Mersey and West Lancashire Teaching Hospitals NHS Trust

Business Continuity Policy

Version No: 2

Document Summary:
The aim of the MWL Business Continuity Policy is to ensure that the Trust has an effective business continuity programme in place, which includes a Business Continuity Management System (BCMS) to ensure continuity of operations during disruptions is maintained on a continual cycle.

Document status	Approved	
Document type	Policy	**Trust wide**
Document number	PD1867	
Approving body	Risk Management Council	
Date approved	09/09/2025	
Date implemented	09/09/2025	
Review date	***3 years from approval date** 30/09/2028	
Accountable Director	Chief Operating Officer	
Policy Author	Head of Emergency Preparedness	
Target audience	All staff	

The intranet version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled", as they may not contain the latest updates and amendments.

Document Control

Section 1 – Document Information	
Title	MWL Business Continuity Policy
Directorate	Corporate
Brief Description of amendments	
Full review in line with the requirements from EPRR Core Standards, NHS Business Continuity Toolkit and ISO22301	
Does the document follow the Trust agreed format?	Yes
Are all mandatory headings complete?	Yes
Does the document outline clearly the monitoring compliance and performance management?	Yes
Equality Analysis completed?	Yes

Section 2 – Consultation Information* *Please remember to consult with all services provided by the Trust, including Community & Primary Care			
Consultation Completed	☑ Trust wide ☐ Local ☐ Specific staff group		
Consultation start date	Click here to enter a date.	**Consultation end date**	Click here to enter a date.

Section 3 – Version Control		
Version	**Date Approved**	**Brief Summary of Changes**
1.0	11/10/2022	New policy
1 PD	14/08/2023	Harmonisation with S&O
2 PD	09/09/2025	Full review in line with the requirements from EPRR Core Standards, NHS Business Continuity Toolkit and ISO22301
	Click here to enter a date.	
	Click here to enter a date.	

Section 4 – Approval *– To be completed by Document Control*			
Document Approved	☑ Approved ☐ Approved with minor amendments		
Assurance provided by Author & Chair	☐ Minutes of Meeting ☐ Email with Chairs approval		
Date approved	09/09/2025	**Review date**	30/09/2028

Section 5 – Withdrawal *– To be completed by Document Control*	
Reason for withdrawal	☐ No longer required ☐ Superseded
Assurance provided by Author & Chair	☐ Minutes of Meeting ☐ Email with Chairs approval
Date Withdrawn:	Click here to enter a date.

Contents

1. Scope

The Mersey and West Lancashire Teaching Hospitals NHS Trust (subsequently referred to as MWL or “the Trust”) Business Continuity Policy applies to the entire Trust.

The Executive Directors are ultimately responsible for ensuring that all MWL services they are responsible for have in place business continuity plans, aligned with this document and guidance.

MWL is not responsible for the business continuity arrangements of their suppliers or contractors. However, as per the NHS Standard contract, providers must have Business Continuity Management Systems (BCMS) in place and MWL must, as per NHS EPRR Core Standards, seek assurance that such arrangements are in place.

In the case of the Trust Private Finance Initiative (PFI) Contract with NewHospitals, they and their subcontractors Vinci, Medirest, GE and Gentian are bound by contractual building and service provision contracts to comply with specifications and method statements agreed in conjunction with the Trust, which includes Business Continuity provisions.

2. Introduction

All NHS organisations have a duty to put in place continuity arrangements, under the Civil Contingencies Act (2004) and the Health and Social Care Act (2022). The NHS England Core Standards for Emergency Preparedness, Resilience and Response (EPRR) set out these requirements for all organisations. This means that services should be maintained to set standards during any disruption or recovered to these standards as soon as possible. This work is referred to in the health service as ‘emergency preparedness, resilience and response’ (EPRR).

Business continuity management (BCM) gives organisations a framework for identifying and managing risks that could disrupt normal service. The holistic process of business continuity management is an essential tool in establishing an organisation’s resilience, this policy outlines the framework that MWL will enact to meet their business continuity management obligations.

3. Statement of Intent

As a category 1 responder, the aim of the MWL Business Continuity Policy is to ensure that the Trust has an effective business continuity programme in place, which includes a Business Continuity Management System (BCMS) to ensure continuity of operations during disruptions is maintained on a continual cycle.

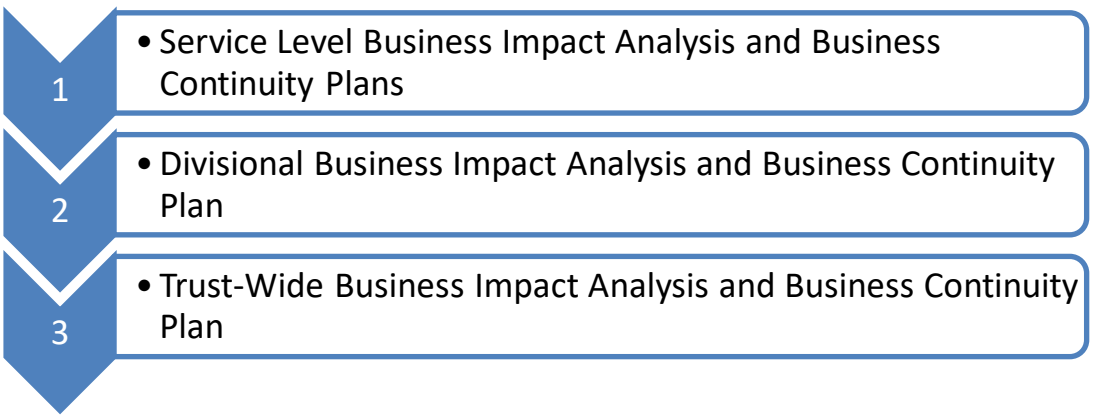
This Policy will act as a strategic framework for the BCMS, outlining the following:

a) Definition of business continuity for use in MWL.
b) Governance for the management of the BCMS.
c) Strategic aims and objectives for the BCMS.
d) Agreed methods and frequency for measurement and review of all stages of the business continuity lifecycle.
e) Identify standards and guidelines that are used as a benchmark for the business continuity programme.
f) Methods for sign-off and communication of the policy and all programme activities
g) How MWL will share their BC provisions with all interested parties.

The content of this policy content is aligned to the ISO-22301:2019 standards and is informed by the practices outlined by the Business Continuity Institute 'Good Practice Guidelines' (2023).

Compliance with this Policy will ensure procedures exist for recording, assessing, and managing business continuity risk; identifying and prioritising activities; and plans are in place to respond to business disruptions or incidents regardless of cause to maintain essential services (or restoring services to a minimum acceptable level).

The business continuity arrangements within the Trust consists of:



4. Definitions

Definition	Meaning
AEO	Accountable Emergency Officer
BCMS	A business continuity management system, or BCMS for short, is a management system that bundles interrelated methods, procedures, and rules to ensure that critical business processes keep running in the event of damage or emergencies and continuously develops and improves them.
BIA	A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment.
Business Continuity Incident	According to the NHS incident classification, is an event or occurrence that disrupts an organisation's normal service delivery, below acceptable predefined levels, where special arrangements are required to be implemented until services can return to an acceptable level.
CCA	Civil Contingency Act 2004
COO	Chief Operating Officer
Critical Incident	According to the NHS incident classification, is any localised incident where the level of disruption results in the organisation temporarily or permanently losing its ability to deliver critical services, patients may have been harmed or the environment is not safe requiring special measures and support from other agencies, to restore normal operating functions.
DDO	Divisional Director of Operations
DDDO	Deputy Divisional Director of Operations
Emergency	An event or situation, with a range of serious consequences, which requires special arrangements to be implemented by one or more emergency responder agencies
EPRR	Emergency Preparedness, Resilience and Response
LCO	Local Care Organisations.
MCS	Managed Clinical Services
MTPD	Maximum Tolerable Period of Disruption is the time frame within which the impacts of not resuming activities would become unacceptable
MWL	Mersey and West Lancashire Teaching Hospitals NHS Trust
Resilience	The ability of an organisation to adapt, respond and recover to disruptions, whether internal or external, to deliver organisationally agreed critical activities.
Response	Decisions and actions taken in accordance with the strategic, tactical, and operational objectives defined by emergency responders.
RMC	Risk Management Council
RTO	Recovery Time Objective is the time frames for resuming disrupted services at a specified minimum acceptable capacity

5. Duties, Accountabilities and Responsibilities

5.1 Accountable Emergency Officer (AEO)

The Chief Operating Officer is the Accountable Emergency Officer (AEO) and has executive authority and responsibility for ensuring the organisation complies with legal requirements, this includes putting in place business continuity management arrangements as per the Civil Contingencies Act 2004. The AEO will provide assurance to the Risk Management Council (RMC) and, by through this, to the Trust Board that this Business Continuity Policy and the management system it provides is actioned across the Trust. The AEO will be aware of their legal duties to ensure preparedness to respond to an incident within the Trust's remit to maintain the public's protection and maximise the NHS response.

Specifically, the AEO will be responsible for:

a) Ensuring that MWL is compliant with the business continuity requirements as set out in the Civil Contingencies Act (2004), the NHS Act (2006) (as amended) and the NHS Standard Contract, including the NHS England EPRR Framework (2022) and the business continuity standards as set out by the NHS England Core Standards for EPRR.
b) Ensuring that the organisation has in place a system to assess the business continuity plans of commissioned providers or suppliers; that these are aligned to ISO 22301:2019 or subsequent guidance, and MWL are assured that these providers business continuity arrangements work with MWL s own business continuity arrangements.
c) Ensuring that the organisation is appropriately prepared and resourced for dealing with a disruptive incident impacting the continuity of MWL operations.
d) Ensuring that the organisation complies with any requirements of NHS England, or agents of NHS England, in respect of monitoring compliance with business continuity arrangements.
e) Providing NHS England with such information as it may require for the purpose of discharging its functions.

5.2 Head of Emergency Preparedness

a) Supporting the implementation of the Business Continuity Policy across all hospital, managed clinical services and local care organisations (LCO).
b) Providing quarterly assurance updates to the Trusts Risk Management Council.
c) Ensuring that business continuity mapping is completed by all MWL services annually, requesting assurance from all Divisional/Deputy Divisional Directors (for non-clinical functions: Heads of Service) that identified services are included in service level business continuity plans.
d) Ensuring Business Continuity Plan ratification is a standing item on the EPRR Group agendas.

e) Providing assurance to the AEO / Board that effective business continuity arrangements are in place that have been reviewed and exercised.
f) Developing, maintaining, and exercising the MWL Business Continuity Plan.
g) Highlighting areas of risk or gaps in business continuity arrangements to both the EPRR Group and the RMC.
h) Ensuring that business continuity training and exercising is in place in line with a training needs analysis, and available to the Trust via the MWL EPRR Training and Exercising Programme.
i) Organising external audits for business continuity quality assurance as appropriate.

5.3 Emergency Preparedness, Resilience and Response (EPRR) Team

The EPRR Team, under direction of the Head of Emergency Preparedness, is responsible for:

a) Develop business continuity mapping for the whole Trust to ensure an accurate overview of services.
b) Supporting the head of services to ensure all mapped services have in place a Service-Level Business Continuity Plan.
c) Highlighting areas of risk or gaps in business continuity arrangements to Head of Emergency Preparedness
d) Working with the service managers to embed business continuity planning across the Trust.

5.4 Divisional Directors/Deputy Divisional Directors (for non-clinical functions: Heads of Service)

a) Ensuring that business continuity is part of everyday culture, promoted and embedded across all services.
b) Ensuring that this Policy, the MWL Business Continuity Plan and the Service-Level Business Continuity Plans are implemented at local level, and that there are appropriate records in place to support Trust governance and audit process.
c) Ensuring all identified services within the business continuity mapping are included in a Service-Level Business Continuity Plan.
d) Escalating any gaps or risks relating to Business Continuity to the EPRR Group.
e) Ensuring adequate support and resource is offered at service level to allow the hospital / MCS / LCO to benefit from the business continuity training and exercising / workshops offered by the EPRR Team.
f) Alerting the EPRR Team to business continuity incidents and requesting support to facilitate debriefing sessions. The Chief Operating Officer will be responsible for any actions highlighted because of the debrief.

5.5All MWL staff[1]

a) Familiarise themselves with business continuity plans relevant to their role.
b) Participate to business continuity training and exercises, as appropriate for their role.
c) Recognise an incident happening and escalate it appropriately, as per instructions of the relevant business continuity plan.
d) Respond appropriately to specific threats, as per instructions of the relevant business continuity plan.

6. Activation of the Plan

6.1 Internal Declaration

Any member of staff may notice an event or incident that gives cause for concern. These should be escalated to their Line Manager. The Line Manager will deal with the incident or event or report it to the most Senior Manager in their area. All decisions about escalation and activation of business continuity plans should be made in conjunction with the STRATEGIC COMMANDER (COO/Strategic on Call) and the TACTICAL COMMANDER (DDDO/Head of Operations/Tactical on Call). The EPRR Team MUST be notified of an internal incident and a 'Business Continuity Incident – Internal SitRep' MUST be emailed to EPRR.MWL@merseywestlancs.nhs.uk regardless of the level of incident (Appendix C).

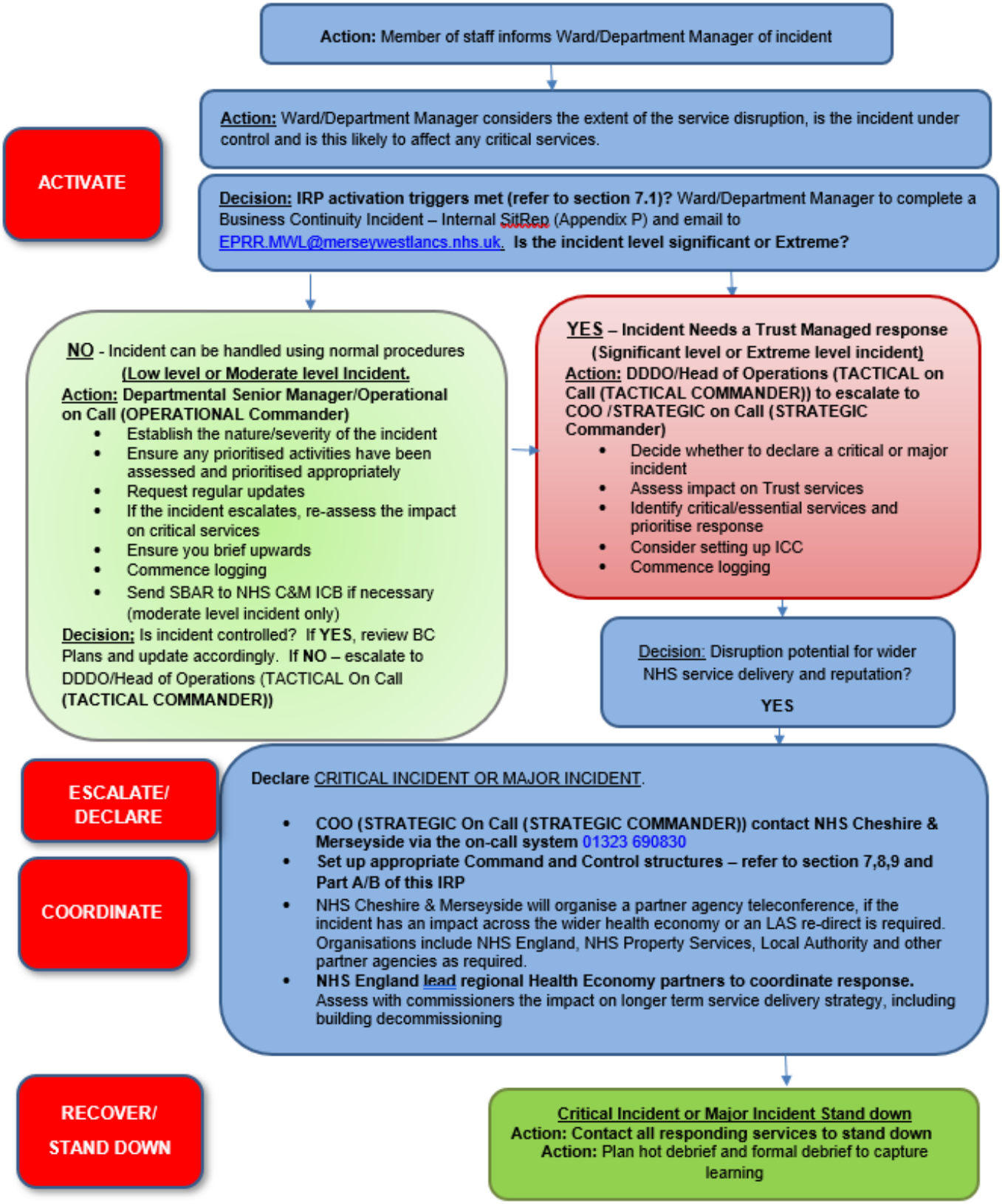
Rising Tide events will follow the same process though this will usually be more measured. Incidents or events may be announced by NHS England.

As the Trust is geographically placed between Merseyside and Lancashire Resilience Forums, it would be expected to respond to incidents within both regions. For the purpose of reporting however, the Trust reports to NHS England Cheshire and Merseyside Integrated Care Board.

More information regarding responding to a Business Continuity Incident can be found within the Trust's Incident Response Plan.

[1] This section applies to all staff working on Trust premises, included agency staff, contactors employees, PFI partners and all other organisations whose employees are present on Trust premises.

6.2 Internal Activation Flowchart



6.3 Business Continuity Management Activation and Process

Once an incident or event has been identified, the AEO or COO will make the decision as to how BCM reporting, and management will occur. This will usually take place in the Incident Coordination Centre (ICC). The location of the ICC will depend upon which site the incident occurs (please refer to the Incident Control Centre Standard Operating procedure). An incident or event may result in full activation of the Incident Response Plan, depending upon the severity.

The following would be expected to provide situation reports on a regular basis and to ensure attendance at Trust meetings:

- Senior Nursing Representative (usually DON or DDON)
- Deputy Divisional Directors of Operations (DDDO)/Head of Operations
- Operational Teams for each of the divisions
- Patient Flow/Operational Site Managers
- Estates and Facilities Senior Managers
- Communications Manager or deputy
- Bed Management representative

6.4 External Reporting

Information will be requested by NHS England/NHS England Cheshire & Merseyside Integrated Care board (ICB) at various times throughout the incident or event. This will include information about business continuity and recovery. The information is shared via Situation, Background, Assessment, Recommendation (SBAR) Reports and requests for information are added as required. The Strategic Commander will be responsible for signing-off and submitting SBAR Reports to NHS England/NHS England Cheshire & Merseyside (please refer to the Incident Response Plan for further information).

6.5 Recovery

Each Business Continuity Plan should include plans for recovery. A graduated return to normal services would be expected as operational plans return to normal. It would be usual for those services that were stopped or reduced last should be the first to be reinstated.

7. Process

7.1 Overview

HM Government Emergency response and Recovery (updated October 2012) highlights the importance of focusing on critical functions and how they can continue to be delivered in the event of a major incident or critical event. The following should be given due consideration when considering Business Continuity Management.

Business Continuity Plans (BCPs) should always be read in conjunction with the Trust's other emergency documentation, especially the Incident Response Plan.

The aims and objectives of BCPs are as follows:

- reduce the effects of any incident or disruption to services.
- reduce or avoid the impact on patients, staff, and the wider community.
- provide an easy-to-read guide for Trust employees and Senior Managers
- ensure a speedy re-establishment of Trust services.
- reduce the impact on the Trusts financial income.
- reduce the impact on the Trusts reputation.

The Plan may be considered from minor events or incidents to high impact events such as a 'Rapid Onset' incident or a Rising Tide event such as Pandemic Flu, in conjunction with other emergency plans.

A Business Continuity Incident is any incident that affects the Trust's ability to deliver one or more services. This could be anything from a minor disruption to something major and may be out of the Trusts control i.e. flood, heatwave, flu. Risks should be continually assessed and must take into account the Community Risk Registers and include scenarios for:

- severe weather (including snow, heatwave, flooding) and climate change
- staff absence (including industrial action)
- loss of equipment, loss of building
- IT and communications failure etc.

7.2 Things to consider when preparing Business Continuity Plans

7.2.1 Criticality

It is essential that all Business Continuity Plans focus on ensuring critical functions can be delivered. Which functions are critical may depend on the nature of the emergency in question and may be different for each department or area. The following guiding principles should be used when deciding whether or not a service or activity is critical.

7.2.2 Emergency Management/Civil Protection

Functions that underpin the capability to respond to the emergency itself, and take effective action to reduce, control or mitigate the effects of the emergency. i.e. electricity generators in the event of a power failure.

7.2.3 Impact on human welfare, the environment and security:

The significance of services to the effective functioning of the community in the event of an emergency should be considered when preparing business continuity plans. This should include any potential impact to the environment.

7.2.4 Climate Change Adaptation

The significance of considering the impact of current and future effects of climate change when writing business continuity plans. Effective planning to reduce mortality and morbidity associated with climate change, whilst ensuring resilience and service continuity.

7.2.5 Legal implications:

Statutory requirements and the threat of litigation if a service is not delivered or is delivered inadequately. i.e., emergency planning provision.

7.2.6 Financial implications:

Loss of revenue and payment of compensation. i.e., theatre failure or outbreak of Hospital or Community Acquired Infection.

7.2.7 Reputation:

Functions that impact on the credibility and public perception of the organisation – quality issues or targets such as cancer and the ED.

7.2.8 Service levels:

The Trust would be required to continue to deliver services at ordinary levels in the event of an emergency. However, some critical functions may need to be increased while others (which are non-critical) may need to be scaled down or suspended. i.e. ED is critical at all times but RVS shop/WHSmiths is not.

7.2.9 Balance of investments:

The Trust cannot commit unlimited resources to BCM. There must therefore be a process for effectively managing the prioritisation of services, see below. However, a budget code has been made available for those times when unexpected expenditure is necessary.

Business Continuity requires the review and prioritising of core services and activities which may include, but is not exhaustive:

- Service Continuity – Delivering safe patient care
- Staff Security and Welfare
- Communications (i.e. fax, phones & mobiles)
- Internet / Intranet / E-mail
- Backup Facility & Data Security
- Building Security
- Health & Safety
- Finance
- Equipment / suppliers
- Flexible Working Practices
- MHA Compliance

7.3 Risk Assessment

The Trust risk register is monitored and managed by the RMC: this will include threats within the Trust's control (for instance: equipment failure, which can be prevented by proper maintenance). Any Business Continuity/EPRR risks identified will be added to the InPhase system as per the Risk Management Policy.

The process of risk assessing business continuity threats is subtly different to the conventional approach, as it is not possible to reduce the likelihood of many of the threats MWL face (for instance: adverse weather): these types of events simply must be planned for on the basis that they can happen. The cause of the problem is, however, usually immaterial when it comes to business continuity (for instance: it doesn't matter whether a building is inaccessible because it

has burned down or is completed flooded; in either case the organisation must respond to a loss of resource). For this reason, MWL will take into consideration the following risks to services as part of the planning assumptions to develop its business continuity arrangements:

Hazard	Risk to Services
Data stolen/lost	Data loss
Destruction of paper files	
Failure of back up or failsafe	
Hard Disk Drive Failure	
Damage to internal telephone network	ICT Failure
Damage to the data network	
Destruction of active directory	
Localised hardware failure	
Loss of major application	
Loss of minor application	
Loss of mobile/telephone phone networks	
Loss of switchboard	
Server failure	
Contamination	Loss of operating premises
Structural defect/failure	
Disruption to direct medical gas	
Disruption to water supplies	
Electric Supply Disruption	
Failure of fixed equipment	
Fire	
Flooding	
Introduction of cordon	
Loss of heating/cooling	
Clustered notice giving	Staffing Shortage
Transport disruption	
Epidemic illness	
Industrial Action	
School closures	
Sudden onset demand	
Contamination/product quality	Supplier Failure
Contract Breach	
Failure to fund/supply	
Industrial action by drivers	
Industrial action in supplier	
Stock management failure	
Supplier goes into administration	
Supply chain collapse	
Under production by supplier	
Contamination/product quality	

Source: NHS EPRR Business Continuity Management Toolkit

For specific planned operations (for instance: downtimes) ad-hoc risk assessments will be carried out and tailored business continuity provisions put in place as appropriate.

7.4 Business Impact Analysis

The Business Impact Analysis (BIA) is the process aimed to identify, quantify, and qualify the business impacts of a loss, interruption, or disruption of services, providing the data from which appropriate continuity strategies can be determined.

The BIA will break each service down into component parts, referred to as functions and will focus on these rather than roles or risks. The BIA will then RED, Amber, and Green (RAG) rate the functions to visually demonstrate how each service will contract and expand around circumstances of disruption. Each function shall have an identified RTO and Maximum Period of disruption (MTPoD), as well as details of the organisation risk that a failure to restore the service would bring.

The process shall:

a) Define the impact types and criteria used to measure them.
b) Assessing the impacts over time resulting from the disruption of these services.
c) Identify the time frame within which the impacts of not resuming activities would become unacceptable: this timeframe is defined as “maximum tolerable period of disruption (MTPD)”.
d) Set prioritised time frames for resuming disrupted services at a specified minimum acceptable capacity: this timeframe is defined as “recovery time objective (RTO)".
e) Identify prioritised services, based on the MTPD and RTO.
f) Determine which resources are needed to support the above-mentioned prioritised services
g) Determine the dependencies, including partners and suppliers, and interdependencies of prioritised services.
h) Will be undertaken annually as part of the BCP annual review schedule

Where a function has been RAG rated, the BIA and all interdependencies will be mapped to that RAG status. This ensures Estates, Information Technology (IT) and data priorities align to the function. Where gaps exist, due to contractual or response constraints, mitigating design solutions will be developed for the intervening period. The most up to date template for the BIA/BCP is available on the Trust intranet.

The BIA will be executed by the service managers in conjunction with the EPRR team and support will be requested to clinical staff or other relevant subject matter experts and it will inform the development of business continuity plans.

The BIA will classify services as follows:

Essential	High Priority	Medium Priority	Low Priority
Cannot tolerate disruption, disruption could present threat to life / harm and significant fiscal / reputational damage.	Can tolerate up to 24 hours of disruption, no immediate threat to life / harm within 24 hours of disruption, patients, staff, and visitors can be directed to another service or activity can be postponed until disruption resides. May have a fiscal impact but no reputational impact.	Can tolerate up to 48 hours of disruption, no immediate threat to life / harm and the activity is easily postponed with no lasting impact. Minimal financial and no reputational impact.	Can tolerate 48-72+hours of disruption. Should disruption last up to 72 hours, can be paused until further notice so resource can focus on any backlog in high/medium priority activities, and be resumed when all other backlogs are sufficiently cleared. No financial or reputational impact.

7.5 Business Continuity Management Cycle

The planning and implementation of Business Continuity Management is focused around key steps, as depicted below:

Step One 'Business Impact analysis and risk assessment'

Focuses on risk assessment and business impact analysis.

It is important that any significant risks threatening the performance of critical functions in the event of an emergency are identified and mitigated for, as this will enable resources to be targeted to the right areas. Both short-term and long-term impacts should be considered.

In this context, there are two strands to risk assessment, relating to external threats (i.e. risk of an emergency occurring) and internal risks (i.e. business risks) that could cause loss or disruption of critical services required to control, reduce or mitigate the effects of an emergency.

These may be identified separately but the business continuity management process and implementation may be the same. i.e. one plan may be suitable for a number of risks.

Business Impact Analysis is crucial to ensure full understanding of the effects of any disruption and how this can be managed. It will also enable priorities to be identified.

Step Two 'Business Continuity Strategy/Leadership'

Identifies the alternative strategies and mitigation that can be put in place to reduce or remove the identified risks and maintain the business-critical functions.

Step Three 'Establish and implement BC Procedures'

Develops the response through improvements or changes to operational management and other factors that may be called into play to enable the business to continue.

Step Four 'Exercising and Testing'

Is the education and awareness of all Trust employees and associated stakeholders. EPRR Group meetings incorporate any Business Continuity Planning issues, and these meetings are held monthly to ensure that each Managed Clinical Area (MCA) is able to request assistance in completing and reviewing their plans if required.

Business Continuity exercises will be raised through the EPRR Group and will contribute to the training cycle for Emergency Preparedness, Resilience and Response.

7.6 Business Continuity Plans

Service managers are responsible for developing the Service-Level Business Continuity Plans, (with support from the MWL EPRR Team as required) based on the data acquired through the BIA. Such plans are developed giving full consideration of the NHS England Business Continuity Management Framework (2013), the NHS Business Continuity Management Toolkit (2023) and other relevant NHS guidance. Service-Level plans are intended for use when incidents or events that could lead to disruption, loss, or emergency occur within single

services or departments and can be managed locally. Escalation criteria are included within these plans, to ensure adequate response is enacted in case the disruption should require additional support to be managed and resolved.

The Service-Level Business Continuity Plans are ratified by the EPRR Group. Business Continuity Plan ratification should be a standing item on the Group agenda. The service-level Business Continuity Plan review schedule and associated compliance figures will be presented to RMC as part of the quarterly EPRR report for Trust Board Assurance.

Once the Service-Level Business Continuity Plans have been developed, tested and approved, divisional leads will perform a gap analysis to identify areas that need to be addressed or mitigated within their respective divisions. This analysis will help prioritise critical functions accordingly.

MWL has a Trust Incident Response Plan which will ensure that MWL has effective arrangements in place to respond to a trust-wide business continuity and critical incidents (please see definitions), in line with current guidance and legislation. This plan is ratified by the Risk Management Committee.

Both the Incident Response Plan and the Service Level Business Continuity Plans will be reviewed annually from their date of initial completion.

7.6.1 Interested Parties, External Suppliers and Contractors

MWL works with many external suppliers, contractors and providers that are important to the daily running of the Trust, these are identified as interested parties. MWL will ensure that all contracts / agreements with commissioned suppliers, contractors, and providers state that their business continuity plans can be requested by MWL at any time for audit to ensure they work with MWL plans and arrangements, and, that their participation in an exercise can be requested.

MWL have a diverse community portfolio, with a range of different sites and providers: this section does apply to them as well. The specific requirements, in this sense, are managed by the MWL Property Department.

As mentioned in section 1, in the case of the Trust Private Finance Initiative (PFI) Contract with NewHospitals, they and their subcontractors Vinci, Medirest, GE and Gentian are bound by contractual building and service provision contracts to comply with specifications and

method statements agreed in conjunction with the Trust, which includes Business Continuity provisions.

7.7 Business Continuity Plan Development

To maximise the benefits of a successful BCMS, it is advised that all NHS organisations should continually refer to the PDCA cycle as depicted below:

Source: Smartsheet, IS0 22301, PDCA Cycle

7.7.1 Step 1 – Understand Your Organisation

Risk Analysis and Business Impact Analysis

To mitigate for the unexpected, it is essential that a 'Business Impact Analysis' is completed (Please refer to the *'Business Continuity Plan Template v3.2025'*). Each ward/department/service area is requested to complete the template so that their risks can be clearly identified, assessed and planned for.

Topics for consideration when completing the assessment:

1. **What would be the impact upon your service if a Major Disruption or Loss affected critical service provision?**

Consider:

- Critical Services that must be kept operational – identify these and put them in priority order of red, amber, and green.

- Identify and consider who the key Internal and External stakeholders are and what their impact would be on the service i.e. Staff, patients, local community, ICBs, local authority, social services.

- Staffing – Levels / Skills / Availability etc. How can extra staff be called in as necessary? Can skills be transferred in the event of an incident? Are staff aware of this? Will they potentially refuse? What would they be expected to do when they are moved? Will they work at their current level? Do they require training prior to an incident occurring?

- Services (internal & external) – Pharmacy, Linen Services, Catering, Finance, Portering, Estates, Mortuary, Procurement. Have you got copies of external business continuity plans? If not, how do you determine how they will provide services in the event of an incident such as extreme weather?

- Environments – Consider suitability and accessibility, alternative locations for services displaced etc. in the event of fire, loss of power. i.e. theatres providing ICU cover if ICU not available. We could transfer services from one hospital site to another if this was necessary and safe to do so.

- Help from the independent healthcare sector – we have an independent healthcare provider located less than 4 miles from the Southport Hospital site so this could be a consideration for additional help in needed.

- Timescales for recovery – will the plans cover for Immediate, Mid-term and Long-term timescales? i.e. theatre out of action for longer than 3 months.

- Systems - Mass Evacuation of service area such as a ward, IT and Medical Records in the event of system failure. Security of the Trust and all associated premises. Machinery and essential equipment – hire in or do without?

Matrix & Risk Assessments

The Business Impact Analysis contains a Risk Assessment Matrix to enable full risk assessment to be completed. By risk assessing each hazard, each area will enable prioritisation of services and provide details of any mitigation put in place to reduce the risk.

7.7.2 Step 2 – Alternative Strategies

The nature of the risk will determine which business continuity strategy is appropriate and what, if any, action is required. At one end of the spectrum, disruptions that are low likelihood and low impact may require no specific action and may be dealt with through generic arrangements. Risks that are high impact and high probability point to the development of specific plans and risk mitigation strategies.

Options available:

a. **DO NOTHING** – in some instances top-level management may consider the risk to be acceptable;

b. **CHANGE, TRANSFER OR END THE PROCESS** – such decisions to alter business process must be taken with regard to the organisation's key objectives and statutory responsibilities;

c. **INSURE** – may provide some financial recompense or support but will not aid the organisation's response and will not meet all losses (e.g. reputation and other non-financial impacts, human consequences);

d. **MITIGATE LOSS** – tangible procedures to eliminate or reduce risk within the business; and

e. **PLAN FOR BUSINESS CONTINUITY** – an approach that seeks to improve resilience to interruption, allowing for the recovery of key business and systems processes within the recovery time frame objective, while maintaining key functions.

7.7.3 Step 3 – Develop and Instigate a Response

Each BCP needs to describe the management process for making these decisions (e.g. how will the prioritisation be made? Who makes this decision and on what basis?), and then the operational process for implementing them.

Where a service needs to be enhanced in the event of an emergency, where will the additional resources come from?

Where a service needs to be scaled down, how will demands on it be managed?

Where a service is withdrawn, how will staff and patients be informed?

7.7.4 Step 4 – Exercising and Testing

Ensure staff are fully aware of departmental BCPs and know what to do should they need to be implemented. Test, review and update regularly.
The Plans will be tested on a regular basis via the organisations Emergency Planning events and usual day to day activities.

7.7.5 Writing the Plan

Short and succinct - it will need to be read and understood in challenging and pressured circumstances.

Realistic - e.g. numbers of staff directly affected by the incident, the effect of the 'backlog trap' (i.e. the impact of the accumulation of tasks left uncompleted on recovery).

Referenced - e.g. guidance, databases, lists of key contacts, resources and suppliers.

Action Plans and Checklists as Required – Plans should be in compliance with ISO 22301:2019.

Clearly Identify Who 'Owns' Key Tasks? – What is expected of team members? Identify roles and who is the lead person.

Communications Management – Both internally and externally. This will usually be handled by the Communications Team. The Comms Team liaise closely with other NHS organisations to ensure messages are consistent. Please ensure the Communications Team are contacted before any messages are circulated.

7.7.6 Business Continuity Plan Governance Process

After the Business Continuity Plan is developed, it must be approved by the Division's governance groups before being submitted to the EPRR Group for final approval. Once approved, the BC Plan can be implemented within the ward, service, department, or division, with a hard copy stored in the Business Continuity Box (Battle Box). The Governance process cycle is outlined in Appendix A.

Following approval, the BCP needs to be exercised or tested to ensure its effectiveness. Any lessons identified during the exercise or test should be documented in a post-exercise report and shared with the EPRR Group. Following the exercise, the plan should be updated to incorporate the identified lessons.

7.8 Business Continuity Review

This Business Continuity Policy will be reviewed 3 yearly and taken to RMC for approval following consultation.

A systematic, independent, and documented process for obtaining audit evidence of Service-level Business Continuity provisions will be implemented across MWL, allowing for evaluation against a set of agreed audit objectives. This business continuity audit cycle will run across three years as recommended by the NHS England Business Continuity Toolkit.

The business continuity review will use the following assessment methods:

1. **Self-Assessment**

MWL Service-Level Business Continuity Plans will need to be self-assessed annually by using the checklist outlined in Appendix B. This checklist has been developed line with the NHS England Business Continuity Plan Checklist and Business Continuity Toolkit.

All services completing a Service-Level Business Continuity Plan will be requested to complete the checklist and return it to the EPRR Group the quarter before due date of revision, so that appropriate actions can be determined to update the plan, if necessary.

Any items of concern should be escalated to the EPRR Group.

2. **Quality Assurance**

Once a year, four plans (one in each quarter) will be selected by stratified sampling for review by the EPRR Group. Formal requirements of the review will not be defined, the EPRR Group will use their collective subject matter expertise to ensure the plans meet the Trust business continuity expectations, meaning that they can suitably manage disruptions outlined in section 6.1.

Should improvements be identified for the plan reviewed, an action plan will be agreed to implement them as per the Business continuity Lifecycle below and the EPRR Team will support the service where required.

Business Continuity Lifecycle

8. IT Infrastructure Business Continuity Process – Planned/Unplanned Outages

For unplanned outages:

1. Any member of staff who recognises that a digital system is unavailable, or not working as it should do, should inform the IT Service Desk as soon as possible, using the IT Self Service Desk (Sostenuto), or by calling extension 5678 at St Helens, Whiston and Newton sites, or extension 6666 at Southport and Ormskirk sites.

2. If the unavailable digital system is used for direct clinical care, or essential to any clinical or operational processes to continue, the individual in charge of the department/service at the time will make the decision of whether to revert to BCP.

3. It is the responsibility of all staff who use digital systems to be familiar with their own department's BCP, and the location of their nearest 'Battle Box' with BCP supplies.

4. The IT Service Desk will keep departments up to date with the status of the outage, and when the system becomes available again, via email. In the event of email being unavailable in addition to critical digital systems, runners will be utilized to deliver essential messaging to departments.

5. When IT Service Desk have advised the system is available again, staff must revert back to using the digital system. BCP documentation provides the true record of patient

care/other data for the time period of the outage and should not be transcribed back into the digital system unless this is absolutely essential for onward process e.g. booking of patient appointments. IT staff must not be utilized for the input of transcribed data, this is the responsibility of the department/service with specialist knowledge of the subject.

For planned outages:

1. When a project/technical colleague has recognised the need for a planned outage of a digital system, e.g. for an essential upgrade, they must inform the Head of Emergency Preparedness and complete the necessary documentation and preparatory work e.g. Trust-wide communications. The planned outage must be approved by the Clinical Safety Working Group (Chaired by the Chief Nurse Information Officer), prior to approval at CAB (Change Advisory Board). All efforts must be taken to ensure the impacted departments are fully aware of the planned outage and have adequate supplies for BCP.

2. It is the responsibility of all staff who use digital systems to be familiar with their own department's BCP, and the location of their nearest 'Battle Box' with BCP supplies.

3. The IT Service Desk will keep departments up to date with the status of the outage, and when the system becomes available again, via email. In the event of email being unavailable in addition to critical digital systems, runners will be utilized to deliver essential messaging to departments.

4. When IT Service Desk have advised the system is available again, staff must revert to using the digital system. BCP documentation provides the true record of patient care/other data for the time period of the outage and should not be transcribed back into the digital system unless this is absolutely essential for onward process e.g. booking of patient appointments. IT staff must not be utilized for the input of transcribed data, this is the responsibility of the department/service with specialist knowledge of the subject. In the case of a large scale planned outage, departments may need to consider arranging additional staffing to support in any data transcription, if this is essential to their service.

9. Training

The EPRR Team develops and manages an annual training and exercising schedule, in line with the requirements set in the NHS EPRR Core Standards. This schedule includes business continuity training, as follows:

a) Training / workshops aimed at those tasked with writing the Service-Level Business Continuity Plans.
b) Business continuity arrangements and responding to a Critical Incident as part of the Commander (Strategic, Tactical, Operational) training.
c) Loggist training for those with tasked with recording key decisions during business continuity incidents.

Also, business continuity exercising will be included in the schedule, and specifically:

a) 1 yearly table-top exercise to test the MWL Business Continuity Plan
b) Service-Level business continuity exercises / workshops on demand, subject to EPRR Team availability.

10. Monitoring Compliance

10.1 Key Performance Indicators (KPIs) of the Policy

No	Key Performance Indicators (KPIs) Expected Outcomes
1	Audit report of Service-Level Business Continuity Plans submitted to RMC (annually)
2	4 Service-Level Business Continuity Plans reviewed (annually)
3	Business Continuity plan review (annually)
4	Service-Level Business Continuity Plan Exercises and Lessons Identified

10.2 Performance Management of the Policy

Minimum Requirement to be Monitored	Lead(s)	Tool	Frequency	Reporting Arrangements	Lead(s) for acting on Recommendations
Report to RMC	Angela Manning	Report	Annual	Submitted to RMC	Lesley Neary
Review of this policy	Angela Manning	Policy document control	3 Yearly	Assurance provided to AEO	Angela Manning

11. References

No	Reference
1	Civil Contingencies Act 2004
2	NHS EPRR Framework 2022
3	NHS Commissioning Board Business Continuity Management Framework 2013
4	NHS EPRR Business Continuity Management Toolkit 2016
5	ISO 22301:2019
6	Business Continuity Institute “BCI Good Practice Guidelines” (2018)

12. Related Trust Documents

No	Related Document
1	MWL EPRR Policy
2	Service-Level Business Continuity Plans
3	Business Continuity and Critical Incident Plan and related appendices

13. Equality Impact Assessment (EIA) Screening Tool

The EIA screening must be carried out on all policies, procedures, organisational changes, service changes, cost improvement programmes and transformation projects at the beginning of the planning stage of any change process. Where the screening identifies that a full EIA needs to be completed, please use the full EIA template.

The completed EIA screening form must be attached to all procedural documents prior to their submission to the appropriate approving body. A separate copy of the assessment must be forwarded to PatientEDI@sthk.nhs.uk for monitoring purpose for EIAs carried out on patient related functions.

If the assessment is related to workforce a copy should be sent to workforceedi@sthk.nhs.uk

If this screening assessment indicates that discrimination could potentially be introduced, then seek advice from the Head of Patient Experience and Inclusion via cheryl.farmer@sthk.nhs.uk for patient related functions or Head of Workforce Equality Diversity and Inclusion via darren.mooney@sthk.nhs.uk for workforce related functions.

A full equality impact assessment must be considered on any cost improvement schemes, organisational changes or service changes that could have an impact on patients or staff.

Title of function	Business Continuity Policy
Brief description of function to be assessed	As a category 1 responder, the aim of the MWL Business Continuity Policy is to ensure that the Trust has an effective business continuity programme in place, which includes a Business Continuity Management System (BCMS) to ensure continuity of operations during disruptions is maintained on a continual cycle
Date of assessment	19/04/2025
Lead Executive Director	Lesley Neary
Name of assessor	Angela Manning
Job title of assessor	Head of Emergency Preparedness

1. Equality, Diversity & Inclusion

Does the policy/proposal:

1) Have the potential to or will in practice, discriminate against equality groups

2) Promote equality of opportunity, or foster good relations between equality groups?

3) Where there is potential unlawful discrimination, is this justifiable?

	Positive impact	Negative impact	No impact	Justification/ evidence
Age	Unknown	No		
Disability	Unknown	No		
Gender reassignment	Unknown	No		
Pregnancy or maternity	Unknown	No		
Race	Unknown	No		
Religion or belief	Unknown	No		
Sex	Unknown	No		

2. Human Rights

Is the policy/proposal infringing on the Human Rights of individuals or groups?

	Yes	No	Justification/ evidence and data source
Right to life	No	Neutral	
Inhumane treatment	No	Neutral	
Liberty	No	Neutral	
Right to privacy/family life, home and correspondence	No	Neutral	
Thought/conscience	No	Neutral	
Freedom of expression	No	Neutral	
Right to a fair trial	No	Neutral	

3. Health Inequalities

Is the policy/proposal addressing health inequalities and are there potential or actual negative impact on health inequality groups, or positive impacts? Where there are potential unlawful impacts is this justifiable.

	Positive Impact	Negative Impact	No Impact	Justification/ evidence and data source
Deprived populations	Unknown	No		

Inclusion health groups	Unknown	No		

4. Sign off

Name of approving manager	Angela Manning
Job title of approving manager	Head of Emergency Preparedness
Date approved	14/07/2025

1. EIA Action Plan

Recommendations	Actions Required	Resources required /costs	Timeframe	Lead officer responsible
-				

Please forward an electronic copy of this action plan with the completed assessment to , Cheryl.farmer@sthk.nhs.uk for patient related assessments or equality&diversity@sthk.nhs.uk for workforce related assessments for monitoring purposes.

14. Data Protection Impact Assessment Screening Tool

If you answer **YES or UNSURE** to any of the questions below a full Data Protection Impact Assessment will need to be completed in line with Trust policy.

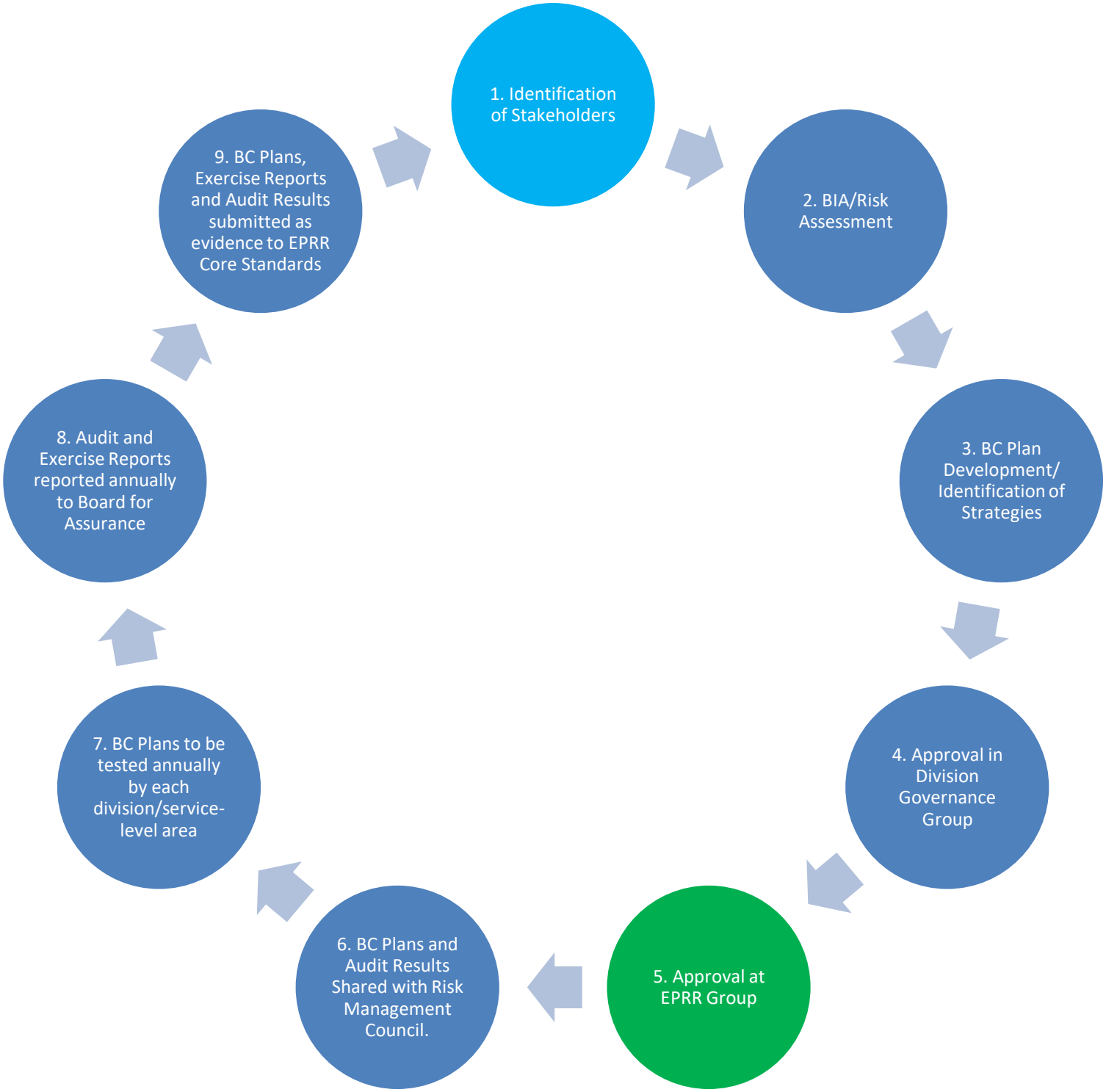
	Yes	No	Unsure	**Comments** - *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		✔		
Will the procedural document lead to the collection of new information about individuals?		✔		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		✔		
Will the implementation of the procedural document require you to contact individuals in ways which they may find intrusive?		✔		
Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		✔		
Does the procedural document involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition		✔		
Will the procedural document result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		✔		
Will the implementation of the procedural document compel individuals to provide information about themselves?		✔		

Sign off if no requirement to continue with Data Protection Impact Assessment:

Confirmation that the responses to the above questions are all NO and therefore there is no requirement to continue with the Data Protection Impact Assessment

Policy author _____ **Date:** **14/07/2025**

Appendix A – Business Continuity Plan Internal Governance Process



Appendix B – Service-Level Business Continuity self-assessment checklist

		Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?		
	Is it clear that the document is a Trust policy?		
2.	**Rationale**		
	Are reasons for development of the policy stated?		
3.	**Development Process**		
	Is the method described in brief?		
	Are individuals involved in the development identified?		
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?		
	Is there evidence of consultation with stakeholders and users?		
	Is the plan linked to the local risk register?		
4.	**Content**		
	Is the aim and objective of the document clear?		
	Is the target population clear and unambiguous?		
	Are the intended outcomes described?		
	Are the statements clear and unambiguous?		
	Are activation/escalation process' included?		
	Is the Command-and-Control structure included?		
	Are internal and external communication requirements included?		
	Are 24/7 capabilities included?		
	Are staff welfare factors included?		
	Does the plan include the stand down/recovery/debriefing process?		

		Yes/No/ Unsure	Comments
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?		
	Are key references cited?		
	Are the references cited in full?		
	Are local/organisational supporting documents referenced?		
6.	**Approval**		
	Does the document identify which committee/group will approve it?		
	If appropriate, have the joint Human Resources/staff side committee (or equivalent) approved the document?		
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?		
	Does the plan include the necessary training/exercising to ensure compliance?		
8.	**Document Control**		
	Does the document include version history and identify key changes since the last approved version?		
	Have previous versions (digital and physical been removed/destroyed)		
9.	**Process for Monitoring Compliance**		
	Are there measurable standards or KPIs to support monitoring compliance of the document?		
	Is there a plan to review or audit compliance with the document?		
10.	**Review Date**		
	Is the review date identified?		

		Yes/No/ Unsure	Comments
	Is the frequency of review identified? If so, is it acceptable (Default is 3 years)?		
11.	**Equipment**		
	Does the plan outline equipment requirements?		
12.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?		

Appendix C: Business Continuity Incident – Internal Situation Report

Complete the following Impact Assessment when a disruption is reported/or is already occurring and will affect the Service being delivered. Once completed, use to make an assessment of priorities and to assist in the service recovery and then forward to person/team identified in your service areas BCP for escalation (i.e. Operational Site Manager/Tactical Command)

Service Delivery Team/Department/Ward	
Service Delivery/Department/Ward Manager	
Contact Details of Service/Department/Ward Manager	
Person reporting the incident (Name and Details)	

Date of Disruption Occurring	**Time of Disruption**	**Date Disruption Reported**	**Time Disruption Reported**

(MAXIMUM PERIOD OF TOLERABLE DISRUPTION (MPTD)

ESSENTIAL Activities Class 0 MPToD: None Permissible	**HIGH PRIORITY Activities Class A MPToD: 24hrs**	**MEDIUM PRIORITY Activities Class B MPToD: 48hrs**	**LOW PRIORITY Activities Class C MPToD: 72hrs+**
Activities which cannot tolerate any disruption. If activities are not resumed immediately it may result in the loss of life, significantly impact patient outcomes, significant impact on other NHS services	Activities which can tolerate very short periods of disruption. If activities are not resumed within 24hrs patient care may be compromised, infrastructure may be lost and/or may result in significant loss of revenue.	disruption between 24hr & 48hr. If service / functions are not resumed in this time frame it may result in deterioration in patient(s) condition, infrastructure or significant loss of revenue.	Activities that could be delayed for 72 hours or more *but are required* in order to return to normal operation conditions and alleviate further disruption to normal conditions.

Confirm the nature and scale of the disruption	
Are there any casualties or significant injuries	
Are the Emergency Services required **- Has 999 been called** **- Are they in attendance now** **- When are they expected**	**YES** **NO**
What resources are affected	**STAFF:** **BUILDINGS:** **ICT/TELEPHONES/BLEEPS:** **UTILITIES:** **OTHER:**
Mutual Aid Request required? **Eg: patient transfers/ambulance divert**	**YES** **NO**

	DETAILS:
Media interest expected/received (please give details)	
How long is the disruption estimated to last?	
What assistance is required by other trust teams?	

Time Scale	Estimated Impact on Service
First 24 Hours	
First 3 Days	
First 7 Days	
Over 7 Days	

Please determine incident severity rating below and include rationale for your decision:

SEVERITY RATING	
1 – Low level incident (Business Continuity Minor Disruption)	
2 – Moderate level incident (Business Continuity Moderate Disruption)	
3 – Significant level incident (Critical Incident)	
4 – Extreme level incident	

NB: Internal Activation Triggers

Incident Level	Description
1 – Low level incident	This level would consist of routine issues which can be dealt with within **business as usual (BAU)** measures and will not impact upon any critical activities/services. i.e. Leaks, spills, generic maintenance issues... **One or more of the following apply:** • Limited impact on patient and staff safety • Incident expected to be fully resolved and closed within 24 hours • Limited but some impact on service delivery in critical areas • One or a number of local contingency plans activated • Incident still expected to be managed through localised contingency arrangements • limited financial/performance impact • limited governance isues • possible public/media/political interest
Incident managed using local contingency arrangements: Where the initial business/service impact assessment grades the situation as a minor disruption, the incident should be managed by the department within the localised BCP. The Managers will escalate to an appropriate DDDO/Head of Operations. Where the incident has the potential to impact on Patient Flow this must be escalated to the Patient Flow Daily Lead Where this incident has the potential to spill over into the evening / weekend the Operational On-call should be notified and informed of the contingency arrangements in place. Low level incidents **do not** need to be escalated to NHS Cheshire & Merseyside ICB; however, the Trust EPRR Team still need to be notified. The nominated Senior Manager (Operational on Call out of hours) will inform EPRR Team by sending the Business Continuity Incident – Internal SitRep to EPRR.MWL@merseywestlancs.nhs.uk	
2 – Moderate level incident	This level would consist of loss of **non-critical activities/services** due to a minor disruption or incident which is not expected to last more than **the Recovery Time Objective (RTO)** and will not impact on critical activities/services i.e. Local flooding, local IT failure, telecoms disruption, localised infection disease outbreak. ….

	• Disruption to a number of critical services likely to last for more than 1 working day • Moderate impact on patients and staff • Access to one or more sites denied where critical services are carried out for more than 24 hours • Suspension of a number of services required • Access to systems denied and incident expected to last more than 1 working day and therefore impacting on operational service delivery • A number of critical services seeking to activate service level contingency plans thus requiring overall management • Impacts on finances and performance • Governance issues • Possible public/media/political interest

Numerous contingency plans activated thus requiring effective management by calling together of a specific multi directorate/ team

Where the initial impact assessment grades the situation as a moderate level disruption, it will need to be formally managed to ensure resources and activities are effectively coordinated. An Incident Management Team should be set up and during working hours, the TACTICAL COMMANDER (Nominated DDDO/Head of Operations) or Tactical on Call out of hours will decide on its composition.

Out of hours, the Operational on Call Manager must be informed first, who in turn will notify the Tactical on Call and the team composition agreed.

The nominated Senior Manager (Operational on Call out of hours) will inform EPRR Team by sending the Business Continuity Incident – Internal SitRep to EPRR.MWL@merseywestlancs.nhs.uk

The TACTICAL COMMANDER (Nominated DDDO/Head of Operations or Tactical on Call out of hours) will inform NHS Cheshire and Merseyside ICB first on call, followed by sending the SBAR to ICC@cheshireandmerseyside.nhs.uk

3 – Significant level incident (Critical Incident)	This level would consist of loss of **critical activities/services** due to a disruption or incident which has a potential to last more than the **Recovery Time Objective (RTO)** but will need the coordination of a senior manager. i.e. Utility failure, damage to site, restricted access to site, partial loss of key suppliers…… • Incident expected to impact on critical services for 8-48 hours • Widespread disruption, loss of a major or multi-occupancy site including, • Major impact on patient and staff safety • Wide-scale incident in a geographical area affecting multiple critical services • Significant disruption to business activities • Local contingency plans inadequate to deal with incident • Outside interest causing major disruption to the smooth running of the hospital (e.g. significant press intrusion, protests at the hospital, protester with a weapon on roof of hospital, hostage situation) • Response requires strategic coordination and assistance from other health economy partners
Widespread incident requiring senior strategic and Tactical management: Where there is significant disruption, the incident will need to be formally managed to ensure resources and activities are effectively coordinated. In hours, the daily Patient Flow Lead, Divisional Director of Operations and Chief Operating Officer must be notified. Out of hours, the Operational, Tactical and Strategic on Call must be notified. O**ut of hours, the Tactical on Call Manager must attend site during a critical incident and if required, request on site support from Strategic on call Manager.** The nominated Senior Manager (Operational on Call out of hours) will inform EPRR Team by sending the Business Continuity Incident – Internal SitRep to EPRR.MWL@Merseywestlancs.nhs.uk The **COO or deputy (Strategic on Call out of hours)** will contact switchboard and ask for the 'Communication Cascade' to be activated and will activate the internal command and control structure. The COO or deputy (Strategic on Call out of hours) will inform NHS Cheshire and Merseyside ICB first on call, followed by sending an SBAR to: ICC@cheshireandmerseyside.nhs.uk	
4 – Extreme level incident	Loss of **critical activities/services** due to a disruption or incident which is expected to **last more than the RTO and may cause risk to patient and staff safety**

	i.e. Fire on a ward resulting in evacuation, Severe weather conditions causing damage to site and access issues, complete prolonged IT or Utility failure, External Major incident • Widespread or prolonged disruption expected to impact on Trust services. • Permanent loss of core service or facility. • Wide-scale incident in a geographical area affecting multiple services (eg incident with large number of casualties or Cyber-attack). • Response requires strategic coordination and assistance from other health economy partners. • Critical incident that is expected to have a significant impact on critical services for more than 48 hours.

Widespread incident requiring overall strategic command and control management.

Where the business/service area Initial impact assessment grades the situation as major disruption the incident will need to be formally managed to ensure resources and activities are effectively coordinated. The COO or deputy (Strategic on Call out of hours) will activate Strategic Command.

In hours, the daily Patient Flow Lead, Divisional Director of Operations and Chief Operating Officer must be notified. Out of hours, the Operational, Tactical and Strategic on Call must be notified.

O**ut of hours, the Tactical on Call Manager must attend site during a critical incident and if required, request on site support from Strategic on call Manager.**

The nominated Senior Manager (Operational on Call out of hours) will inform EPRR Team by sending the Business Continuity Incident – Internal SitRep to EPRR.MWL@Merseywestlancs.nhs.uk

The COO or deputy (Strategic on Call out of hours) will inform NHS Cheshire and Merseyside ICB first on call and consider national escalation to co-ordinate the response. The STRATEGIC Commander will also consider if the situation warrants a major incident to be declared. **Please note that a major incident should only be declared in a severe event or situation with a range of significant impacts**, **which requires special arrangements to be implemented by one or more emergency responder organisations** e.g. major hospital power failure requiring evacuation etc.
A major incident is:

a) beyond the scope of normal operations or business-as-usual;
b) likely to involve serious harm, damage or risk to human life or welfare, essential services, the environment or to the security of the UK;
c) a situation where the severity of impacts associated with a major incident are likely to constrain or complicate the ability of emergency responders to manage the incident;
d) likely to require a multi-agency response, rather than just a single agency response, which may include multi-agency support to a primary responding agency