

Policy Number OP104

Business Continuity Management Policy

Contents

1.0 Policy Statement	2
2.0 Definitions	2
3.0 Accountabilities	4
4.0 Policy Detail	8
5.0 Financial Risk Assessment	14
6.0 Equality Impact Assessment	14
7.0 Maintenance	15
8.0 Communication and Training	15
9.0 Audit Process	15
10.0 References	15

Annexes

A Business Continuity Management Toolkit	17
B Plan, Do, Check, Act Cycle	18
C Critical Departments	19

1.0 POLICY STATEMENT

- 1.1 Business Continuity is about maintaining our ability to deliver essential services during a major incident or emergency situation e.g. a major security incident or an influenza pandemic. Effective Business Continuity Management (BCM) is therefore about the identification, management and mitigation of particular risks to our ability to deliver these essential services.
- 1.2 This document contains the Business Continuity Policy for The Royal Wolverhampton NHS Trust (“the Trust”). Its aim is to establish a framework whereby the Trust has business continuity plans in place to enable it to respond to any untoward events in a co-ordinated manner, whilst continuing to provide the services to the people of Wolverhampton, Cannock and Partnership Organisations within the Black Country area, and to the extended catchment populations for which the Trust provides tertiary services in line with its regulatory obligations.
- 1.3 The objective of this policy is to provide a framework for the Trust’s business continuity arrangements which complements its Risk Management and Patient Safety Reporting Policy (OP10). The purpose of these arrangements is to enhance the resilience of the services provided by the Trust and to monitor the resilience of any services commissioned by the Trust.
- 1.4 This policy outlines the strategies and operational arrangements required to allow the Trust to continue to provide its essential services during a major incident or an emergency situation. This policy is the overarching policy, there are separate divisional and directorate business continuity plans containing specific operational details, arrangements and guidelines.
- 1.5 The Trust will keep its activities under review and will carry out regular assessments to identify risks to the achievement of the Trust’s corporate objectives, and to document how these risks are being managed. The Trust also develops, maintains and implements the Assurance Framework which identifies the principal (high-level) risks which may affect achievement of the Trust’s objectives and which provides assurance to the Board that these risks are effectively managed throughout the Trust.
- 1.6 This document explains the process steps involved in Business Continuity Management and outlines the arrangements required to manage risk and improve service resilience.
- 1.7. This policy complements and supplements The Royal Wolverhampton NHS Trust’s Risk Management and Patient Safety Reporting Policy.

2.0 DEFINITIONS

The following definitions are used in relation to business continuity and a requirement of ISO 22301/22313 compliance.

2.1. Business Continuity Policy

The key document sets out the scope and governance of the BCMS programme and reflects the reasons why it is being implemented.

2.2. Business Continuity (BC)

This is defined as a strategic and tactical capability of the Trust to prepare for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.

2.3 Business Continuity Management (BCM)

Is defined as: 'A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities,' (*Business Continuity Institute, Good Practice Guidelines, March 2019*).

For the NHS, BCM can more specifically be understood as the management process that enables an NHS organisation:

- To identify those key services which, if interrupted for any reason, would have the greatest impact upon the community, the health economy and the organization;
- To identify and reduce the risks and threats to the continuation of these key services;
- To develop plans which enable the organisation to recover and/or maintain core services in the shortest possible time.

2.4. Business Continuity Management System (BCMS)

BCMS 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.

2.5 Business Continuity Plans (BCP)

Service level Business Continuity Plans (BCP) are the foundation of BCM planning and set out the response arrangements within for the Trust, bringing together service information and incident response structure within each of the Trust's services. The components and content of a service level BCP will vary from Department to Department and will have a different level of detail based on the essential functions identified.

Directorate Business Continuity Plans sit above service level plans to provide the response framework to be utilised when more than one specialist service within a Directorate is affected.

Divisional Business Continuity Plans sit over these Directorate Plans to provide response arrangements in the event of a response being required from the Division as a whole.

2.6 Business Impact Analysis (BIA)

The BIA identifies, quantifies and qualifies the impacts and their effects of a loss, interruption or disruption and measures the impact of disruptions to its processes on the organisation. This typically covers resources, services and activities required to ensure the continuity of critical business functions it provides information that underpins later decisions about business continuity strategies.

2.7. Maximum tolerable period of disruption (MTPD)

This is the duration after which an organization's viability will be irrevocably threatened if product/service delivery cannot be resumed.

2.8. Recovery time objective (RTO)

Target time set for resumption of product, service or activity delivery after an incident.

2.9 Critical Activities

Those activities which have to be performed in order to deliver the key products and services which enable an organisation to meet its most important time sensitive objectives.

2.10 Disruption

For the NHS, **service interruption** may be defined as:

“Any disruptive challenge that threatens personnel, buildings or the operational procedures of an organisation and which requires special measures to be taken to restore normal operating functions which could be short, medium or long term”. For NHS organization's there may be a long 'tail' to an emergency event, for example, loss of facilities, provision of services to patients injured or affected in the event, and psychological support to victims and/or staff.

3.0 ACCOUNTABILITIES

Executive directors, managers and staff are responsible for establishing, maintaining and supporting a holistic approach to business continuity management. Some members of staff and Committees have particular specialist functions in relation to business continuity management as described below.

3.1 Trust Board

The Board's main role is to set the strategic direction of the Trust and to monitor performance over the year. It is the ultimate decision-making body in the Trust, accountable for overall performance and ensures that statutory, financial and legal responsibilities for the Trust are met. These responsibilities fall both to executive and

non-executive directors. The Board acts as the guardian of public interest, and is responsible for reviewing the effectiveness of internal controls – financial, organisational and clinical. The Board is required to satisfy itself that the management of the Trust is doing its “reasonable best” to manage the Trust’s affairs efficiently and effectively through the implementation of internal controls to manage the risks to the delivery of the Trust’s essential services.

3.2 Chief Executive

The Chief Executive is ultimately responsible for the Business Continuity Management system.

3.3 Accountable Emergency Officer (AEO)

The Accountable Emergency Officer (AEO) has overall responsibility for ensuring effective business continuity management is in place for the Trust. The Accountable Emergency Officer (AEO) is the Chief Operating Officer who will lead on promoting a culture of business continuity within the Trust, ensuring the Trust has robust business continuity planning arrangements in place, which reflect the standards set out in the Framework for Health Services Resilience and ISO 22301.

As AEO, the Chief Operating Officer is a member of the West Midlands Conurbation Local Health Resilience Partnership (LHRP), supported by the Head of Emergency Planning and Business Continuity.

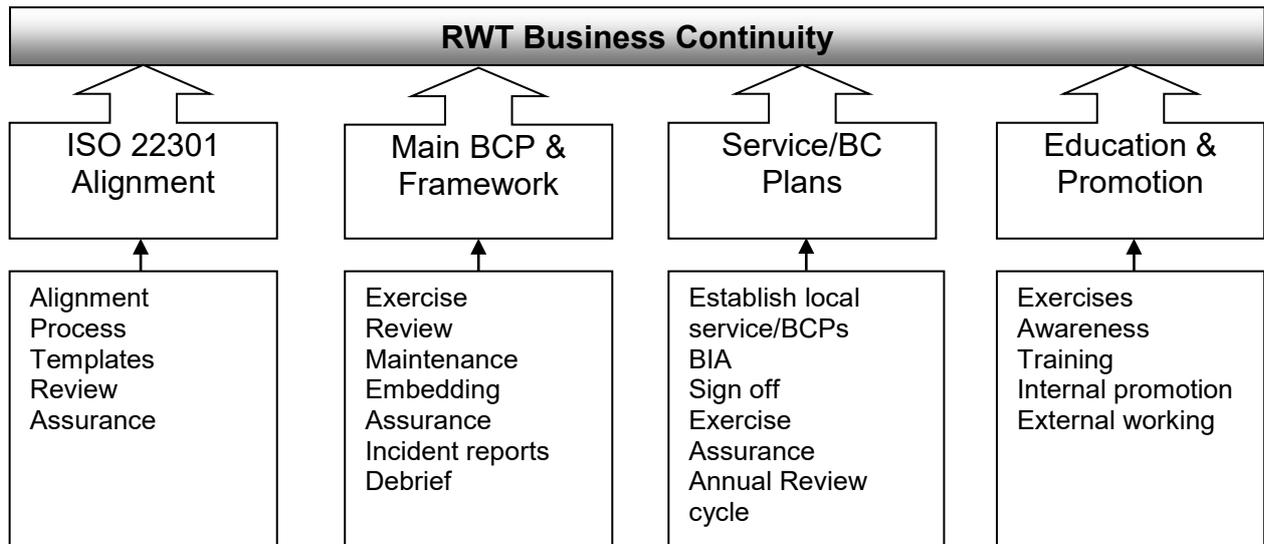
3.4 Head of Emergency Preparedness, Resilience & Response (EPRR) & Business Continuity

Accountable for overseeing the Trust’s BCMS and providing assurance, in line with the EPRR core standards requirements. They will act on behalf of the AEO, supporting the planning, reviewing, training and testing/exercising of the Trust’s plans in order for the Trust to meet its statutory obligations under the Civil Contingencies Act (2004).

The Emergency Planning Department will assist in supporting all Divisions, Directorates and Departments to develop, review and maintain their own business continuity plans, however overall responsibility for developing and maintain these plans remains with each Division, Directorate, Department and service area. These must be included in their business planning process each year.

BCM is overseen on a daily basis by the Head of EPRR & Business Continuity. The various work programs are depicted within *Figure 1* below.

Figure 1 BCM work programme



3.5 Emergency Planning Group (EPG)

Chaired by the AEO the EPG has responsibility for ensuring that the work of the Business Continuity Sub Group meets the requirements set out by the EPG and is undertaking the necessary actions and within stipulated timescales. The EPG is required to report to the Trust Management Committee and ultimately the Trust Board.

3.6 Business Continuity Sub Group

- Supporting the Trust in meeting the CCA requirements
- Providing the general principles to guide heads of departments, Deputy Chief Operating Officers/Divisional Managers or equivalents, Directorate Managers, Matrons, Senior Nurses in developing service level, Directorate and Divisional BCPs.
- Providing guidance to Primary Care Practices.
- Providing the generic templates to be used for the writing of service level, Directorate and Divisional BCPs.
- Ensuring that all critical and essential services are identified.
- Ensuring all plans are comprehensive and cover as a minimum the critical areas that all NHS organizations will cover:

People	Clinical Services
IT Systems, Telephony and Communications	Supplies & Suppliers (supply chain)
Premises	
Utilities	

- Ensuring that the Trust has an agreed and ratified overall corporate business continuity policy.
- The Business Continuity Sub Group is required to report to the Emergency Planning Group on its work plan and progress.

3.7. Information Governance Steering Group (IGSG)

To receive assurance that business continuity plans are up-to-date and tested for all critical information assets (data processing facilities, communications services and data) – specific measures are in place in line with Data Security and protection toolkit, Assertion 7. For further details refer to the [Information Governance Policy OP13](#).

Under information governance arrangements, the Senior Information Risk Owner (*SIRO*) is responsible for owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners (IAOs). It is therefore important that there is a sign off of any business continuity arrangements that impact on information assets including any associated dependencies. The IAO is responsible for knowing and contributing to business continuity plans that impact on their information assets including any associated dependencies, as well as understanding and addressing risks to the asset, and impact to the service and providing assurance to the SIRO. Any potential risks which need to be escalated to the SIRO will be dynamically risk assessed and reported to the Trust's SIRO, via local governance arrangements or through the Business Continuity Sub Group. Any specific work undertaken by IT in terms of 'continuity' of services following critical service interruptions will need to be risk assessed.

3.8 Deputy Chief Operating Officers/Divisional Managers or equivalents

Accountable for ensuring all departments/areas have robust service level BCPs.

3.9 Head of Departments, Service Leads, Community GP Practices, Group Managers, Directorate Managers, Matrons, and Senior Nurses

Selected operational managers will be referred to as Business Continuity Leads (BCLs).

As BCP Leads this group is responsible for:

- Ensuring that their departments/areas have comprehensive service level and Directorate BCPs in place, which are approved and shared;
- Driving forward their Business Impact Analysis/identification of threats/hazards with their teams;
- Carrying out a yearly self-assessment setting out review of plans including their business impact analysis;
- Ensuring that all relevant staff are informed and have received training in the use of the plans;
- Engaging with business continuity exercises and promotion of business continuity within their teams.
- Discharging their corporate responsibility that every directorate and department within the Trust is involved in business continuity management.

3.10 Employees

Employees are responsible for ensuring that they are familiar with and comply with all relevant policies and procedures for business continuity, including Health & Safety. They will support and engage with the business continuity management process and actively promote a culture of business continuity within the Trust.

4.0 POLICY DETAIL

In producing this policy a suite of business continuity models and tools have been consulted, including the statutory guidance on business continuity contained in Chapter 6 of the Emergency Preparedness document, published by the Government in support of the *Civil Contingencies Act 2004*.

The model adopted accords with the best practice expectations placed upon all NHS organisations in the *NHS England Business Continuity Management Framework (service resilience) 2013* and the associated requirements listed in the *NHS England Core Standards for Emergency Preparedness, Resilience and Response (EPRR)* being:

- a. ISO 22301 Societal Security – Business Continuity Management Systems Requirements;
- b. NHS England Emergency Preparedness, Resilience and Response (EPRR) Business Continuity Management Toolkit;
- c. Expectations and indicators good practice set for category 1 and 2 responders;
- d. Reflective of the British Standards Institute's PAS 2015:2010 *Framework for health services resilience* developed for the NHS.

The concept of cyclical BCM programme management which follows and the associated stages are directly derived from ISO 22301 and specifically the ISO 22313 Guidance:

1. Understanding the organization;
2. Selecting business continuity options;
3. Developing and implementing a business continuity response;
4. Exercising and testing.

Figure 2 below demonstrates that steps 1 - 4 are cyclical and they must be repeated at least annually to ensure compliance, currency and quality. Thus business continuity plans and associated elements developed as a result of this policy will be living documents that will change and grow as incidents happen, exercises are held and risks are reassessed.

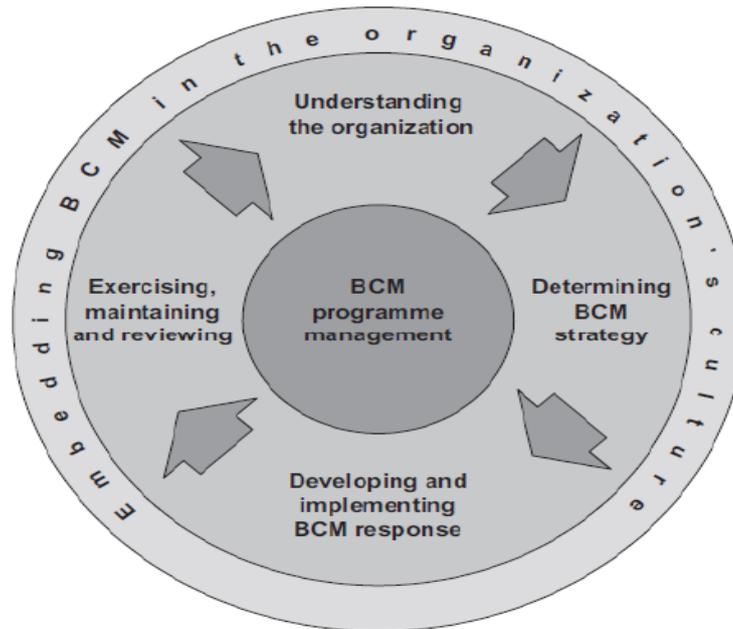


Figure 2 Business Continuity Management Lifecycle (Source: British Standard Business Continuity Management Part 1: Code of Practice, ISO 22313)

Supporting the BCM Management lifecycle a Plan, Do, Check, Act (PDCA) cycle is used. This is shown in [Annex B](#). and involves planning, implementing and reviewing business continuity arrangements.

4.1 Stage 1: Understanding your Business

A BCM strategy relies on clarity about the organisation's mission and defining the essential processes within that mission.

The Trust's vision is to be an NHS organisation that continually strives to improve patients' experiences and outcomes. Its core values can be summarised as:

- Patients are at the centre of all that the Trust does;
- The Trust will be innovative in how it works;
- The Trust will create an environment in which it thrives;
- Working together the Trust delivers top quality services.

The Trust's specific organisational goals are to:

- Provide patients and staff with a safe environment;
- Be the employer of choice;
- Achieve a balance between demand for services and capacity to deliver;
- Progressively improve the image and perception of the Trust;
- Be in the national NHS top quartile of benchmarks;
- Deliver services within financial allocations;
- Be a high quality educator;
- Agree with the wider health community appropriate population catchment areas for Trust services;

- Develop the Trust's position as a tertiary centre;
- Consolidate the Trust's position as a leading healthcare provider.

Informed by this context, Head of Departments, Group Managers, Directorate Managers, Matrons and Senior Nurses identify the critical, essential and routine processes of services within their departments, and consider the resources which support and contribute to the normal operation of the organisation and any statutory obligations or legal requirements placed on the Trust.

The Trust's Emergency Planning and Business Continuity Lead has developed a prioritisation methodology to assist Head of Departments/service leads, Group Managers, Directorate Managers, Matrons, and Senior Nurses in defining critical, essential and routine processes. This forms part of a business continuity toolkit, see [Annex A](#).

Where appropriate, the Trust will also review existing contracts, develop service level agreements and/or memoranda of understanding which will help in monitoring the business continuity arrangements of relevant external service providers/contractors.

4.1.2. Business Impact Analysis (BIA)

Having identified critical, essential and routine processes, the impact upon the organisation's goals and targets if these were disrupted or lost is determined through a Business Impact Analysis (BIA).

The BIA process:

- a. Defines the activity and its supporting processes;
- b. Maps the distinct stages of each activity and process;
- c. Determines the impacts of a disruption;
- d. Quantifies the maximum tolerable period of disruption (MTPD) for each process, the timeframe during which recovery must become effective before an outage compromises the ability of the Trust to achieve its business objectives.
- e. Defines the recovery time objectives (RTO), as the period of time following an incident within which a product or service must be resumed, activity must be resumed, or resources must be recovered; it must be less than the MTPD
- f. Determines the minimum resources needed to meet those objectives.

The BIA toolkit is included at

As part of the BIA process a privacy impact assessment (PIA) needs to be considered on all high risk data processing systems that involve clinical information, to ensure privacy risks are included as part of any plans in place. The PIA needs to highlight the need for BC in systems and processes.

4.1.3. Business Disruption Risk Assessment (BDRA)

To ensure delivery of a Trust-wide risk assessment element of this Policy which can be successfully embedded within the Trust's broader risk monitoring and management, a risk analysis methodology consistent with the preferred approach in use across the Trust is used for the identification and management of business

disruption risks. As such, Business Continuity risks are governed by the Trust’s wider risk assessment process and reported via the assurance framework as appropriate. The corporate risk register containing only extreme risks will be presented to the Trust Management Committee as appropriate through the Emergency Planning Group.

In following this approach and in assessing the generic, operational risks faced by the Trust the following sources of information are routinely referred to:

- Existing Trust Risk Registers;
- The Community Risk Register for the West Midlands Conurbation (drawn up by the Local Resilience Forum);
- The Incident History for The Royal Wolverhampton NHS Trust (if available);
- The Incident History for the West Midlands Conurbation Local Health Resilience Partnership;
- Regional Incident History.

Based on the outcomes of the risk assessment, strategies are devised for all risks identified from very high to low scores, based on the following framework.

Mitigation	Identifying strategies, activities, modifications or controls aimed at reducing the risk.
Acceptance	Ensuring the risk is owned at the appropriate level (normally director level) within the organization.
Transferring	Changing the process, ceasing the practice, outsourcing the service or transferring the risk (if financial by means of insurance)
Eliminating	Removing the cause, avoiding the risk or introducing preventative measures (if possible).
Recovery	Developing and testing recovery plans to deal with any threats and hazards identified.

For significant risks (rated High or Extreme) this may involve developing specific contingency plans, if appropriate, as part of Trust-wide business continuity planning. Other risks (rated Medium or Low) are managed at Divisional level as part of the Divisional service business continuity plans. Details of the business disruption risk methodology to used are included at [Annex A](#)

4.2 **Stage 2: Selecting Business Continuity Options**

The following paragraphs contain details of the key issues affecting service resilience and how they are addressed as part of the BCM policy for the Trust.

4.2.1. People – Loss of Staff

In the event of any Business Continuity Event which has a significant impact upon the Trust, whether or not a major incident is declared, there is minimal disruption to the delivery of essential services.

There may be several types of incidents which will affect the services provided by the Trust and its staff:

- Industrial unrest – the principles laid out in this document will be used should the Trust be affected by industrial action however, please refer to the specific management guidance should the need arise which is available;
- Influenza pandemic;
- Major Incident or Mass Casualty Incident;
- Inclement Weather Conditions – both in the event of extremely hazardous journeys i.e. snow or during a nationally declared heat wave;
- Fuel shortage.

The aim would be to ensure minimal disruption to the delivery of essential services. A large scale staff loss has been covered as part of pandemic planning but it is also recognised that the impact on the loss of staff may be different based on the event. Prioritisation of service, effective utilisation of resources and trigger levels for implementing agreed mitigation measures form part of BCPs and pandemic planning.

In the event of an incident affecting larger numbers of staff within the Trust (for example a flu outbreak), each directorate will manage its own staff to ensure that critical services can continue. Where this is not possible, other suitably qualified staff within the Trust will be redeployed as necessary. Please refer to policies [HR01](#), [HR02](#), [HR07](#), and [HR13](#).

4.2.2. Supplies and Suppliers

The Trust has confirmed the business continuity arrangements that are in place through the NHS supply chain to maintain an adequate supply of common consumables. The requirements for consumables and specialist items needed to support critical services will be identified by all directorates and will be reviewed on a regular basis.

The business continuity status of suppliers of critical services or goods will be assessed as part of the contract process. Suppliers are expected to adhere to business continuity best practice, following the principles of ISO 22301. This will include a defined business continuity plan to ensure the continuity of supply to the Trust.

Where possible, alternate suppliers will be identified for critical goods or services. At the time of a disruption to services or goods, the Trust will liaise with suppliers to minimise the impact of any disruption. If necessary, alternative suppliers will be engaged and Departments will identify opportunities for mutual support through other hospitals.

4.2.3. Equipment and Other Resources

All departments and services have identified alternative sources for obtaining specialist equipment, including mutual aid through NHS networks. Details are captured in departmental business continuity plans.

Where necessary, patients or procedures will be transferred to other hospitals until replacement equipment is commissioned.

4.2.4. Critical IT System/Applications

The Trust has identified its critical IT applications which are available on each of the Trust's computer desk tops under 'RWH Critical Applications', along with associated information to users. In the event of a 'cyber security' incident, service areas will need to implement local BCPs should any of their systems not be available. Identified system issues will be communicated through the Trust's IT Department via various communication links.

It is recognised that the Trust has a variety of IT applications which are directly administrated through different suppliers eg, Pathology, Radiography, Human Resources, predominately being web based – local service areas are required to include these in their local BIA assessments and BC plans.

4.2.5. Critical Departments

A list of Critical Departments which have services that need to be performed within 24 hours or less have been outlined by the Trust (see [Annex C](#))

4.2.6. Patient Transport Services

In the event of disruption to the provision of patient transport services, the Trust major incident plan would be used in terms of extra provision. In relation to accommodation of the service, the plan would be to utilise the contractor premises situated on Ettingshall Road, Wolverhampton and have access to their system. Mobile phones to contact other services would also be utilised.

Within the Trust, other offices would be used e.g. General Office or The Bereavement Centre.

4.3 Stage 3: Developing and Implementing a Business Continuity Response

In addition to a broad policy statement it is important to develop suitable business continuity plans. These are operational plans containing the arrangements required to address generic and specific threats faced by the Trust.

To supplement The Royal Wolverhampton NHS Trust's organisation-wide Business Continuity Plan, each service area will be required to develop its own business continuity plans. This will ensure that key stakeholders take responsibility for owning the BCM process at every level and for developing the arrangements required to respond to and recovery from an incident. These business continuity plans will build on pre-existing documents and good practice. The Royal Wolverhampton NHS Trust already has a range of supporting policies, plans and documentation in place to deal with a variety of incidents and emergency situations.

Plans will be available locally or on the Trust's shared point for business continuity.

4.4 Stage 4: Exercising and Testing

As illustrated in Figure 1 above, business continuity is a cyclical process. Risk registers, associated arrangements and plans need to be revisited on a regular basis.

The Trust will conduct incident or exercise debriefs and update plans and associated

documentation based on the lessons learnt. Risk registers will be reviewed and updated to allow for any change in circumstances and as new information becomes available.

As part of the ongoing business continuity cycle the Trust will re-evaluate its arrangements, identify the most vulnerable processes, improve resilience and thereby reduce the level of risk faced by the Trust.

Every 12 months, Emergency Planning will run a 'plan health check review,' which will run alongside the formal reviews that are conducted by the plan owners and will require completion of the plan health check document in the review process. At the very least business continuity plans will be reviewed as part of this yearly audit cycle.

5.0 FINANCIAL RISK ASSESSMENT

1	Does the implementation of this policy require any additional Capital resources	No
2	Does the implementation of this policy require additional revenue resources	No
3	Does the implementation of this policy require additional manpower	No
4	Does the implementation of this policy release any manpower costs through a change in practice	No
5	Are there additional staff training costs associated with implementing this policy which cannot be delivered through current training programmes or allocated training times for staff.	No
	Other comments	

6.0 EQUALITY IMPACT ASSESSMENT

The Trust has a commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment, pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of the development of this document and its impact on equality has been analysed and no detriment identified.

7.0 MAINTENANCE

This Policy will be maintained and reviewed on a 3 yearly basis by the Trust's Business Continuity Sub Group or earlier in the event of organisational changes within the Trust or changes to the relevant NHS England EPRR Core Standards.

8.0 COMMUNICATIONS AND TRAINING

This policy will be launched to all staff and key external stakeholders via email, staff bulletin and individual team briefing sessions as appropriate and a briefing at the Trust's Senior Managers meeting. This will also be available on the Trust's intranet site and via an external intranet site 'Resilience Direct' for key stakeholders.

9.0 AUDIT PROCESS

Criterion	Lead	Monitoring method	Frequency	Committee
NHS England EPRR Core Standards	Chief Operating Officer/ Accountable Emergency Officer	Self- assessment	Annually	Emergency Planning Group meeting
	Head of Emergency Planning	SharePoint established for Business Continuity Plan Owners and associated action tracker.	Quarterly	Business Continuity Sub Group

10. REFERENCES

Source of data	Date of publication / issue	Detail of requirement
ISO 22301 (BS 25999	This British standard was published under the authority of the Standards Policy – May 2012 – adopted by the NHS 2013	This is an international standard that establishes the process, principles and terminology of business continuity management. The common framework for achieving resilience across the NHS and now forms part of the EPRR core standards.

CCA 2004	Civil Contingencies Act 2004	Sets out the responsibilities for Category 1 and Category emergency responders.
Emergency Preparedness, Resilience and Response arrangements (EPRR) Framework	February 2019	Structure for emergency preparedness, under the NHS.
<p>EPRR Core Standards</p>  <p>core-standards-for-epr-rr-guidance-v5.0.pdf</p>	Updated June 2019	These are the minimum standards which NHS organisations and providers of NHS funded care must meet.
Good Practice Guidelines Business Continuity Institute	March 2019	Provides guidance for organisations on business continuity and resilience. It is an information source for raising awareness implementing Business Continuity Management.
<p>EPRR Business Continuity Management Toolkit</p> <p>https://www.england.nhs.uk/wp-content/uploads/2016/03/bcm-toolkit-cover-feb16.pdf</p>	February 2016	This is a best practice toolkit developed to aid NHS organisations in planning for business continuity incidents.

Business Continuity Management Toolkit



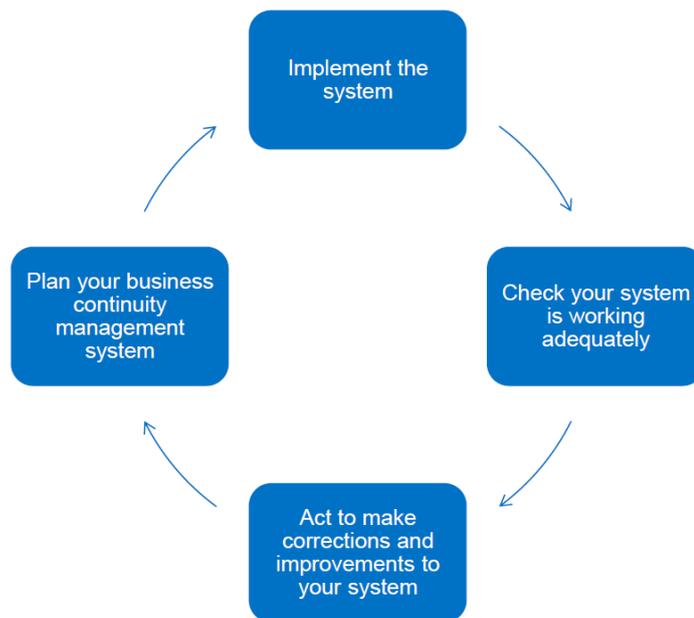
Annex A - BIA
template_ (2).xlsx



Annex A (2) - BDRA
template (2).xlsx

Plan, Do, Check, Act cycle

The Plan, Do, Check, Act cycle (PDCA), described below, is a four step process that involves planning, implementing and reviewing business continuity arrangements. It should be used alongside the business continuity management cycle and the purpose is to drive the continuous improvements in planning and effectiveness of business continuity across the Trust.



Source: *EPRR Business Continuity Management Toolkit, 2016*

Planning

- Developing policy
- Management Strategy (System design)
- Risk Assessments and Business Impact Assessment
- Plans

Do

- Implementation
- Training

Check

- Exercising
- Auditing and Review

Act

- Debriefing
- Action and improvement plans

CRITICAL DEPARTMENTS

The list below outlines the critical departments outlined by the Trust, in which services that need to be performed within 24 hours or less.

- Adult Community Services; District Nursing, Hospital at Home
- Emergency Department, AMU, Walk in Centres, NX & Phoenix Health,
- Hotel Services; catering, portering, domestics
- Estates
- Coronary care/Cardiothoracic
- Children's; Neonatal, Community, school and health visiting
- Diagnostic imaging
- Renal Dialysis Unit (s)
- Endoscopy
- Hospital sterilisation & Disinfection
- Intensive Critical Care Unit
- Maternity Department
- Medical Wards
- Oncology Oncology/Cancer Services
- Haematology
- Surgical Wards
- Pathology Department
- Pharmacy Department
- Physiotherapy
- Switchboard
- Theatres and Day Surgical Unit
- Information Management & Technology

Note: *This is not an exhaustive list.*

Reference Number and Policy name: OP 104 Trust Business Continuity Management Policy	Version: 3.0	Status: Final	Author: Head of Emergency Planning and Business Continuity Director Sponsor: Accountable Emergency Officer/Chief Operating Officer	
Version / Amendment History	Version	Date	Author	Reason
	1.0	April 2015	Head of Emergency Planning and Business Continuity	New policy required to evidence full compliance with NHS England EPRR Core Standards & Statutory Obligations under the CCA.
	2.0	July 2018	Emergency Planning Support Officer	Review date Inclusion of General Practices (Vertical Integration) & GDPS implications
	3.0	May 2021	Head of EPRR & Business Continuity	Policy expired – now reviewed and updated.
Intended Recipients: All Trust personnel				
Consultation Group / Role Titles and Date: Emergency Planning Group, Accountable Emergency Officer (AEO)/Chief Operating Officer, Business Continuity Sub Group Chair, Heads of Services.				
Name and date of Trust level group where reviewed	Emergency Planning Group Trust Policy Group – August 2021			
Name and date of final approval committee	Trust Management Committee – September 2021			
Date of Policy issue	October 2021			

<p>Review Date and Frequency (standard review frequency is 3 yearly unless otherwise indicated)</p>	<p>August 2024 - 3 Yearly from the date of approval or as determined by changes to the relevant NHS England Emergency Preparedness, Resilience and Response (EPRR) Core Standards</p>
<p>Training and Dissemination: To all Staff and other key stakeholders through the development of staff bulletins, Resilience Direct, the Trust Emergency Preparedness intranet site.</p>	
<p>To be read in conjunction with: OP 10 Trust Risk Management and Patient Safety Reporting Policy and associated Attachments and Procedures, HR01, HR02, HR07, HR13</p>	
<p>Initial Equality Impact Assessment (all policies): Completed Yes Full Equality Impact assessment (as required): Completed NA If you require this document in an alternative format e.g., larger print please contact Central Governance Department on Ext 85114</p>	
<p>Contact for Review</p>	<p>Head of EPRR & Business Continuity</p>
<p>Implementation plan / arrangements (Name implementation lead)</p>	<p>Head of Emergency Planning and Business Continuity</p>
<p>Monitoring arrangements and Committee</p>	<p>Review through Business Continuity Sub Group, Emergency Planning Group and Trust Management Committee.</p>
<p>Document summary / key issues covered: This document contains the Business Continuity Policy for The Royal Wolverhampton NHS Trust. It provides the strategic framework for the Trust’s business continuity arrangements. This document explores the strategies and operational arrangements required to allow the Trust to continue to provide its critical services during a major incident or an emergency situation in accordance with:</p> <ul style="list-style-type: none"> i. Legislative requirements and NHS England expectations; and ii. NHS recommended best practice in Business Continuity Management. 	

VALIDITY STATEMENT

This document is due for review on the latest date shown above. After this date, policy and process documents may become invalid. The electronic copy of this document is the only version that is maintained. Printed copies must not be relied upon to contain the latest updates and amendments.

Part B

Ratification Assurance Statement

Name of document: Business Continuity Management Policy

Name of author: Diane Preston

Job Title: Head of Emergency Planning & BC I, the above named author confirm that:

- The Strategy/Policy/Procedure/Guidelines (please delete) presented for ratification meet all legislative, best practice and other guidance issued and known to me at the time of development of the said document.
- I am not aware of any omissions to the said document, and I will bring to the attention of the Executive Director any information which may affect the validity of the document presented as soon as this becomes known.
- The document meets the requirements as outlined in the document entitled Governance of Trust wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines(OP01).
- The document meets the requirements of the NHSLA Risk Management Standards to achieve as a minimum level 2 compliance, where applicable.
- I have undertaken appropriate and thorough consultation on this document and I have detailed the names of those individuals who responded as part of the consultation within the document. I have also fed back to responders to the consultation on the changes made to the document following consultation.
- I will send the document and signed ratification checklist to the Policy Administrator for publication at my earliest opportunity following ratification.
- I will keep this document under review and ensure that it is reviewed prior to the review date.

Signature of Author:

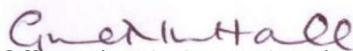
Date: 28 May 2021



Name of Person Ratifying this document (Chief Officer or Nominee):

Job Title: Chief Operating Officer/AEO

Signature:



I, the named Chief Officer (or their nominee) am responsible for the overall good governance and management of this document including its timely review and updates and confirming a new author should the current post-holder/author change.

To the person approving this document:

Please ensure this page has been completed correctly, then print, sign and email this page only to:
The Policy Administrator

IMPLEMENTATION PLAN

To be completed when submitted to the appropriate committee for consideration/approval

Policy number and policy version OP 104 v3	Policy Title Business Continuity Management	
Reviewing Group	Policy Group	Date reviewed: June 2021 (TBC)
Implementation lead: Diane Preston diane.preston@nhs.net		
Implementation Issue to be considered (add additional issues where necessary)	Action Summary	Action lead / s (Timescale for completion)
Strategy; Consider (if appropriate) 1. Development of a pocket guide of strategy aims for staff 2. Include responsibilities of staff in relation to strategy in pocket guide.		
Training; Consider 1. Mandatory training approval process 2. Completion of mandatory training form		
Development of Forms, leaflets etc; Consider 1. Any forms developed for use and retention within the clinical record MUST be approved by Health Records Group prior to roll out. 2. Type, quantity required, where they will be kept / accessed/stored when completed		
Strategy / Policy / Procedure communication; Consider 1. Key communication messages from the policy / procedure, who to and how?	To share with senior managers, BC plan owners, via intranet, email, staff bulletin	Head of EP with Communications Dept July 2021.
Financial cost implementation Consider Business case development		
Other specific Policy issues / actions as required e.g. Risks of failure to implement, gaps or barriers to implementation		