective and on-going awareness and training scheme can be developed.
- How all individuals will be made aware of their roles and responsibilities with a full understanding of who deputises for whom in the eventuality of absenteeism.
- The critical assets and resources needed to be able to perform the emergency fall back and resumption procedures.
- The plan will include key contact details for utilities and other key suppliers.

- The plan will include contact details of the local authority, local health services, including CQC and other commissioners and where relevant out of hours contact details.

Emergency Contact Information

Utility	Provider	Emergency Contact Details
Electrical	Pozitive Energy (0333 370 990).	(0161 8373395)
Gas	Our gas is provided by SEFE	0161 8373395
Water	Water Plus	(0345 072 6072)
Telecommunications (land line, fax, internet)	Gifgaf	0800
Mobile phone	Gifgaf	Francis proxycare personnel ltd IT personnel and or Gifgaf customer care
Broadband	Our broadband is provided by Technology	02079538800
IT supplier (add lines for each provider)	We source that privately as the need arises	Francis
PPE supplier	Glove man	Glove man
Landlord	Bizspace	02083717180 Kinnaird House, 1 Pall Mall East, London, SW1Y 5AU headoffice@bizspace.co.uk
Building maintenance	Bizspace	eliza.kettle@bizspace.co.uk 07811 996090 www.bizspace.co.uk Paramount House Business Centre, 1 Delta Way, , Egham , TW20 8RX
Water management/Legionella	Our Water is provided by Water Plus, we do not do this as we rent the office space from Bizspace and pay our all inclusive bills rent as Bizspace manages the property.	0345 072 6072

Plumbing Issues

Location of stopcock: in the lounge on the first floor

103 Paramount House, 1 DELTA WAY

v1 Last Reviewed: (Care Coordinator) Wed Jun 03 2026

Next Review: Registered Manager Thu Jul 01 2027

Locally Responsible: Akosua Konadu

IT Failure

The company uses IT for a range of activities including staff rota systems, communications between clients and suppliers and storage of records.

- Paper records are retained securely of all crucial contracts, orders and receipts.
- Any data on local systems will also be backed up to the cloud where possible.
- Data that cannot be backed up to the cloud will be held on a secondary data server for emergency access.
- IT back up procedures for the service include:
 - At Proxycare Personnel Ltd, IT backup procedures are essential for safeguarding data and ensuring business continuity. The backup procedures for each IT service include the following key measures: 1. Data Storage & Backup Frequency: Cloud-Based Services: All critical files and documents are stored using secure, cloud-based services with automated daily backups. Local Storage Backup: Any local data stored on company devices is backed up weekly to an external hard drive or a secure network storage system. Database Backup: Any internal databases used for operations or client records are backed up daily to ensure no data loss in the event of system failure. 2. Backup Types: Incremental Backups: Changes to files are captured incrementally throughout the day to minimize the risk of data loss between full backups. Full Backups: A full backup of all systems and data is performed at least once a week. 3. Disaster Recovery Plan: Offsite Backup: A copy of critical data is stored offsite (via cloud services) to ensure availability in the event of a disaster at the office location. Testing and Monitoring: Regular tests of the backup and recovery process are performed to verify that data can be successfully restored when needed. 4. Security Measures: Encryption: All data backups, whether cloud-based or local, are encrypted to protect against unauthorized access. Access Controls: Only authorized personnel have access to backup systems, reducing the risk of accidental deletion or tampering. 5. Backup Retention: Retention Periods: Backup files are kept for a period of 30 days before being overwritten, ensuring there is a sufficient history of data available in case of accidental deletion or corruption. Compliance: Backup procedures comply with relevant data protection regulations to ensure the security and confidentiality of service user information. 6. Documentation: Backup Logs: Backup operations are logged, and records are maintained to track the status of each backup, ensuring transparency and accountability. Procedure Documentation: Detailed instructions for performing backups and data recovery are documented and made available to IT staff to facilitate swift recovery in the event of data loss. This backup protocol ensures that all critical IT services and data are protected from loss or damage, and can be quickly restored when needed

Adverse Weather Conditions

If we are unable to reach our company offices, due to adverse weather conditions, it is expected that staff will hold sufficient supplies and equipment to maintain business continuity for 24 hours. Any periods longer than this and the management team will liaise with staff on restocking their supplies of Personal Protective Equipment.

If staff are affected by adverse weather conditions and are therefore unable to attend a community care appointment, they must inform their Line Manager of this as soon as possible so that alternative arrangements can be made.

Where their attendance is delayed, due to adverse weather conditions, this should be relayed to their Line Manager and the office will provide the service user with a revised arrival time.

Disruption of Service

The organisation has a pre-defined list of service users who have been prioritised based on need/vulnerability to assist the organisation in managing a disruptive incident to service provision which reduces available staff numbers and/or geographic coverage.

Rating	Priority	Criteria
Red	1	Service users who require complete support, e.g. personal hygiene, feeding, medication assistance, through the night cover. Service users who are immobile and isolated and whose only daily contact is the Care Support Worker. Service users who must be seen on time, e.g. Time Specific Medication (e.g. insulin).
Amber	2	Again, complete support required (as above) but have other support mechanisms that can be used i.e. family, friends and/or other Agencies who also provide a service to them. Client Must be seen that day but not time specific.
Green	3	Service users who are more able and receive companionship, help with household chores and/or shopping, and who will be able to meet their own needs for a few days. Service users who do not need to be seen or have effective support from family and friends close by.

Service users are therefore prioritised in the event of a disruptive incident (regardless of the type of incident) which will ensure an appropriate and effective response based on an individual's needs.

This system will be initiated at times of service disruption due to:

- Snow and floods
- Traffic congestion
- Unexpected high levels of staff illness
- Unexpected levels of staff shortages

In addition, the organisation will work with local authorities (LA), Clinical Commissioning Groups, the NHS, police and other providers to ensure a coordinated approach to any local, regional and national incidents, e.g. COVID-19.

The organisation will use a range of guidance, communication and information to adapt and improve its response and update the business continuity response.

It will be the responsibility of the Registered Manager to review and update the guidance in line with the nature of the incident and the timing of information being published. Updates will be published to staff in the form of policy and procedure changes, training updates and information provided at staff meetings etc.

Closure of a Service

The registered provider, working with the management team including the Registered Manager, will prepare and implement an action plan which sets out what will happen to the service users accommodated at the registered location in the event of the service ceasing to provide accommodation (either temporarily or permanently). This plan will be developed in partnership with private residents, social and health service commissioners, CQC, and relevant other agencies.

Ceasing to provide accommodation could be as a result of financial insolvency, or due to cancellation or suspension of the registration by CQC, or the imposition of restrictions on particular settings or conditions imposed by CQC.

The Contingency/Disaster Recovery Plan will set out the measures that would be undertaken to ensure the appropriate transfer of records, safe transfer of service users, TUPE of staff where relevant, effective communication with all stakeholders, especially service users, family and staff.

The registered person should ensure that disruption to residents' lives is kept to a minimum in the event of service closure, that service users are kept informed of what is happening and why and that there is consistency of support throughout.

The registered provider and the management team will provide the contingency plan to the commissioning authority. The registered person should work with the commissioning authority to ensure that alternative accommodation is provided in the event of temporary or permanent closure.

Care Quality Commission (Registration) Regulations

2009: Regulation 18: Notification of Other Incidents

Providers must notify CQC of all incidents that affect the health, safety and welfare of people who use service.

In all events the manager, will make a Regulation 18a notification to CQC within 24 hours of an incident. The regulation requires a notification to be made in:

- Any event which prevents, or appears to the service provider to be likely to threaten to prevent, the service provider's ability to continue to carry on the regulated activity safely, or in accordance with the registration requirements, including:
 - An insufficient number of suitably qualified, skilled and experienced persons being employed for the purposes of carrying on the regulated activity,
 - An interruption in the supply to premises owned or used by the service provider for the purposes of carrying on the regulated activity of electricity, gas, water or sewerage where that interruption has lasted for longer than a continuous period of 24 hours,
 - Physical damage to premises owned or used by the service provider for the purposes of carrying on the regulated activity which has, or is likely to have, a detrimental effect on the treatment or care provided to service users, and
 - The failure, or malfunctioning, of fire alarms or other safety devices in premises owned or used by the service provider for the purposes of carrying on the regulated activity where that failure or malfunctioning has lasted for longer than a continuous period of 24 hours.

CQC can prosecute for a breach of this regulation or a breach of part of the regulation. This means that CQC can move directly to prosecution without first serving a warning notice.

Pandemic Management

Public Health England (PHE) has responsibility to protect the public from an outbreak and to provide guidance to organisations. A pandemic is recognised as high risk to the health and social care sector. PHE publish preparedness strategies and response plans in their preparation.

The five phases of detection, assessment, treatment, escalation, and recovery are monitored, appropriate data collected, the route of the pandemic tracked, and advice and guidance issued, as appropriate. This has been seen during the COVID-19 pandemic, and has highlighted the required need for preparation, planning and the effect on staffing levels.

Force Majeure Situations

When a *force majeure* occurs, e.g. flooding, road blockages, and winter conditions, we will take advice/guidance and co-operate with local authorities and emergency teams, as well as all relevant statutory agencies. For example:

- Emergency centres.
- Evacuation procedures.
- Staff secondment.
- Supporting other providers with staffing.

We will use our local knowledge, and our relationships with multi-agency partners to enable us to deliver the service, except where advice is given not to. We are knowledgeable of winter plans from our local councils and NHS and will review guidance updates immediately in order to manage the situation effectively.

A statutory notification must be sent to CQC, if any of the above situations were likely to last more than 24 hours and impact on the quality or effectiveness of the service.

COVID-19 Statement

Currently there are no COVID-19 rules or restrictions in the UK, though this could change if there is another major outbreak.

It is the responsibility of the Registered Manager and organisation to monitor the English Government guidelines for any changes to the guidance and law. See '[Adult social care: guidance](#).'

In addition, there is guidance in place from NHS England, the UK Government and Health and Safety Executive on how care settings should minimise risk to both care workers and service users.

This advice should be incorporated into the risk management and health and safety policies, procedures, and systems of work where appropriate.

Please see:

- [COVID-19 restrictions replaced by public health advice, HSE](#)
- [Infection prevention and control in adult social care: acute respiratory infection](#)

Specific additional ACS Guidance (used in conjunction with 'Infection prevention and control in adult social care: acute respiratory infection'):

- [Infection prevention and control in adult social care settings](#)
- [Infection prevention and control: resource for adult social care](#)
- [Infection prevention and control: quick guide for care workers](#)

References and Further Reading

[Care Quality Commission \(Registration\) Regulations 2009](#)

[The Care Quality Commission \(Registration\) and \(Additional Functions\) and Health and Social Care Act 2008 \(Regulated Activities\) \(Amendment\) Regulations 2012](#)

[Guidance for providers on meeting the regulations, CQC](#)

[Business Continuity Planning, Care Provider Alliance](#)

[Power disruption and costs, Care Provider Alliance](#)

[Business Continuity Planning Guidance and Templates, The Care Provider Alliance](#)

[Fuel Disruption, The Care Provider Alliance](#)

[Better Security, Better Care, Digital Care Hub](#)

[Infection prevention and control in adult social care: acute respiratory infection](#)

[UKHSA health protection teams](#)

[COVID-19 restrictions replaced by public health advice, HSE](#)

[Infection prevention and control in adult social care: acute respiratory infection](#)

[Infection prevention and control in adult social care settings](#)

[Infection prevention and control: resource for adult social care](#)

[Infection prevention and control: quick guide for care workers](#)

Quality Statements

Safe systems, pathways and transitions

We work with people and our partners to establish and maintain safe systems of care, in which safety is managed, monitored and assured. We ensure continuity of care, including when people move between different services.

Safe environments

We detect and control potential risks in the care environment. We make sure that the equipment, facilities and technology support the delivery of safe care.

Safe and effective staffing

We make sure there are enough qualified, skilled and experienced people, who receive effective support, supervision and development. They work together effectively to provide safe care that meets people's individual needs.

How staff, teams and services work together

We work effectively across teams and services to support people. We make sure they only need to tell their story once by sharing their assessment of needs when they move between different services.

Responding to people's immediate needs

We listen to and understand people's needs, views and wishes. We respond to these in that moment and will act to minimise any discomfort, concern or distress.

Care provision, integration, and continuity

We understand the diverse health and care needs of people and our local communities, so care is joined-up, flexible and supports choice and continuity.

Governance, management and sustainability

We have clear responsibilities, roles, systems of accountability and good governance. We use these to manage and deliver good quality, sustainable care, treatment and support. We act on the best information about risk, performance and outcomes, and we share this securely with others when appropriate.

Partnerships and communities

We understand our duty to collaborate and work in partnership, so our services work seamlessly for people. We share information and learning with partners and collaborate for improvement.

Learning, improvement and innovation

We focus on continuous learning, innovation and improvement across our organisation and the local system. We encourage creative ways of delivering equality of experience, outcome and quality of life for people. We actively contribute to safe, effective practice and research.

[Key questions and quality statements - Care Quality Commission](#)

Appendix A: Critical Incident Response

CRITICAL INCIDENT	DETAILS	CONTINGENCY/DISASTER RECOVERY PLAN (ACTION TO BE TAKEN)
1. Natural Disasters	Flooding through heavy rain or burst pipes. Structural damages to premises following a storm.	All persons to be moved to empty rooms within the building. If whole building affected people will evacuate. At Proxycare Personnel Ltd, in the event that the office buildings are unavailable for more than 72 hours due to a natural disaster, the organization has the following contingency plans in place to ensure continuity of operations: 1. Remote Working: Remote Access for Staff: All essential staff members are equipped to work remotely using laptops, mobile phones, and secure access to cloud-based systems. This allows business functions to continue without the need for physical access to the office. Communication Tools: The organization uses video conferencing tools and instant messaging platforms (e.g., Microsoft Teams or Zoom) to ensure ongoing communication between team members and with clients. 2. Cloud-Based Data and Systems: Cloud Infrastructure: All critical business systems,

including care management systems, document storage, and communication platforms, are cloud-based. This ensures that staff can access data and services from any location with internet connectivity.

Data Backup & Access: Regular backups ensure that no data is lost, and recovery can be implemented quickly without physical access to servers located on-site.

3. Emergency Contact Protocol: Staff and Client Communication: A predefined communication protocol is in place for notifying staff, clients, and stakeholders about building inaccessibility and alternative plans. This includes email, SMS alerts, and WhatsApp notifications.

4. Temporary Office Locations: Alternative Workspace: In case of long-term building inaccessibility, arrangements have been made with business centers or co-working spaces to provide temporary office accommodations for key personnel.

5. IT Support: Technical Assistance: IT support is available to resolve any technical issues that may arise with remote access, ensuring that systems remain operational even in the event of extended building closures. These measures ensure that Proxycare Personnel Ltd can continue to operate effectively even in the face of a natural disaster that renders the physical office unavailable for an extended period.

To determine if the area where Proxycare Personnel Ltd is located is a flood concern, it's essential to consult local flood risk assessments and guidance. Here are some general steps and resources to consider:

1. Flood Risk Assessment: Local Council Website: Check the local council's website for flood risk maps and assessments. Many councils provide detailed information about flood-prone areas, including historical data

		and risk levels. Environment Agency: In the UK, the Environment Agency offers comprehensive flood risk maps, showing areas at risk of flooding from rivers, surface water, and the sea. Their website can be accessed for specific area assessments. 2. Local Flood Guidance: Flood Alerts and Warnings: Sign up for flood alerts through your local authority or the Environment Agency. They provide timely information about potential flooding and recommended actions. Emergency Preparedness: Local authorities often publish guides on preparing for floods, which include tips on safeguarding property and ensuring the safety of individuals. 3. Emergency Contacts: Local Emergency Services: Keep contact information for local emergency services, including police, fire, and ambulance services, readily available. Floodline: In the UK, you can contact Floodline at 0345 988 1188 for immediate flood advice and updates. Local Council Emergency Planning Team: Reach out to your local council's emergency planning team for information on flood response strategies and support services available in your area. For more specific information regarding flood concerns in your area, consider visiting the following resources: Environment Agency - Flood Risk Local Council Flood Information By keeping informed and prepared, you can better protect the organization and its stakeholders from potential flooding issues.
2. Fire	Fire outbreak causing loss of facilities, equipment and data.	See the 'Fire Safety Policy.' At Proxycare Personnel Ltd, we have established comprehensive plans to ensure operational continuity in the event that our buildings are unavailable for more than 72 hours due to a fire. The following measures

are in place: 1. Emergency Response Protocol: Immediate Evacuation Procedures: All staff are trained in emergency evacuation procedures to ensure their safety during a fire incident. Regular fire drills are conducted to familiarize everyone with the protocols. Incident Reporting: Any fire incident is reported immediately to emergency services and relevant authorities to ensure a swift response. 2. Remote Work Capability: Cloud-Based Operations: All essential operations are conducted through cloud-based systems, allowing staff to access necessary data and applications from any location with internet connectivity. Remote Access Tools: Employees are provided with secure remote access to facilitate their ability to work from home or alternative locations as needed. 3. Communication Plans: Staff Notifications: A communication protocol is in place to notify staff of the situation and any changes to operations via email, SMS alerts, and instant messaging platforms. Client and Stakeholder Communication: Clients and stakeholders are promptly informed about the incident and the organization's contingency plans to maintain trust and transparency. 4. Alternative Workspaces: Prearranged Co-Working Spaces: In case the primary office space is unavailable for an extended period, arrangements have been made with local co-working spaces or business centers where staff can work temporarily. Equipment Access: Essential equipment and supplies are available at alternative locations to support staff in continuing their work effectively. 5. Data Backup and Recovery: Regular Data Backups: The organization employs routine backups of all critical data to secure locations, ensuring data integrity and availability for recovery if needed. Disaster

		Recovery Plan: A documented disaster recovery plan is in place, detailing the steps to recover operations following a fire incident, including data restoration and system recovery processes. 6. Regular Reviews and Drills: Plan Review: The fire response and recovery plans are reviewed annually to incorporate any updates based on best practices and regulatory changes. Training and Drills: Staff are regularly trained on fire safety and emergency procedures, and fire drills are conducted to ensure preparedness. These measures collectively ensure that Proxycare Personnel Ltd can maintain its operations and support its staff and clients effectively, even in the unfortunate event of a fire disrupting access to the buildings
3. Loss of Power	Power cuts.	Contact power supplier. Duty Manager has a mobile phone. In the event of a power loss lasting over 48 hours, Proxycare Personnel Ltd has established plans to ensure the continued operation of essential functions using laptops, mobile phones, and other necessary technology. Here are the key components of our power loss contingency plan: 1. Alternative Power Sources - Portable Generators: Maintain a portable generator for temporary power to critical devices and systems in the office. Ensure that staff trained in generator operation are available. - Uninterruptible Power Supply (UPS) Utilize UPS systems for laptops and critical devices to provide short-term backup power, allowing time for proper shutdown or transition to alternative power sources. 2. Remote Work Capabilities - Work-from-Home Policies: Encourage staff to work from home if the office is without power for an extended period. Ensure all staff have access to remote work capabilities and

necessary tools (e.g., VPN, cloud applications). - Mobile Hotspots: Ensure that staff have access to mobile hotspots or sufficient mobile data on company phones to facilitate remote work. 3. Device Management - Laptop and Mobile Phone Usage: Advise staff to utilize fully charged laptops and mobile phones to maintain communication and access to essential systems. - Charging Stations: Identify charging stations in the office or nearby facilities where staff can recharge devices if needed. 4. Communication Plan - Internal Communication: Utilize mobile phones and messaging apps to keep staff informed about the situation and any necessary actions. - External Communication: Maintain contact with service users, stakeholders, and partners to provide updates and coordinate service delivery. 5. Data Backup and Access - Cloud-Based Solutions: Ensure that critical data and applications are accessible via cloud-based solutions, allowing staff to continue working from any location with internet access. - Regular Backups: Ensure that all data is backed up regularly to prevent loss of important information during a power outage. 6. Staff Safety and Well-Being - Health and Safety Protocols: Ensure that staff are aware of safety procedures during extended power outages, including guidelines for using portable generators and maintaining a safe environment. - Support Services: Provide access to mental health support for staff affected by extended power outages, as they may experience stress or uncertainty. 7. Emergency Resources - Emergency Contact List: Maintain an updated list of emergency contacts, including utility providers, emergency services, and key personnel responsible for implementing the

		contingency plan. - Local Facilities: Identify local facilities (e.g., coworking spaces, libraries) that may have power and can accommodate staff during an outage. 8. Review and Training - Regular Drills and Training: Conduct regular training sessions and drills to familiarize staff with the power loss contingency plan and their roles in the event of an outage. - Plan Review: Regularly review and update the power loss contingency plan based on feedback from drills and real-life scenarios. By implementing these plans, Proxycare Personnel Ltd aims to minimize disruptions to operations and ensure the safety and well-being of our staff and service users in the event of a power loss lasting over 48 hours.
4. IT System Failures	System crash and lack of proper back-up facilities. Attack by hackers/viruses.	Paper back up would be used if required. All IT systems can be supported remotely. In the event of an IT system failure lasting over 48 hours, the organization should have contingency plans in place to ensure continued operations and minimize disruption. Here are some key strategies that could be implemented: Alternative Communication Methods: Staff should have access to alternative communication tools, such as mobile phones and messaging apps, to maintain contact with colleagues and clients. This ensures that critical information can still be shared even if the primary IT systems are down. Manual Operations: Key processes and functions should have manual alternatives that can be activated. This may include using paper-based forms for data collection and recording, ensuring that essential services can continue without digital systems. Access to Back-Up Devices: The organization should maintain a supply of laptops and mobile devices that are pre-

		configured for essential tasks. These devices should be regularly updated to ensure that staff can switch to them quickly when needed. Remote Access Solutions: If possible, staff should have the capability to access necessary files and applications remotely, through a secure virtual private network (VPN) or other secure means. This allows work to continue from alternative locations if office systems are down. Prioritization of Critical Services: Identify critical services and functions that must continue during an IT failure. Staff should be assigned specific responsibilities to ensure these services are prioritized and maintained throughout the outage. Regular Training and Drills: Conduct training sessions and drills to ensure that all staff members are familiar with the contingency plans and know how to respond in the event of an IT failure. By implementing these strategies, the organization can enhance its resilience to IT system failures and ensure that essential operations continue with minimal disruption. For more information on IT disaster recovery planning, you may refer to resources like TechTarget or NIST Guidelines.
5. Theft, Burglary or Vandalism	Theft of computer equipment, resulting in data loss. Vandalism to property resulting in interruptions to service provision.	Data is backed up. Police would be called for any vandalism and the building would be made secure by our own maintenance team or local contractors. In the event of equipment theft or vandalism resulting in a lack of necessary tools for over 48 hours, it's essential to have contingency plans in place to ensure that operations can continue smoothly. Here are some strategies to consider: Emergency Equipment Access: The organization should maintain a reserve of essential equipment, such as laptops and mobile devices, that

can be quickly deployed to staff members. These devices should be configured with the necessary software and access credentials to allow for seamless operation. Remote Work Capabilities: If equipment is stolen, staff should have the ability to work remotely using personal devices. Guidelines should be established to ensure secure access to company networks and data, such as using a Virtual Private Network (VPN) to protect sensitive information. Utilization of Mobile Phones: Encourage staff to use mobile phones for communication and accessing essential applications. Implementing mobile-friendly platforms can help maintain productivity, allowing staff to check emails, communicate with team members, and perform key tasks even without access to their usual equipment. Manual Operations: Establish procedures for manual operations in critical areas. This may include paper-based methods for record-keeping and communication, ensuring that core functions can still be carried out until the situation is resolved. Collaboration with Local Vendors: Develop relationships with local equipment rental or leasing companies. In the event of theft, these vendors can provide temporary replacements or backup equipment until the situation is stabilized. Incident Reporting and Insurance Claims: Ensure that there are clear procedures for reporting incidents of theft or vandalism. Quick reporting can facilitate insurance claims, which may help in the replacement of stolen equipment. Regular Training and Awareness: Conduct regular training sessions to ensure that all staff are aware of the contingency plans and know how to utilize alternative tools effectively. This preparation can significantly reduce downtime in case of equipment loss.

By implementing these strategies, an organization can mitigate the impact of equipment theft or vandalism and ensure continuity of operations. For further insights into disaster recovery and contingency planning, resources like the Federal Emergency Management Agency (FEMA) and National Institute of Standards and Technology (NIST) can be valuable references

When equipment is stolen or vandalized, it's crucial to have robust security measures in place to protect personal data in compliance with data protection laws and regulations. Here are several key strategies that can help secure personal data in such scenarios:

Data Encryption: Encrypting sensitive data ensures that, even if equipment is stolen, the information cannot be easily accessed without the appropriate decryption keys. Encryption should be applied both at rest (when stored) and in transit (when being transmitted over networks) to safeguard personal data effectively.

Access Controls: Implement strict access control measures to limit who can access sensitive information. This includes using strong, unique passwords, two-factor authentication (2FA), and role-based access controls to ensure that only authorized personnel have access to personal data.

Data Minimization: Collect and retain only the personal data necessary for business operations. This practice not only complies with data protection laws but also reduces the amount of sensitive information at risk if equipment is compromised.

Regular Backups: Regularly backing up data ensures that in the event of theft or loss, personal data can be restored from secure backup locations. These backups should also be encrypted and

stored separately from primary data to enhance security. Incident Response Plans: Establish and maintain an incident response plan that outlines procedures to follow in case of equipment theft or data breaches. This plan should include immediate steps for data protection, notification protocols for affected individuals, and reporting to relevant authorities as required by data protection laws. Physical Security Measures: Enhance physical security measures in the workplace to prevent theft or vandalism. This can include security cameras, alarms, secure storage areas for equipment, and visitor management protocols to limit unauthorized access to facilities. Training and Awareness: Provide regular training to employees about data protection policies, recognizing potential threats, and responding to security incidents. Awareness of data protection regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act, is essential for compliance and safeguarding personal data. Policy Review and Compliance: Regularly review and update data protection policies to ensure compliance with current laws and best practices. This includes assessing the effectiveness of security measures and making adjustments based on evolving threats. These measures align with data protection regulations and help to mitigate risks associated with the theft or vandalism of equipment. For more detailed guidance on securing personal data and compliance with data protection laws, you can refer to resources from the Information Commissioner's Office (ICO) or the European Data Protection Board (EDPB). ICO Data Security EDPB Guidelines

6. Restricted Access to Premises	Bomb scare, gas leak etc. resulting in evacuation.	All persons to be evacuated. In the event that the buildings are unavailable for more than 72 hours due to restricted access, such as a bomb scare or gas leak, it is crucial for an organization to have comprehensive contingency plans in place. Here are some potential strategies that could be implemented: Emergency Communication Plan: Establish a clear communication strategy to inform staff, clients, and stakeholders about the situation. This may include using multiple channels such as email, text messages, and social media updates to keep everyone informed about the status and any changes in procedures. Alternative Work Locations: Identify and prepare alternative locations where staff can continue their work if the primary premises are inaccessible. This may involve partnering with nearby organizations to use their facilities or having designated remote work capabilities in place. Remote Work Infrastructure: Ensure that employees have the necessary tools and access to work remotely. This includes secure access to company systems via Virtual Private Networks (VPNs), cloud storage solutions for data access, and communication tools to maintain collaboration. Essential Services Continuity: Identify critical functions that must continue during an emergency and allocate resources accordingly. This may include delegating essential tasks to specific team members who can operate remotely or from an alternative location. Data Backup and Recovery: Regularly back up data and maintain recovery protocols to ensure that information is safe and can be restored quickly if needed. This practice helps minimize downtime and data loss. Staff Support Services: Provide support
---	---	--

		services for employees affected by the incident, including counseling and assistance programs. This can help staff manage stress and maintain morale during difficult situations. Regular Drills and Training: Conduct regular emergency response drills to ensure staff are familiar with procedures in case of restricted access to the premises. This training helps to build confidence and efficiency in handling emergencies. Review and Update Policies: Continuously review and update the emergency response plans to adapt to changing circumstances, lessons learned from previous incidents, and feedback from staff. This ongoing assessment ensures that the organization remains prepared for potential emergencies. For further insights into emergency planning and response, organizations can refer to resources from agencies like the Federal Emergency Management Agency (FEMA) and local public safety departments: FEMA Emergency Planning Local Emergency Management
7. Crisis Affecting Suppliers	Key material supplies are interrupted through critical events at the suppliers.	Alternative purchases would be made. In the event of a crisis affecting your expected suppliers of personal protective equipment (PPE), it's essential to have alternative suppliers identified. Here are some potential alternatives you might consider: Online Retailers: Websites like Amazon Business and eBay can be useful for sourcing PPE quickly, especially during emergencies. They feature multiple sellers and a wide selection of products. Government and Nonprofit Resources: Some governmental and nonprofit organizations maintain lists of approved PPE suppliers. For example, the Federal Emergency Management Agency (FEMA) provides resources and guidance during crises. By

		diversifying your supplier options, you can help ensure a steady supply of PPE even in times of crisis. It's advisable to regularly review and update this list based on market conditions and supplier reliability.
8. Unsafe Structures	Any areas of the service deemed to be unsafe to use because of unsafe walls or ceilings etc.	Isolate using exclusion zones and/or barriers. Arrange repairs with local contractor. In the event that the buildings are deemed unsafe for more than 72 hours due to structural issues like unsafe walls or ceilings, the organization should have a well-defined contingency plan in place. Here are key elements to consider: Immediate Communication Protocols: Establish clear communication channels to notify employees, clients, and stakeholders about the situation. This may involve using emails, text alerts, or company intranet announcements to keep everyone informed. Alternative Work Arrangements: Identify temporary work locations such as nearby office spaces, coworking facilities, or enabling remote work options. Employees should be equipped with the necessary technology and access to perform their tasks from these alternative locations. Data Management and Security: Ensure that critical data is backed up and accessible. Utilize cloud storage solutions to allow remote access to important files and maintain data integrity during the transition. Safety Assessments and Remediation Plans: Engage structural engineers or safety professionals to assess the extent of the damage and outline necessary repairs. Establish a timeline for remediation and communicate updates regularly. Employee Support Services: Provide resources for employees affected by the situation, such as access to counseling services or employee

		assistance programs (EAPs), to help them cope with potential stress or anxiety. Training and Drills: Regularly conduct emergency drills to prepare staff for evacuations and relocations, ensuring they are familiar with the emergency protocols. Regular Review of Safety Policies: Continuously assess and update emergency response plans to reflect lessons learned from any incidents. This ensures that the plans remain effective and relevant. Legal and Insurance Considerations: Consult with legal and insurance advisors to understand the implications of building unavailability and ensure compliance with safety regulations and coverage for business interruptions. For more detailed guidelines on emergency preparedness and organizational response strategies, you can refer to the following resources: FEMA's Business Continuity Planning Suite: Offers comprehensive guidance on developing business continuity plans. FEMA Business Continuity Planning Occupational Safety and Health Administration (OSHA): Provides resources for emergency preparedness in workplaces. OSHA Emergency Preparedness Having a clear and well-communicated plan in place can significantly mitigate disruptions and ensure the safety and well-being of employees during such situations.
9. Loss of staff	Infection, illness, bad weather, resignations, etc and inability to replace staff quickly, either with temporary (Agency) staff, or with permanent staff.	Contact all available staff to ask for cover before contacting a local agency. Instigate Disruption of Service RAG response where staff shortages mean some service users cannot be covered. Inform Commissioner and CQC where there is a disruption to services.

Develop action plan with commissioner where services will be disrupted for extended period of time.

Arrange a recruitment drive.

Ensure Public Health England informed of any relevant infectious outbreak.

Business Failure Response

CRITICAL EVENT	DETAILS	CONTINGENCY/DISASTER RECOVERY PLAN (ACTION TO BE TAKEN)
1. Enforced Suspension or Closure of Business	Regulatory Enforcement Notices (e.g. Regulatory Authority, Environmental Health, Health & Safety Executive).	Inform and agree an action plan with commissioners, CQC and any other relevant agency (e.g. health commissioner) so people to be moved to other services are transferred in a controlled and safe manner. In the event of a crisis affecting your expected suppliers of personal protective equipment (PPE), it's essential to have alternative suppliers identified. Here are some potential alternatives you might consider: Online Retailers: Websites like Amazon Business and eBay can be useful for sourcing PPE quickly, especially during emergencies. They feature multiple sellers and a wide selection of products. Government and Nonprofit Resources: Some governmental and nonprofit organizations maintain lists of approved PPE suppliers. For example, the Federal Emergency Management Agency (FEMA) provides resources and guidance during crises. By diversifying your supplier options, you can help ensure a steady supply of PPE even in times of crisis. It's advisable to regularly review and update this list based on market conditions and supplier reliability.
2. Financial Problems	Cash-flow or solvency problems which could compromise on-going service delivery.	Develop an action plan with commissioners, contractors and CQC so financial support would be available.

If unable to resolve financial issues, agree and action plan with commissioners and private clients so people to be moved to other services are transferred in a controlled and safe manner.

In the event of equipment theft or vandalism resulting in a lack of necessary tools for over 48 hours, it's essential to have contingency plans in place to ensure that operations can continue smoothly. Here are some strategies to consider:

Emergency Equipment Access: The organization should maintain a reserve of essential equipment, such as laptops and mobile devices, that can be quickly deployed to staff members. These devices should be configured with the necessary software and access credentials to allow for seamless operation.

Remote Work Capabilities: If equipment is stolen, staff should have the ability to work remotely using personal devices. Guidelines should be established to ensure secure access to company networks and data, such as using a Virtual Private Network (VPN) to protect sensitive information.

Utilization of Mobile Phones: Encourage staff to use mobile phones for communication and accessing essential applications. Implementing mobile-friendly platforms can help maintain productivity, allowing staff to check emails, communicate with team members, and perform key tasks even without access to their usual equipment.

Manual Operations: Establish procedures for manual operations in critical areas. This may include paper-based methods for record-keeping and communication, ensuring that core functions can still be carried out until the situation is resolved.

Collaboration with Local Vendors: Develop relationships with local equipment rental or leasing companies. In the event of theft, these vendors can provide

temporary replacements or backup equipment until the situation is stabilized.

Incident Reporting and Insurance Claims: Ensure that there are clear procedures for reporting incidents of theft or vandalism. Quick reporting can facilitate insurance claims, which may help in the replacement of stolen equipment.

Regular Training and Awareness: Conduct regular training sessions to ensure that all staff are aware of the contingency plans and know how to utilize alternative tools effectively. This preparation can significantly reduce downtime in case of equipment loss. By implementing these strategies, an organization can mitigate the impact of equipment theft or vandalism and ensure continuity of operations.

For further insights into disaster recovery and contingency planning, resources like the Federal Emergency Management Agency (FEMA) and National Institute of Standards and Technology (NIST) can be valuable references