UT COMPLIANCE

A TRADING NAME OF UNIQUE TENDERS LIMITED

POLICY DOCUMENT

Business Continuity Policy

True Supported Living

SUPPORTED LIVING

DOCUMENT REFERENCE —	EFFECTIVE DATE 21 December 2025
VERSION SL/BCP/001	REVIEW DATE —
STATUS Publish	APPROVED BY Olakunle Agunbiade

CONFIDENTIAL DOCUMENT

This document is intended for authorised personnel only. Unauthorised distribution is prohibited.

1. Scope

1.1 Purpose

This Business Continuity Policy establishes the framework for ensuring True Supported Living can continue to provide safe, high-quality care and support to service users during disruptive incidents, emergencies, or significant operational challenges. The policy aims to:

Protect the health, safety, and wellbeing of service users, staff, and visitors during crisis situations; maintain essential care services with minimal disruption; ensure compliance with Care Quality Commission (CQC) fundamental standards and regulatory requirements; establish clear roles, responsibilities, and decision-making protocols for business continuity management; provide a structured approach to risk assessment, incident response, and recovery planning; and safeguard the organisation's reputation and operational viability.

1.2 Application

This policy applies to all staff employed by True Supported Living, including permanent, temporary, and agency workers; all service users receiving supported living services; contractors, volunteers, and visitors to our services; and all operational sites and locations managed by the organisation.

The policy is applicable during all phases of business continuity management: preparation and planning, incident response and activation, service continuity and recovery, and post-incident review and organisational learning.

1.3 Organisational Context

True Supported Living provides supported living services to adults with learning disabilities, autism, mental health needs, and physical disabilities across multiple locations. Our services support vulnerable individuals who rely on consistent, personalised care to maintain their independence, dignity, and quality of life. Any disruption to service delivery could have severe consequences for service user welfare, making robust business continuity planning essential.

1.4 Critical Services

The following services are designated as critical and must be maintained during any disruption: personal care and support; medication administration and healthcare coordination; safeguarding and safety monitoring; nutrition and meal provision; communication with service users, families, and external agencies; and maintenance of safe, habitable living environments.

1.5 Integration with Other Policies

This policy operates in conjunction with and supports the implementation of: Safeguarding Adults Policy; Health and Safety Policy; Fire Safety and Emergency Evacuation Policy; Infection Prevention and Control Policy; Risk Assessment and Management Policy; Incident and Accident Reporting Policy; Data Protection and Information Governance Policy; and Whistleblowing Policy.

1.6 Review and Updates

This policy will be reviewed annually or following any major incident, regulatory change, or significant organisational restructuring. All staff will be notified of updates, and training will be provided where changes affect operational procedures.

2. Legal and Regulatory Framework

True Supported Living operates within a comprehensive legal and regulatory framework that mandates business continuity planning and resilience. The following legislation and regulations establish our obligations:

Legislation/Regulation	Requirements
Health and Social Care Act 2008 (Regulated Activities) Regulations 2014	Regulation 12 requires providers to ensure service continuity, assess risks, and implement appropriate safety systems. Regulation 17 mandates good governance including business continuity planning and risk management systems.
Care Act 2014	Sections 48-57 establish duties for local authorities and care providers to ensure continuity of care, prevent service failure, and protect vulnerable adults during emergencies or provider business failure.
CQC Fundamental Standards	Requires providers to have robust business continuity plans covering staffing, premises, equipment failures, and external emergencies. Evidence of planning is assessed during CQC inspections under the 'Well-Led' key question.
Civil Contingencies Act 2004	Category 2 responder obligations to cooperate with emergency services and local resilience forums during civil emergencies, major incidents, and public health crises.
UK General Data Protection Regulation (UK GDPR) 2018	Article 32 requires appropriate technical and organisational measures including business continuity procedures to ensure ongoing confidentiality, integrity, and availability of personal data processing systems.
Health and Safety at Work etc. Act 1974	Section 2 requires employers to ensure health, safety and welfare of employees and service users, including during emergencies. Section 3 extends duty to others affected by work activities.
Management of Health and Safety at Work Regulations 1999	Regulation 3 requires risk assessments including emergency scenarios. Regulation 8 mandates appropriate emergency procedures, training, and testing for serious and imminent dangers.
Regulatory Reform (Fire Safety) Order 2005	Article 15 requires fire risk assessments and emergency plans. Articles 21-22 mandate maintenance of fire safety equipment and staff training in emergency procedures.
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)	Requires reporting of work-related deaths, specified injuries, occupational diseases, and dangerous occurrences. Business continuity plans must include RIDDOR reporting procedures.
Public Health (Control of Disease) Act 1984	Sections 45A-45T provide powers during public health emergencies including infectious disease outbreaks. Providers must cooperate with public health authorities and implement infection control measures.

Equality Act 2010	Section 149 (Public Sector Equality Duty) requires consideration of protected characteristics when planning emergency responses. Business continuity plans must address needs of disabled service users and staff.
Corporate Manslaughter and Corporate Homicide Act 2007	Organisations can be prosecuted if management failures causing death constitute gross breach of duty of care. Business continuity planning forms part of demonstrating appropriate management systems.

3. Definitions of Key Terms

Term	Definition
Business Continuity	The capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident. In care services, this means maintaining safe, quality care regardless of operational challenges.
Business Continuity Plan (BCP)	A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical functions at an acceptable predefined level.
Business Impact Analysis (BIA)	A systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency. Identifies time-critical functions and their recovery priorities.
Incident	Any event that disrupts, or could disrupt, normal service delivery. This includes internal failures (staffing, equipment, premises) and external threats (weather, utilities, public health emergencies).
Critical Function	An activity or process essential to service user safety and wellbeing that must continue during any disruption. For supported living, this includes personal care, medication administration, safeguarding, and basic nutrition.
Recovery Time Objective (RTO)	The target time set for resumption of critical functions following an incident. For care services, many critical functions have an RTO of zero (immediate continuation required).
Recovery Point Objective (RPO)	The point in time to which systems and data must be recovered after an incident. For care records and safeguarding information, RPO is typically minimal to prevent information loss.
Invocation	The formal activation of the Business Continuity Plan in response to an incident. Invocation triggers specific response procedures, roles, and communication protocols.
Resilience	The ability of an organisation to anticipate, prepare for, respond to, and adapt to incremental change and sudden disruptions in order to survive and prosper.
Major Incident	An event or situation with a range of serious consequences which requires special arrangements by one or more emergency services, the NHS, or a local authority. May affect multiple sites or large numbers of people.
Alternate Site	A location designated for use if primary service premises become unavailable. May include emergency accommodation, respite facilities, or arrangements with partner organisations.
Essential Supplies	Critical resources required for maintaining service delivery including medications, personal protective equipment (PPE), food, utilities (water, electricity, heating), and communication systems.

Mutual Aid Agreement	Formal arrangements between care providers to support each other during emergencies, including staff sharing, temporary accommodation, or resource provision.
Stand-Down	The formal deactivation of business continuity arrangements once normal operations have been restored and it is safe to resume standard procedures.
Pandemic	An epidemic of infectious disease that has spread across a large region affecting a substantial number of people. Requires specific infection control measures and continuity planning for prolonged staff absence.

4. Policy Statement

4.1 Commitment

True Supported Living is committed to ensuring business continuity and resilience in all circumstances. We recognise that service users depend on us for essential care and support, and that any disruption to service delivery could have serious consequences for their health, safety, and wellbeing.

We commit to maintaining comprehensive business continuity plans that are regularly tested, updated, and embedded in our organisational culture. Our approach prioritises service user safety above all else, ensures regulatory compliance, maintains staff competence in emergency response, and demonstrates transparent accountability to service users, families, commissioners, and regulators.

4.2 Core Principles

Service User-Centred Approach: All business continuity planning and incident response prioritises service user safety, dignity, and continuity of care. Service users and their representatives are informed and involved in emergency planning where appropriate.

Proportionate Response: We maintain flexible, scalable response procedures appropriate to incident severity, from minor operational disruptions to major emergencies affecting multiple sites or prolonged periods.

Continuous Improvement: Business continuity arrangements are subject to regular testing, review, and refinement based on lessons learned from exercises, actual incidents, and changes in service delivery or risk profile.

Collaborative Working: We work closely with local authorities, NHS partners, emergency services, other care providers, and Local Resilience Forums to ensure coordinated emergency response and mutual aid.

Transparency and Accountability: We maintain clear governance structures for business continuity management with defined roles, responsibilities, and decision-making authority. Incidents are reported appropriately to CQC, local authorities, and other stakeholders.

4.3 Risk Management Integration

Business continuity planning is integrated with our organisation-wide risk management framework. We conduct regular Business Impact Analyses to identify critical functions, assess vulnerabilities, and determine recovery priorities. Risk assessments specifically consider business continuity threats including staffing shortages, premises failures, utility disruptions, supply chain failures, cyber-attacks, public health emergencies, and extreme weather events.

4.4 Resource Allocation

True Supported Living allocates appropriate financial, human, and technological resources to business continuity management. This includes maintaining emergency supplies and equipment, funding staff training and exercises, investing in backup systems and communications, and maintaining insurance coverage appropriate to identified risks.

4.5 Staff Competence and Wellbeing

All staff receive appropriate training in business continuity procedures relevant to their role. We recognise that incidents can be stressful for staff and provide appropriate support including debriefing, supervision, and access to occupational health services. Staff wellbeing is monitored during prolonged incidents, with appropriate measures taken to prevent burnout and maintain operational capacity.

5. Roles and Responsibilities

Clear allocation of responsibilities is essential for effective business continuity management. The following roles carry specific accountabilities:

Role	Responsibilities
All Staff	Familiarise themselves with business continuity procedures relevant to their role; participate in training and exercises; report potential threats to service continuity promptly; follow instructions during incident response; maintain service user safety as the primary priority; document actions taken during incidents; and support colleagues and service users during stressful situations.
Registered Manager Anne Whiteley	Overall accountability for business continuity planning and implementation; approval of Business Continuity Plan and related procedures; authorisation of plan invocation and stand-down; strategic decision-making during major incidents; liaison with senior leadership, CQC, local authorities, and external agencies; resource allocation for business continuity management; oversight of training, exercising, and plan maintenance; appointment of business continuity coordination roles; review of incident reports and implementation of lessons learned; and ensuring business continuity arrangements meet regulatory requirements.
Duty Manager	Day-to-day operational leadership and frontline coordination during incidents; initial assessment of incident severity and immediate response requirements; coordination of staff deployment and emergency rotas; direct communication with service users, families, and frontline staff; activation of site-specific emergency procedures; liaison with emergency services and external responders; monitoring service delivery standards during disruption; escalation to Registered Manager when incident exceeds local response capacity; documentation of operational decisions and actions taken; supervision of staff wellbeing during prolonged incidents; and ensuring continuity of critical care functions at service delivery level.
Safeguarding Lead Anne Whiteley	Assessment of safeguarding implications during business continuity incidents; ensuring vulnerable adults remain protected throughout disruption; liaison with local authority safeguarding teams regarding incident impact; coordination of safeguarding referrals arising from incidents; monitoring for increased safeguarding risks during service disruption; ensuring compliance with safeguarding procedures during emergency response; and advising incident management team on safeguarding considerations in decision-making.

Health and Safety Officer `Eni Oladapo	Assessment of health and safety risks during incidents; ensuring safe working conditions for staff during emergency response; coordination of premises safety checks and emergency repairs; liaison with utilities providers, contractors, and facilities management; RIDDOR reporting for work-related injuries and dangerous occurrences; management of emergency evacuation procedures; monitoring compliance with fire safety and infection control during disruption; provision of personal protective equipment (PPE) and safety equipment; and advising incident management team on health and safety implications of response options.
Data Protection Officer Anne Whiteley	Protection of personal data during business continuity incidents; assessment of data security risks during disruption; coordination of data breach response procedures; ensuring access to critical service user records during system failures; oversight of backup and recovery procedures for electronic records; compliance with UK GDPR during emergency response; notification to Information Commissioner's Office (ICO) of data breaches; advising on lawful processing during emergency situations; and maintaining confidentiality when sharing information with external agencies.
Business Continuity Coordinator	Maintenance and regular review of Business Continuity Plan; coordination of business impact analyses and risk assessments; organisation of training programmes and exercises; maintenance of emergency contact lists and call-out procedures; management of business continuity documentation and resources; liaison with Local Resilience Forum and partner organisations; monitoring of emerging threats and updating of plans accordingly; coordination of plan testing and exercise programmes; collection and analysis of incident data for continuous improvement; and provision of business continuity advice and guidance to staff.
Communications Lead	Internal and external communications during incidents; preparation of staff briefings and service user notifications; liaison with families, advocates, and commissioners; coordination of media responses if required; maintenance of communication systems and alternative contact methods; ensuring accessible communication for service users with communication needs; documentation of communications sent and received; and management of social media and public-facing communications during incidents.
Finance Manager	Financial management during business continuity incidents; authorisation of emergency expenditure; maintenance of financial records and systems during disruption; liaison with insurance providers regarding incident claims; ensuring continued payroll processing; management of emergency procurement procedures; tracking of incident-related costs; and financial reporting to senior leadership and external stakeholders.
IT Manager	Maintenance of IT systems and infrastructure during incidents; implementation of data backup and recovery procedures; coordination of alternative working arrangements (remote access, etc.); management of cyber security during disruption; liaison with IT service providers and technology vendors; ensuring access to critical electronic care records; communication systems support including phones and internet; and restoration of IT services during recovery phase.

6. Procedures

6.1 Business Impact Analysis

The Business Continuity Coordinator conducts an annual Business Impact Analysis to identify critical functions, assess vulnerabilities, and determine recovery priorities. The process includes: identifying all service functions and activities; determining which functions are critical to service user safety and wellbeing; assessing the impact of disruption at different time intervals (1 hour, 4 hours, 24 hours, 1 week); identifying dependencies (staff, premises, equipment, utilities, supplies, IT systems); determining Recovery Time Objectives (RTO) for each critical function; and documenting resource requirements for maintaining critical functions.

Critical functions typically include: personal care and support delivery; medication administration and healthcare coordination; safeguarding monitoring and response; meal preparation and nutrition; safe, habitable accommodation; communication with

service users, families, and external agencies; and care record maintenance and information access.

6.2 Risk Assessment and Threat Identification

Business continuity risk assessments are conducted annually and reviewed following significant incidents or changes to service delivery. The assessment considers:

Staffing risks: sudden absence of key personnel, pandemic-related staff shortages, industrial action, recruitment difficulties, loss of specialist skills.

Premises risks: fire, flood, structural damage, gas leaks, heating system failure, water supply interruption, access denial.

Utility failures: electricity outages, water supply disruption, telecommunications failure, internet connectivity loss, heating/cooling system failure.

Supply chain disruption: medication shortages, food supply issues, PPE unavailability, equipment failure, supplier business failure.

External threats: severe weather events, public health emergencies (pandemic, outbreak), civil disturbances, transport disruption, local emergency incidents affecting service area.

Technology failures: IT system outages, cyber-attacks, data loss, electronic care record system failure, communication system breakdown.

Financial risks: sudden loss of income, unexpected major expenditure, insurance claim rejection, commissioner contract termination.

Each identified risk is assessed for likelihood and impact, with appropriate mitigation measures implemented. High-priority risks inform business continuity planning priorities.

6.3 Incident Response and Plan Activation

Incident Detection and Initial Response:

Any member of staff identifying a potential business continuity incident must immediately inform the Duty Manager. The Duty Manager conducts an initial assessment of the situation including nature and severity of incident, immediate threat to service user safety, number of service users and staff affected, availability of essential services and resources, and anticipated duration of disruption.

Based on initial assessment, incidents are categorised as: Level 1 (Minor) – localised incident managed through normal procedures with minor impact; Level 2 (Moderate) – significant disruption requiring coordination and possible external assistance; or Level 3 (Major) – severe incident threatening service delivery across multiple sites or prolonged period.

Plan Invocation:

Level 1 incidents are managed by the Duty Manager using standard operational procedures. Level 2 incidents trigger notification to the Registered Manager who determines whether to invoke formal business continuity procedures. Level 3 incidents automatically invoke the Business Continuity Plan.

Upon plan invocation, the following immediate actions are taken: establish incident command structure and activate designated roles; convene incident management team (Registered Manager, Duty Manager, relevant functional leads); ensure immediate safety of all service users and staff; implement emergency communication procedures; initiate incident log to document all

decisions and actions; activate alternative arrangements for critical functions as required; notify CQC, local authority, and other relevant external agencies; and brief all staff on incident status and their role in response.

6.4 Communication During Incidents

Effective communication is critical during business continuity incidents. The Communications Lead coordinates all internal and external communications.

Internal Communications: All staff are briefed on incident status, their specific responsibilities, and any changes to normal procedures. Regular updates are provided at intervals appropriate to incident severity. Communication methods include staff meetings, email, text messages, phone calls, and notice boards. Staff working remotely or off-site receive equivalent information in accessible formats.

Service User Communications: Service users are informed of incidents in accessible, age-appropriate language. Communication considers individual needs including learning disabilities, sensory impairments, and language requirements. Service users are reassured about their safety and the steps being taken to maintain their care. Where appropriate, service users are involved in decision-making about their care during the incident.

Family and Representative Communications: Families, advocates, and representatives are notified promptly of any incident affecting their relative's care. Communication includes incident nature, impact on the individual, actions being taken, and expected timeline. Contact details and communication preferences from care plans are used. Regular updates are provided, with families encouraged to contact the organisation with concerns or questions.

External Stakeholder Communications: The Registered Manager or designated senior staff notify CQC using the statutory notification process for relevant incidents. Local authority commissioning and safeguarding teams are informed as appropriate. Emergency services, NHS partners, and other external agencies receive necessary information to coordinate response. Professional advisors (insurance, legal, HR) are contacted as required.

6.5 Staffing Arrangements During Disruption

Maintaining adequate staffing is often the most critical challenge during business continuity incidents. The following procedures apply:

Staff Recall and Deployment: The Duty Manager maintains an updated staff contact list including emergency contact details. During incidents, off-duty staff may be recalled using telephone cascade procedures. Staff are deployed flexibly across sites and roles based on competence and service user needs. Enhanced rates of pay or time off in lieu may be offered to incentivise availability during prolonged incidents.

Alternative Staffing Resources: Bank and agency staff are contacted to fill gaps in rotas. Mutual aid agreements with partner care providers may be activated to share staff resources. Senior management and administrative staff with current care qualifications may work clinical shifts if required. Volunteers and family members cannot replace regulated care staff but may support with non-care tasks.

Skill Mix and Competence: Safe minimum staffing levels for each service are determined based on service user acuity and needs. Skill mix is maintained to ensure qualified staff supervise support workers. Inexperienced staff are paired with experienced colleagues. Only competent, trained staff administer medications or provide specialist care interventions.

Staff Welfare During Prolonged Incidents: Maximum working hours are monitored to prevent fatigue. Rest breaks and meal breaks are protected. Accommodation may be arranged for staff unable to travel home during severe weather or transport disruption. Support and supervision are provided to staff experiencing stress or emotional impact. Debriefing and counselling services are accessible for staff affected by traumatic incidents.

6.6 Premises and Accommodation Management

When service premises become unavailable or unsafe, the following procedures are implemented:

Immediate Safety Response: If premises present immediate danger (fire, gas leak, structural damage), emergency evacuation procedures are activated immediately. Emergency services are contacted as appropriate. Service users are evacuated to designated assembly points and safety is confirmed. Staff account for all service users and colleagues.

Alternative Accommodation Assessment: The Health and Safety Officer assesses whether premises can be made safe through emergency repairs or temporary measures. If premises cannot be occupied, alternative accommodation options are evaluated including vacant properties within the organisation, partner provider facilities, hotel or temporary housing, respite services, and family home placement (with service user and family consent).

Service User Placement: Service users are placed in alternative accommodation that meets their assessed needs and maintains their dignity and wellbeing. Individual care plans are followed in the new setting. Personal belongings, medications, and care documentation accompany service users. Families and commissioners are informed of placement arrangements.

Premises Recovery: Once premises are deemed safe, thorough inspection is conducted before service users return. Essential services (utilities, safety systems) are tested and confirmed operational. Deep cleaning and infection control measures are implemented if required. Service users return in planned, managed manner with appropriate support.

6.7 Utility and Essential Services Management

Utility Failure Response:

Electricity Outage: Backup lighting systems are activated. Temperature control is monitored, particularly for medication storage. Alternative heating and cooking arrangements are implemented. Essential medical equipment is transferred to generator power or battery backup. Utility provider is contacted for estimated restoration time.

Water Supply Interruption: Bottled water stocks are accessed for drinking, medication preparation, and handwashing. Alternative arrangements for bathing and personal care are implemented. Toilet facilities are managed using stored water if possible. Public health advice is followed regarding water use once supply is restored.

Heating System Failure: Additional blankets and warm clothing are provided to service users. Alternative heating sources (fan heaters, etc.) are used safely. Room temperatures are monitored, particularly in bedrooms and care areas. Vulnerable service users are prioritised for warmest areas or alternative accommodation if necessary.

Gas Supply Disruption: Emergency gas shut-off procedures are followed if leak suspected. Alternative cooking arrangements are implemented using electric equipment or external catering. Hot water supply is maintained through alternative means.

Telecommunications Failure: Mobile phones are used as backup communication method. Service users and families are informed of temporary contact number. Priority calls (emergency services, safeguarding, medication queries) are identified. Internet-dependent systems (care records, monitoring) are accessed via mobile data or alternative location.

6.8 Medication Management During Disruption

Medication administration must continue without interruption during business continuity incidents. Procedures include: maintaining minimum 7-day stock of all prescribed medications in secure storage; emergency prescription arrangements with pharmacies and GP practices; cold chain management using cool bags with ice packs if refrigeration fails; medication transfer protocols if service users are relocated; paper-based medication administration recording if electronic systems fail; 24-hour access to pharmacy advice and emergency medicine supply; and clear protocols for managing missed doses or administration

errors during disruption.

6.9 Supply Chain and Resource Management

Essential supplies are maintained at levels sufficient for 72-hour self-sufficiency including: food and beverages for all meals and snacks; personal protective equipment (gloves, aprons, masks); continence products and personal care supplies; cleaning and disinfection materials; first aid equipment and basic medical supplies; batteries, torches, and emergency lighting; blankets and emergency heating equipment; and bottled water.

Alternative suppliers are identified for critical items with mutual aid agreements in place where appropriate. Emergency procurement procedures allow rapid sourcing of supplies outside normal ordering processes. Stock levels are checked regularly and replenished promptly.

6.10 Information and Data Management

Access to service user care records is essential during any incident. The following arrangements ensure information availability: electronic care records are backed up daily to secure cloud storage; paper copies of critical information (personal emergency evacuation plans, medication records, emergency contacts) are stored in grab bags; mobile access to electronic systems via smartphone/tablet for staff working off-site; emergency contact lists for staff, service users, families, and external agencies are maintained in multiple formats; and data protection principles are maintained throughout, with personal information only shared on need-to-know basis.

6.11 Service User Evacuation and Relocation

If service users must be evacuated or relocated, the following procedures apply: Personal Emergency Evacuation Plans (PEEPs) for each service user are followed; grab bags containing essential items (medications, care documentation, personal items) are prepared and kept accessible; service users requiring additional support during evacuation are identified and prioritised; accessible transport is arranged considering mobility needs and anxiety; service users are accompanied by familiar staff where possible to reduce distress; destination accommodation is prepared in advance with necessary equipment and supplies; care plans and risk assessments are updated to reflect temporary placement; and family members and advocates are informed promptly with details of new location and contact arrangements.

6.12 Financial Management During Incidents

Business continuity incidents often incur unexpected costs. The Finance Manager maintains emergency expenditure authorisation procedures and tracks all incident-related costs for insurance claims or commissioner reimbursement. Petty cash float is available for immediate purchases. Corporate credit cards enable rapid procurement. Emergency contractors and suppliers can be engaged outside normal procurement processes when service user safety requires. All expenditure is documented with clear justification.

6.13 Recovery and Return to Normal Operations

Recovery planning begins as soon as the immediate emergency response is stabilised. The Registered Manager assesses: when normal operations can safely resume; what infrastructure or resource restoration is required; whether temporary arrangements can be safely withdrawn; if any permanent changes to service delivery are needed; and what support staff and service users require during transition back to normal.

Stand-down procedures include: formal notification to all stakeholders that business continuity arrangements are deactivated; restoration of normal rotas, procedures, and systems; debriefing sessions for staff involved in incident response; thank you recognition for staff who went above and beyond; welfare checks on service users affected by the incident; review of any temporary safeguarding measures implemented; and update of care plans if service user needs have changed.

The incident management team conducts a post-incident review within 2 weeks of stand-down, examining what happened, what worked well, what could be improved, whether plans and procedures were adequate, training or resource needs identified, and changes needed to prevent similar incidents. Findings and recommendations are documented and implemented.

7. Training and Development

7.1 Training Requirements

All staff receive business continuity training appropriate to their role. Training is provided during induction and refreshed annually.

Induction Training: All new staff receive overview of business continuity policy and procedures; location and content of Business Continuity Plan; their role and responsibilities during incidents; emergency contact procedures and escalation pathways; location of emergency equipment and supplies; and specific procedures for the service where they will work (fire evacuation, utility failure response, etc.).

Role-Specific Training: Managers and senior staff receive enhanced training in incident command, decision-making under pressure, multi-agency coordination, and communication with external stakeholders. Duty Managers receive specific training in initial incident assessment, activation procedures, and operational coordination. Specialist roles (Health and Safety Officer, Data Protection Officer, Safeguarding Lead) receive training relevant to their business continuity responsibilities.

Scenario-Based Training: Staff participate in scenario-based exercises at least annually to practice emergency procedures. Scenarios reflect identified risks (severe weather, pandemic, utilities failure, etc.) and allow staff to rehearse their response in safe environment. Exercises are debriefed to identify learning points and areas for improvement.

7.2 Competency Assessment

Competence in business continuity procedures is assessed through: knowledge checks during supervision; observation during exercises and drills; performance review during actual incidents; and feedback from colleagues and incident management team. Staff requiring additional support are identified and receive further training or mentoring. Competency in emergency procedures is considered essential for all care staff and forms part of capability assessment.

7.3 Continuous Learning and Development

Learning from incidents and exercises is systematically captured and shared. Post-incident reviews identify training needs which inform future training programmes. Examples from actual incidents (anonymised where appropriate) are used in training to make learning relevant and practical. Staff are encouraged to identify business continuity risks and suggest improvements to plans and procedures. Lessons learned from other organisations, national incident reviews, and sector guidance are incorporated into training and plan updates.

7.4 Training Records and Compliance

Training attendance is recorded and monitored. Compliance rates are reported to senior management and form part of CQC evidence. Training refresher dates are tracked and staff reminded when updates are due. Training effectiveness is evaluated through participant feedback, competency assessment, and performance during exercises and actual incidents.

8. Monitoring and Review

8.1 Plan Testing and Exercising

The Business Continuity Plan is tested through regular exercises to ensure it remains effective and staff are familiar with procedures. Testing programme includes:

Desktop Exercises (annually): Tabletop scenarios discussed by management team to test decision-making processes, coordination, and plan adequacy without disrupting service delivery. Identify gaps or weaknesses requiring plan updates.

Communication Exercises (bi-annually): Test staff call-out procedures, emergency contact lists, and communication cascades. Verify contact details are current and staff respond appropriately to alerts.

Functional Exercises (annually): Test specific elements of the plan such as evacuation procedures, utility failure response, or IT system recovery. Involve relevant staff in realistic scenarios requiring practical implementation of procedures.

Full-Scale Exercises (every 3 years): Comprehensive test involving all aspects of business continuity response, multiple teams, and potentially external partners. As close to real incident as possible without compromising service user safety or wellbeing.

All exercises are formally evaluated with lessons learned documented and actions implemented. Exercise reports are shared with senior leadership and inform plan updates.

8.2 Performance Monitoring

Business continuity performance is monitored through key indicators including: frequency and severity of business continuity incidents; time to invoke Business Continuity Plan when required; time to restore normal operations (recovery time); impact on service users (safeguarding incidents, complaints, service disruption); staff competency levels (training compliance, exercise performance); plan testing frequency and outcomes; and implementation rate of post-incident recommendations.

8.3 Policy and Plan Review

This policy is reviewed annually as minimum, or sooner if: major incident occurs requiring plan invocation; significant changes to service delivery, staffing structure, or premises; changes to regulatory requirements or statutory guidance; recommendations from CQC inspection or external audit; lessons learned from exercises or actual incidents; or changes to risk profile or identification of new threats.

Business Continuity Plan documents are reviewed and updated at least every 6 months. Review process includes: verification that contact details and emergency procedures are current; assessment of whether identified risks and scenarios remain relevant; review of resource requirements and availability; checking that roles and responsibilities reflect current staffing; incorporating lessons learned from incidents and exercises; and aligning with updated legislation, regulations, and best practice guidance.

8.4 Quality Assurance

Business continuity arrangements are subject to internal audit and quality assurance processes. Audits assess: completeness and currency of Business Continuity Plan documentation; staff awareness and understanding of procedures; availability and condition of emergency equipment and supplies; adequacy of training and exercising programmes; compliance with regulatory requirements; and effectiveness of previous incident responses and recovery.

Audit findings and recommendations are reported to senior management with action plans developed to address identified gaps or weaknesses. Progress against action plans is monitored through governance structures.

8.5 Continuous Improvement

Business continuity management is subject to continuous improvement methodology. Improvement opportunities are identified through: post-incident reviews and lessons learned; exercise debriefings and evaluations; staff suggestions and feedback; benchmarking against other organisations; sector guidance and best practice updates; and regulatory feedback from CQC inspections. Improvement actions are prioritised, resourced, and implemented with progress tracked through governance structures.

9. Reporting Concerns

9.1 Staff Duty to Report

All staff have a duty to report potential business continuity threats, near-miss incidents, or concerns about the adequacy of emergency preparedness. This includes: identification of new risks or changes to existing risks; equipment failures or resource shortages that could affect service continuity; staffing concerns that may impact emergency response capability; premises safety issues or utility system problems; concerns about plan adequacy or effectiveness; and suggestions for improving business continuity arrangements.

Staff should not wait for certainty before raising concerns. Early reporting allows preventive action to be taken and potentially avoids incidents occurring.

9.2 Reporting Channels

Staff can report business continuity concerns through: immediate verbal report to Duty Manager or line manager for urgent issues; incident reporting system for near-misses or minor incidents; direct contact with Business Continuity Coordinator for plan-related feedback; health and safety reporting procedures for premises or equipment issues; supervision sessions for non-urgent concerns or suggestions; and anonymous reporting via whistleblowing procedures if staff are concerned about reprisals.

9.3 Response to Reports

All reports are taken seriously and investigated appropriately. The recipient of a report acknowledges receipt within 24 hours and provides feedback on action taken within 5 working days. Where immediate action is required, this is taken without delay and the reporting staff member is informed. Staff are thanked for reporting concerns and encouraged to continue being vigilant.

9.4 Whistleblowing Protection

Staff who raise genuine concerns about business continuity, safety, or regulatory compliance are protected from detriment or victimisation under the organisation's Whistleblowing Policy and Public Interest Disclosure Act 1998. No member of staff will face disciplinary action or unfair treatment for raising legitimate concerns in good faith, even if those concerns prove to be unfounded. Allegations of victimisation or retaliation against whistleblowers are investigated thoroughly and addressed seriously.

9.5 Investigation Procedures

Significant concerns or near-miss incidents are investigated using root cause analysis methodology to identify underlying causes and systemic issues. Investigations focus on learning and improvement rather than blame. Staff involved in incidents are supported and treated fairly. Investigation findings inform plan updates, training programmes, and risk management strategies. Where individual performance issues are identified, these are addressed through supervision and capability procedures separate from the learning process.

10. Business Continuity Scenarios

The following table outlines specific business continuity scenarios, their potential impacts, and response procedures. These scenarios inform our planning, training, and exercising activities.

Scenario	Potential Impact	Response Procedures	Recovery Time
COVID-19 or Pandemic Outbreak	High staff absence (30-50%), inability to maintain rotas; service user illness requiring enhanced care; infection control requirements affecting normal routines; visitor restrictions impacting service user wellbeing; supply shortages (PPE, cleaning materials); potential service closure if outbreak severe.	Implement infection prevention and control measures per government/Public Health England guidance; cohort affected service users; enhance cleaning and hygiene protocols; daily symptom monitoring of staff and service users; activate mutual aid agreements for staff sharing; utilise bank/agency staff; redeploy management to care duties; provide remote support via video calls where appropriate; maintain communication with families; coordinate with local health protection teams; ensure adequate PPE stocks; support staff and service user mental health.	2-6 weeks for outbreak control; 3-12 months for service normalisation
Severe Weather: Heavy Snow/Ice	Staff unable to travel to work; service users unable to access community activities; increased risk of falls on icy surfaces; heating system strain or failure; delayed deliveries (food, medications, supplies); potential isolation if roads impassable.	Monitor weather forecasts and pre-position staff overnight if severe weather predicted; arrange 4×4 transport for staff where possible; stock additional food, medications, and essential supplies in advance; suspend non-essential community activities; grit pathways and building entrances; check heating systems and have backup heaters ready; arrange alternative accommodation for stranded staff; maintain regular welfare checks on service users; coordinate with local authority emergency services for priority gritting; increase frequency of safety checks.	1-5 days depending on severity and thaw

Severe Weather: Flooding	Premises damage and uninhabitability; loss of utilities (electricity, water, heating); contamination of ground floor areas; damage to equipment, furnishings, records; displacement of service users; road access prevented; potential sewage contamination.	Activate flood emergency plan if flood warnings issued; move vulnerable service users and essential items to upper floors if safe; evacuate if directed by emergency services or if premises unsafe; activate alternative accommodation arrangements; contact insurance provider immediately; coordinate with emergency services and local authority; arrange emergency pumping and cleaning services; conduct safety assessment before re-entry; implement deep cleaning and decontamination; replace damaged equipment and furnishings; update care plans for temporarily relocated service users; provide emotional support for distressed service users.	1-3 days for evacuation; 2-8 weeks for premises restoration
Severe Weather: Extreme Heat	Increased risk for vulnerable service users (dehydration, heat exhaustion, heatstroke); staff fatigue and reduced capacity; air conditioning failure or absence; medication storage concerns if temperatures exceed limits; increased agitation or behavioural changes; power outages from grid strain.	Implement heatwave plan following Public Health England guidance; increase fluid intake monitoring; close curtains/blinds during hottest periods; use fans and cool rooms; monitor room temperatures regularly; check vulnerable individuals frequently for signs of heat stress; adjust activity schedules to cooler times; provide cool showers/baths; ensure adequate staff breaks in cool areas; move temperature-sensitive medications to coolest storage; activate emergency cold chain procedures if needed; reduce non-essential physical activities; provide light, frequent meals.	Duration of heatwave (typically 2-7 days)
Fire	Immediate threat to life; potential injuries or fatalities; property destruction; smoke and water damage; displacement from premises; loss of possessions and records; psychological trauma; regulatory scrutiny and potential enforcement.	Activate fire evacuation procedures immediately; call 999; evacuate all persons to assembly point via nearest safe exit; account for all service users and staff; administer first aid if required; do not re-enter building; cooperate fully with fire service; arrange immediate alternative accommodation; contact families and local authority; secure site once fire service confirms safe; conduct welfare checks on all involved; arrange counselling support; preserve evidence for investigation; notify CQC and insurers; coordinate with fire investigation; implement lessons learned; review and update fire safety measures.	Immediate evacuation; 1-6 months for premises repair depending on damage severity
Gas Leak	Explosion risk; poisoning/asphyxiation risk; need for emergency evacuation; loss of heating and cooking facilities; premises closure until certified safe.	If gas smell detected: no electrical switches or flames; open windows and doors; evacuate building immediately; call gas emergency number (0800 111 999) from outside; call 999 if anyone symptomatic; account for all persons; do not re-enter until certified safe by gas engineer; arrange alternative accommodation if evacuation prolonged; arrange alternative cooking facilities; notify utility provider; have heating system inspected before resuming use.	2-24 hours for emergency response and safety certification

Electricity Outage	Loss of lighting, heating, refrigeration; inability to prepare hot food; electronic care record system unavailable; medication refrigeration failure; loss of assistive technology; communication system failure; security system failure.	Activate backup lighting systems; notify utility provider and obtain estimated restoration time; implement emergency lighting procedures; move to manual recording systems; monitor medication storage temperatures (discard if exceeded); use mobile phones for communication; prepare cold meals or use alternative cooking methods; prioritise vulnerable service users for warmth; consider relocation if outage prolonged (>6 hours in winter); maintain security presence; contact emergency services if medical equipment affected; document all actions taken.	1-24 hours depending on cause and utility response
Water Supply Failure	No drinking water, handwashing, or toilet facilities; inability to prepare food or medications; infection control compromised; dignity and hygiene affected; potential dehydration.	Notify water company and ascertain cause and duration; access emergency bottled water stocks; arrange additional water delivery if needed; implement strict water rationing for essential use only; use bottled water for drinking, medications, and handwashing; suspend bathing unless alternative water available; use sanitary facilities sparingly; consider relocation if outage prolonged (>6 hours); maintain high standards of hand hygiene using alcohol gel; serve pre-packaged foods if possible; monitor service users for signs of dehydration.	2-12 hours for supply restoration
IT System Failure/Cyber Attack	Loss of electronic care records; inability to access care plans, risk assessments; medication administration record unavailable; safeguarding information inaccessible; communication systems down; data breach risk; potential ransomware demands.	Immediately disconnect affected systems to prevent spread; contact IT support/provider; notify Data Protection Officer; implement paper-based recording systems; access backup/printed copies of critical information (care plans, medication records, emergency contacts); maintain service user safety using available information; do not pay ransomware demands; preserve evidence for investigation; notify ICO if personal data breach; inform affected service users/families if appropriate; engage cyber security specialists; restore from clean backups once threat neutralised; review and strengthen IT security measures.	4-72 hours for system restoration; longer if major attack
Mass Staff Absence (Non-Pandemic)	Inability to maintain safe staffing levels; cancellation of activities and appointments; increased pressure on available staff; potential inability to deliver personal care; risk of service user neglect.	Activate staff recall procedures; utilise bank and agency staff; request staff cancel annual leave; offer enhanced pay rates/incentives for extra shifts; activate mutual aid agreements with partner providers; redeploy management and administrative staff to care duties; prioritise critical care tasks (medication, personal care, safety checks); suspend non-essential activities; communicate with families about reduced services; notify commissioners and CQC if sustained shortage; consider temporary service capacity reduction; ensure remaining staff receive adequate breaks and support.	3-14 days depending on absence cause

Sudden Death of Service User	Trauma for co-residents and staff; police investigation if unexpected; media attention if suspicious; regulatory scrutiny; family distress; reputational impact; staff emotional impact.	Call 999 if death unexpected; preserve scene if death suspicious; notify police, senior management, CQC; provide immediate support to service users who witnessed/discovered; contact family with sensitivity; cooperate fully with police and coroner; notify GP and healthcare professionals; complete safeguarding referral if concerns exist; submit statutory notifications; arrange counselling for affected staff and service users; conduct internal review; hold memorial/remembrance if appropriate; review and learn from incident; support deceased's family with practical arrangements.	Immediate response; 1-6 months for investigations and emotional recovery
Serious Safeguarding Incident	Immediate risk to service user; potential police investigation; suspension of staff; regulatory investigation and enforcement; media scrutiny; commissioner contract review; reputational damage; service closure risk.	Ensure immediate safety of service user; make safeguarding referral to local authority immediately; contact police if criminal offence suspected; preserve evidence; suspend implicated staff pending investigation; increase monitoring and supervision of affected service user; notify CQC via statutory notification; engage fully with safeguarding investigation; implement interim safety measures; review all relevant policies and procedures; provide support to whistleblower and witnesses; take appropriate disciplinary action; implement improvements identified; maintain transparent communication with commissioners; consider independent safeguarding review.	Immediate safety response; 1-6 months for investigations
Major Supplier Failure	Loss of essential services (food, laundry, pharmacy, equipment); inability to maintain service standards; urgent need for alternative arrangements; potential additional costs; service user disruption.	Identify nature and duration of supplier failure; activate alternative supplier arrangements from contingency list; emergency procurement procedures to source replacement rapidly; utilise emergency stock while new arrangements established; notify commissioners if costs significantly affected; communicate with service users about temporary changes; monitor quality of alternative suppliers; if pharmacy failure, coordinate emergency prescription services; if food supplier failure, use local shops or catering services; review supplier dependencies and diversify to reduce single points of failure.	1-7 days to establish alternative arrangements

Loss of Key Personnel	Loss of expertise and organisational knowledge; decision-making gaps; impact on service quality and consistency; staff morale affected; increased workload on remaining staff; regulatory concern if Registered Manager.	If Registered Manager: notify CQC and appoint interim manager immediately; if specialist role: redistribute responsibilities among existing staff; accelerate recruitment process; utilise interim/consultant support if needed; conduct knowledge transfer from departing staff if possible; access retained knowledge (policies, procedures, documentation); increase supervision and support for staff taking on additional responsibilities; notify relevant external stakeholders; maintain service continuity and standards; develop succession planning to prevent future gaps.	1-3 months for interim arrangements; 3-6 months for permanent replacement

11. Related Policies

This Business Continuity Policy should be read in conjunction with the following organisational policies:

Safeguarding Adults Policy; Health and Safety Policy; Fire Safety and Emergency Evacuation Policy; Infection Prevention and Control Policy; Risk Assessment and Management Policy; Incident and Accident Reporting Policy; Data Protection and Information Governance Policy; Whistleblowing Policy; Business Continuity Plan (operational document); Personal Emergency Evacuation Plans (PEEPs); Major Incident Plan; Pandemic Response Plan; Severe Weather Procedures; and Emergency Communication Procedures.

12. Approval and Review

Policy Approval:

Policy Owner: Anne Whiteley, Registered Manager

Approved by: Senior Management Team

Date of Approval: [To be completed upon approval]

Effective Date: [To be completed upon approval]

Review Schedule:

This policy will be reviewed annually as minimum, or sooner if required by regulatory changes, major incidents, or organisational restructuring.

Next Review Date: [12 months from approval date]

Document Control:

Version: 1.0

Document Location: Quality Management System / Policy Library

Accessibility: Available to all staff via company intranet, hard copies in each service location

13. Commissioner Assurance and Provider Failure Protocols

This section provides commissioners, local authorities, and external stakeholders with assurance regarding True Supported Living's organisational resilience, financial sustainability, and arrangements to ensure continuity of care in all circumstances including potential provider failure. These provisions comply with Care Act 2014 Section 48 duties and demonstrate our commitment to transparent partnership working.

13.1 Financial Resilience and Sustainability

True Supported Living maintains robust financial controls and reserves to ensure organisational sustainability and the ability to respond to business continuity incidents without compromising service delivery.

Financial Reserves:

The organisation maintains financial reserves equivalent to minimum 3 months' operating costs to provide working capital during disruptions, cover emergency expenditure without cash flow strain, and ensure payroll continuity if income temporarily affected. Reserve levels are monitored monthly by the Finance Manager and reported to the Board/Senior Management Team quarterly. Any draw-down on reserves is subject to formal approval and requires a replenishment plan.

Insurance Coverage:

Comprehensive insurance coverage includes: employers' liability insurance (£#xA3;10 million minimum); public liability insurance (£#xA3;5 million minimum); professional indemnity insurance (£#xA3;5 million minimum); property and contents insurance including business interruption cover; cyber liability insurance covering data breaches and system recovery; and key person insurance for critical management roles.

Business interruption insurance provides coverage for loss of income during service disruption caused by insurable events (fire, flood, etc.) with indemnity period of 12 months minimum. All insurance policies are reviewed annually and certificates provided to commissioners upon request.

Cash Flow Management:

Monthly cash flow forecasting identifies potential shortfalls minimum 3 months in advance. Contingency funding arrangements include access to emergency credit facilities, relationships with multiple banking providers, and ability to accelerate commissioner invoicing if required. We maintain 30-day payment terms with suppliers while monitoring debtor days to protect cash position.

Financial Stress Indicators:

We monitor key financial indicators that could signal organisational distress: reserves falling below 2 months' operating costs; consistent failure to pay suppliers within terms; difficulty meeting payroll; breach of banking covenants; or loss of major contracts without replacement revenue. Any indicator triggering would prompt immediate notification to commissioners and implementation of recovery plans.

13.2 Commissioner Notification and Escalation Matrix

Clear notification protocols ensure commissioners are informed appropriately based on incident severity and potential impact on commissioned services. The following matrix defines notification requirements:

Immediate Notification (within 1 hour):

Death of service user (unexpected); serious safeguarding incident requiring police involvement; fire, flood, or major premises incident requiring evacuation; complete loss of utilities expected to exceed 24 hours; major IT system failure affecting care delivery or data security; outbreak of notifiable infectious disease; incident involving multiple casualties; regulatory enforcement action by CQC; and media enquiries about service delivery or incidents.

Same Day Notification (within 8 working hours):

Staffing shortage requiring service capacity reduction; partial premises closure affecting service user accommodation; utility disruption between 6-24 hours; significant supplier failure affecting service delivery; Business Continuity Plan formal invocation; serious injury to service user or staff member; safeguarding concern referred to local authority; and planned relocation of service users due to premises issues.

5 Working Day Notification:

Registered Manager resignation or absence exceeding 28 days; financial difficulties or contract losses affecting sustainability; changes to service registration or conditions; planned service reconfiguration or closure; significant quality concerns identified through audit; persistent recruitment challenges affecting service model; and insurance claim exceeding £#xA3;50,000.

Regular Reporting (monthly/quarterly as per contract):

Summary of business continuity incidents and response; staff vacancy and turnover rates; safeguarding activity; complaints and compliments; quality assurance outcomes; and financial performance against budget.

Notification Method and Content:

All commissioner notifications include: date, time, and nature of incident; number of service users affected; immediate actions taken to ensure safety; anticipated duration and impact on service delivery; support required from commissioners (if any); named contact person for further information; and follow-up reporting schedule. Notifications are made via telephone for immediate/same-day incidents (followed by written confirmation) and via email for non-urgent notifications.

13.3 Provider Failure Contingency (Care Act Section 48 Compliance)

In the unlikely event that True Supported Living faces potential business failure, the following protocols ensure orderly service transition and protection of service user welfare in compliance with Care Act 2014 duties.

Early Warning Indicators:

We will notify commissioners immediately if any of the following circumstances arise: inability to meet payroll within 7 days; reserves depleted below 1 month’s operating costs; formal insolvency or administration proceedings commenced; loss of insurance coverage; CQC enforcement action restricting admissions or requiring service closure; loss of multiple contracts creating unsustainable financial position; or Registered Manager resignation with no succession plan.

Service User Placement Plan:

In event of provider failure, we maintain current information on alternative providers who could accommodate our service users including provider contact details, specialisms, and current vacancy position. We will work with commissioners and local authority safeguarding teams to: assess each service user’s needs and suitable alternative placements; prioritise placements based on vulnerability and risk; facilitate visits and transitions to new providers; transfer all care documentation, risk assessments, and personal records; ensure medication continuity and healthcare handovers; support families through the transition process; and maintain dignity and choice for service users throughout.

Staff TUPE Arrangements:

Staff directly employed in service delivery would transfer to the new provider under TUPE regulations (Transfer of Undertakings Protection of Employment 2006). We will: maintain accurate staff records including terms and conditions; cooperate fully with TUPE information and consultation requirements; facilitate staff meetings with incoming provider; ensure pension and benefits continuity; and support staff through the transfer process. Where TUPE does not apply, we will provide references and support staff to secure alternative employment.

Orderly Wind-Down Procedures:

If business failure is unavoidable, we commit to: providing minimum 90 days' notice to commissioners where possible (or maximum notice available); maintaining service delivery standards throughout transition period; cooperating with local authority to ensure Care Act Section 48 duties discharged; providing all necessary information to facilitate smooth transitions; settling outstanding obligations to staff and suppliers; returning deposits and unused fees to service users and families; and conducting exit reviews to support sector learning.

13.4 Quality Metrics and Standards During Disruption

Commissioners require assurance that quality and safety standards are maintained even during business continuity incidents. The following minimum standards apply at all times:

Non-Negotiable Safety Standards:

These standards must be maintained regardless of disruption: safe staffing levels as defined by dependency assessments; medication administration without omissions or errors; safeguarding monitoring and response; fire safety and emergency evacuation capability; food safety and nutritional standards; infection prevention and control; and access to emergency healthcare.

Acceptable Temporary Service Modifications:

During major incidents, the following modifications may be implemented temporarily with service user consent and commissioner notification: reduction in community activities and social outings; simplified meal choices using available ingredients; postponement of non-urgent healthcare appointments; modified shift patterns to maintain essential staffing; temporary changes to visiting arrangements; and use of agency staff to supplement core team. All modifications are documented, time-limited, and subject to regular review for impact on service user wellbeing.

Quality Monitoring During Incidents:

Enhanced monitoring is implemented during business continuity incidents: daily senior management presence on-site; increased supervision of temporary or redeployed staff; daily service user welfare checks; medication administration audits; incident and accident monitoring; complaint and concern tracking; family feedback collection; and staff wellbeing assessments. Monitoring data is shared with commissioners as requested.

Evidence of Quality Maintenance:

Post-incident reviews include analysis of quality indicators during the disruption period: safeguarding incidents; medication errors; falls and injuries; complaints; staff incidents; and service user feedback. This evidence demonstrates our ability to maintain standards under pressure and identifies any areas requiring improvement. Reports are provided to commissioners upon request.

13.5 Supply Chain Resilience and Due Diligence

We recognise that our service delivery depends on reliable supply chains. The following arrangements ensure supplier

resilience and alternative provision if primary suppliers fail.

Critical Supply Dependencies:

Our critical suppliers include: community pharmacy for medication supply; food wholesaler/caterer for meal provision; PPE and clinical supplies distributor; utilities providers (electricity, water, gas); IT systems and electronic care records provider; payroll services provider; and agency staff providers. Each critical supplier is assessed annually for business continuity capability, financial stability, and contingency arrangements.

Alternative Supplier Arrangements:

We maintain relationships with alternative suppliers who can provide rapid replacement if primary supplier fails: secondary pharmacy with emergency prescription arrangements; alternative food suppliers including local retailers and wholesale markets; backup PPE suppliers with 24-hour delivery capability; multiple agency staff providers across different organisations; IT support from alternative providers or internal capability; and payroll bureau contingency arrangements. Contracts include service level agreements with response times for critical failures.

Supplier Business Continuity Assessment:

When selecting and reviewing critical suppliers, we assess: evidence of their own business continuity planning; financial stability and insurance coverage; geographic diversity (avoiding single site dependencies); alternative delivery options if normal routes disrupted; communication protocols for supply issues; and references from other care providers. Suppliers demonstrating poor business continuity capability are not appointed or are replaced during contract reviews.

Emergency Stock Holdings:

To provide buffer against supply chain disruption, we maintain: 72-hour food stock including frozen, chilled, and ambient foods suitable for various dietary needs; 14-day supply of essential PPE (gloves, aprons, masks) based on normal usage rates; 7-day medication supply for all service users with secure storage; cleaning and disinfection materials for 2 weeks; continence products and personal care supplies for 1 week; first aid supplies and basic medical equipment; and emergency equipment (torches, batteries, blankets, portable heaters). Stock levels are checked monthly and replenished immediately when depleted.

13.6 Information Sharing and Data Protection During Emergencies

During business continuity incidents, appropriate information sharing is essential while maintaining data protection compliance. The following protocols balance these requirements:

Lawful Basis for Emergency Information Sharing:

Under UK GDPR Article 6(1)(d), we can share personal information without consent where processing is necessary to protect vital interests of the data subject or another person. During emergencies, this allows us to share service user information with emergency services, healthcare providers, commissioners, alternative care providers, and families where necessary for safety and welfare. All emergency information sharing is documented with justification recorded.

Commissioner Access to Information:

During major incidents, commissioners may require access to service user information to: verify welfare and safety of funded individuals; coordinate alternative placements if required; discharge Care Act duties to ensure continuity; assess provider capability and sustainability; and coordinate multi-agency response. We will provide requested information promptly while ensuring it is limited to what is necessary, relevant, and proportionate to the circumstances. Data sharing agreements with commissioners specify emergency access protocols.

Secure Information Transfer Methods:

Even during emergencies, information security standards are maintained: encrypted email for electronic transmission; secure file transfer systems where available; password-protected documents with passwords communicated separately; verbal information sharing recorded in writing afterwards; hard copy records transferred in sealed envelopes with signed receipt; and no personal information shared via unencrypted methods (standard email, text message, social media). If systems failure prevents secure transfer, we document alternative methods used and security measures applied.

Data Breach Notification:

If a business continuity incident results in personal data breach (loss of records, unauthorised access, cyber-attack, etc.), we notify the Information Commissioner's Office within 72 hours as required by UK GDPR Article 33. Affected service users and families are informed without undue delay if the breach poses high risk to their rights and freedoms. Commissioners are notified as key stakeholders and we cooperate fully with any ICO investigation.

13.7 Service User and Family Co-Production

Service users and their families are partners in business continuity planning. We ensure they are informed, involved, and empowered throughout emergency preparedness and response.

Accessible Information About Emergency Procedures:

Every service user receives accessible information about what happens in emergencies including: fire evacuation procedures tailored to their abilities; what to expect if they need to move temporarily; how we'll keep them safe during disruptions; how families will be contacted; and their rights during emergencies. Information is provided in formats appropriate to communication needs: easy read documents for people with learning disabilities; visual guides for people with autism; translated materials for non-English speakers; and audio or large print for people with visual impairments.

Personal Emergency Evacuation Plans (PEEPs):

Each service user has a PEEP developed in consultation with them, their family, and relevant professionals. PEEPs specify: individual mobility and sensory needs during evacuation; communication requirements during emergencies; specific anxieties or triggers that may arise; equipment or aids required (wheelchair, walking frame, hearing aids, etc.); preferred support person during stressful situations; and any medication or items essential to take if relocating. PEEPs are reviewed annually or when needs change and copies stored in accessible locations for quick reference.

Family Emergency Contacts and Involvement:

We maintain current emergency contact details for families, advocates, and representatives with multiple contact numbers where possible. Families are informed promptly during incidents with updates on their relative's safety, location, and wellbeing. Families are consulted about temporary arrangements where service user lacks capacity to decide. We recognise families' anxiety during disruption and provide reassurance, access, and information as needed.

Service User Choice and Consent:

Where service users have capacity, their choices about emergency arrangements are respected including preferences for temporary accommodation, whether to stay with family during disruption, involvement of specific people in emergency response, and communication preferences during stressful situations. Mental Capacity Act principles apply throughout: presumption of capacity; supported decision-making; best interests decisions for those lacking capacity; least restrictive option; and respect for advance wishes where known.

Feedback and Learning from Service User Experience:

Following incidents, we seek feedback from service users and families about their experience including: what went well and

what could improve; whether information and communication were adequate; impact on wellbeing and how distress was managed; and suggestions for improving future response. This feedback informs plan updates and training programmes. Service users and families are thanked for their cooperation and resilience during difficult circumstances.

13.8 Pandemic-Specific Resilience (Post-COVID-19 Learning)

The COVID-19 pandemic highlighted specific resilience requirements for care providers during prolonged public health emergencies. We maintain enhanced preparedness for future pandemic scenarios.

Infection Prevention and Control Surge Capacity:

Our pandemic preparedness includes: enhanced PPE stocks (minimum 4-week supply of masks, gloves, aprons, eye protection); isolation facilities or zoning arrangements to separate infected and non-infected residents; enhanced cleaning and disinfection protocols ready for immediate implementation; staff training in donning and doffing PPE and infection control procedures; access to rapid testing capabilities; and relationships with public health teams for outbreak management support.

Staffing Resilience During Pandemic:

Pandemic planning assumes potential 30-50% staff absence through illness or isolation. Response measures include: cross-training staff to work flexibly across roles; arrangements for staff to stay on-site to prevent infection transmission; redeployment of administrative and management staff to care duties; mutual aid agreements with other providers for staff sharing; bank and agency relationships capable of surge capacity; and enhanced staff support including mental health resources, childcare assistance, and financial support for those unable to work.

Service User Wellbeing During Restrictions:

Pandemic responses often require restrictions on movement and visiting which significantly impact service user wellbeing. We maintain capability for: virtual visiting using video calls when physical visiting restricted; meaningful activities within service setting; outdoor access where safe; maintaining contact with family and friends through all available channels; monitoring mental health and emotional wellbeing with enhanced support where needed; and balancing infection control with human rights, dignity, and quality of life.

Vaccination and Prevention Strategies:

We actively support vaccination programmes for both service users and staff during pandemic scenarios. This includes: facilitation of vaccination clinics at our services; education and information about vaccine safety and benefits; addressing concerns and vaccine hesitancy through trusted healthcare professionals; documentation of vaccination status (with consent); and consideration of vaccination in risk assessments and service planning. We recognise vaccination as key preventive measure while respecting individual choice.

13.9 Commissioner Assurance Evidence and Documentation

Commissioners can request documentary evidence of our business continuity capability. We maintain readily available documentation including:

Business Continuity Plan (full operational document); Business Impact Analysis and risk assessments; testing and exercise records with outcomes and actions; insurance certificates (employers' liability, public liability, professional indemnity, business interruption); financial accounts and reserves statements; supplier contracts and alternative provider agreements; staff training records for emergency procedures; incident response logs and post-incident review reports; quality monitoring data during previous disruptions; PEEPs for all service users; accessible information materials for service users and families; and mutual aid agreements with partner organisations.

This documentation is available for commissioner audit, CQC inspection, and contract monitoring purposes. We welcome commissioner engagement in our business continuity planning and exercising activities to build confidence in our preparedness.

Policy Approval & Review

APPROVED BY	SIGNATURE
Olakunle Agunbiade	
REVIEW DATE	**NEXT REVIEW DATE**
16 February 2026	**16 February 2027**