NHS
Cheshire and Wirral
Partnership
NHS Foundation Trust

Document level: (TW)
Code: EP1
Issue number: 1.01 2019

CWP Business Continuity Management System Policy and Procedures

Lead executive	Director of Operations
Authors details	Accountable Emergency Office – 01625 508542 Emergency Planning & Business Continuity Co-ordinator – 0300 303 4582

Type of document	Policy
Target audience	All CWP Staff
Document purpose	This policy defines the scope, purpose and responsibilities relating to the Business Continuity Management System (BCMS) and approach to Business Continuity adopted by CWP or the organisation.

Approving meeting	Emergency Planning Sub Committee	14th May 2019
Implementation date	May 2019	

CWP documents to be read in conjunction with	
HR6	Trust-wide learning and development requirements including the training needs analysis (TNA)
GR7	Major Incident Plan
GR12	Media Policy

Document change history	
What is different?	Transfer to new CWP Template
Appendices / electronic forms	None
What is the impact of change?	None

Training requirements	No- Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Kate Chapman (East), Glenda Bryan (Wirral), Sharon Vernon (West)
Corporate services	Performance & Redesign
External agencies	No

Financial resource implications	None

External references

1. Department of Health. NHS Emergency Planning Guidance 2005
2. Department of Health. NHS Resilience and Business Continuity Management Guidance 2008
3. Emergency Preparedness (statutory guidance on Part 1 of the CCA). http://www.ukresilience.co.uk

4. Healthcare Commission. Standards for Better Health
5. HM Government. Business Continuity Management Toolkit http://www.preparingforemergencies.gov.uk/
6. Sharp. J. The Route Map to Business Continuity Management. Meeting the requirements of BS 25999. BSI order ref: BIP 2142
7. The Civil Contingencies Act 2004. http://www.ukresilience.co.uk
8. ISO 22301 (2012)

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
N/A		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

Contents

1. Introduction

This policy defines the scope, purpose and responsibilities relating to the Business Continuity Management System (BCMS) and approach to Business Continuity adopted by Cheshire and Wirral Partnership NHS Foundation Trust hereafter referred to as CWP or the organisation. The following is to be read in conjunction with the CWP Major Incident Plan.

The Civil Contingencies Act (2004) and the Health and Social Care Act (2012) requires organisations, including Foundation Trusts, to have business continuity management system, to ensure that they can continue to deliver their critical functions in the event of an emergency. This organisation must ensure that it can mobilise the functions that it needs to deal with the emergency, minimise the impact on the day-to-day activity and maintain vital services for the community at an appropriate level. *Each NHS organisation is required to ensure they have in place robust mechanisms to enable them to plan for, and respond to, and recover from major incidents in conjunction with the command and control arrangements of the wider response community.*

The Business Continuity Management System (BCMS) establishes a strategic and operational framework to implement, proactively, an organisation's resilience to disruption, interruption, risk or loss in providing its services. BCMS requires planning across many facets of the organisation; therefore its resilience depends equally on its management and operational staff, as well as technology.

Implementation of this policy will ensure compliance with the statutory duties under the Civil Contingencies Act (2004), Health and Social Care Act (2012), relevant sections of the Essential Standards for Quality and Safety, comply with the Department of Health NHS Emergency Planning Guidance (2005) and ISO 22301 (2012)

1.1 Aim and Objectives

1.1.1 Aim

The aim of this Policy is to ensure that the framework is in place within the organisation to support an effective Business Continuity Management System.

1.1.2 Objectives

To set out how the Trust will meet statutory and no statutory obligations regarding BCM arrangements. The objectives of the CWP Business Continuity Management System Policy and Procedures are;

- Outline Business Continuity Management roles, responsibilities, competencies and authorities;
- To fully embed Business Continuity Management into the Trusts routine operations and management processes;
- Determine resources to establish, implement, operate and maintain the Business Continuity Management System;
- Provide a Business Continuity Management Structure through which;
  - A comprehensive BCM system is established and maintained;
  - Key services, together with their supporting critical activities, processes and resources, will be identified;
  - Business impact analysis and risk assessment will be applied to our key services and their supporting critical activities, processes and resources;
  - Risk mitigation strategies will be applied to reduce the impact of disruption or negative impact on delivery on key services;
  - Plans will be developed to ensure continuity of key services at a minimum acceptable standard following disruption and enable full restoration of services in the event of unavoidable interruption of those services;
  - Invocation of business continuity plans can be managed;
  - Plans are subject to ongoing exercising and revision;
  - Ensure that Business Continuity and the associated policies, standards, procedures and plans are embedded in the day to day operational activities and culture of the business;
  - The Board can be assured that the BCM system remains up to date and relevant.

1.2 Scope

This document will inform CWP staff, service users and key stakeholders of the coordinated approach to a business continuity management system. This policy will support each clinical and non-clinical/ corporate service to effectively respond and recover to a disruption to critical activity, and dependencies utilised by these services. This document assumes that each clinical and non-clinical/ corporate service will have local business continuity plans and that staff will be trained as appropriate.

1.3 Testing and Validation

This plan will be tested and validated through exercises developed as part of CWP's annual emergency planning training and exercising programme as approved and ratified by the Emergency Planning Sub Committee. Testing of the Business Continuity Management System will be consistent with the requirements set out in the CCA and the NHS England Emergency Preparedness, Resilience and Response Framework 2015 (EPRR) and evaluated for effectiveness by Business Continuity Leads.

The policy will be reviewed as necessary in light of learning from incidents, exercises and comments received. Learning will be captured in a Trust Evaluation and Feedback form documented in the form of a debrief report and approved by the Emergency Planning Sub Committee; the policy will be reviewed to capture any learning identified

1.4 Audit and amendment

The plan will be subject to on-going review and revision by the Emergency Planning Sub Committee. A formal review of the plan will be completed by the Emergency Planning Sub Committee in line with the agreed policy review date. Additional reviews may take place following the activation of the plan during exercises or live incidents and/ or significant organisational changes within CWP.

All amendments will be audited through the Emergency Planning Sub Committee and communicated to stakeholders as appropriate. Any amendments to the document will require both approval and ratification at the Emergency Planning Sub Committee and Document Quality Group respectively.

1.5 Debrief Reports

Following activation of the policy during exercises or live incidents a debrief report will be produced. The report will outline lessons identified, recommendations and actions to assess the response to an exercise scenario and/ or incident. The debrief report will be approved and ratified by the Emergency Planning Sub Committee and noted by the Operations Board where required.

1.6 Freedom of information

Release of information contained in this document should be considered with regard to Freedom of Information and Data Protection legislation;

Please contact cwp.foi@nhs.net with any queries.

2. Business Continuity Management (BCM)

2.1 Legislation

The Civil Contingencies Act 2004 places a statutory duty on the organisation to have Business Continuity Management arrangements in place. The Act requires the organisation to maintain plans to ensure that it can continue to exercise its functions in the event of an emergency so far as is reasonably practicable. The Act also states that the organisation must have regard to assessments of internal and external risks when developing and reviewing business continuity plans.

Plans must include a clear procedure for invoking the business continuity plan and must have arrangements in place for training and exercises to ensure that the plan is effective. All plans must be reviewed and kept up to date.

In addition, BCM is a requirement of the commissioning and associated performance management processes.

All NHS organisations are required to deliver their responsibilities as defined by the CCA 2004; this includes ensuring the contribution to multi agency planning frameworks of Local Resilience Forums. CWP is a CCA (2004) Category 2 responder with Category 1 responsibilities within Community Care Western Cheshire. The CCA (2004) outlines roles and responsibilities for each responding organisation including; leadership in the event of a major incident, with requirements to support other agencies being deemed good practice for individual organisations.

Duties under the CCA (2004);

- *Risk assess*
  Dynamically assess the local and national emergencies, threats, risks and hazards that CWP may face in response to an incident ensuring that plans are sound and proportionate to risks.

- *Make business continuity arrangements*
  Set the scope and strategy of the preparedness, response and recovery to business continuity incidents with a Business Continuity Management System Policy and Procedures, and CWP Strategic Business Continuity Plan.

- *Conduct emergency planning*
  Have an Emergency Planning Team under the direction of the CWP Emergency Planning Officer conduct emergency planning trust wide.

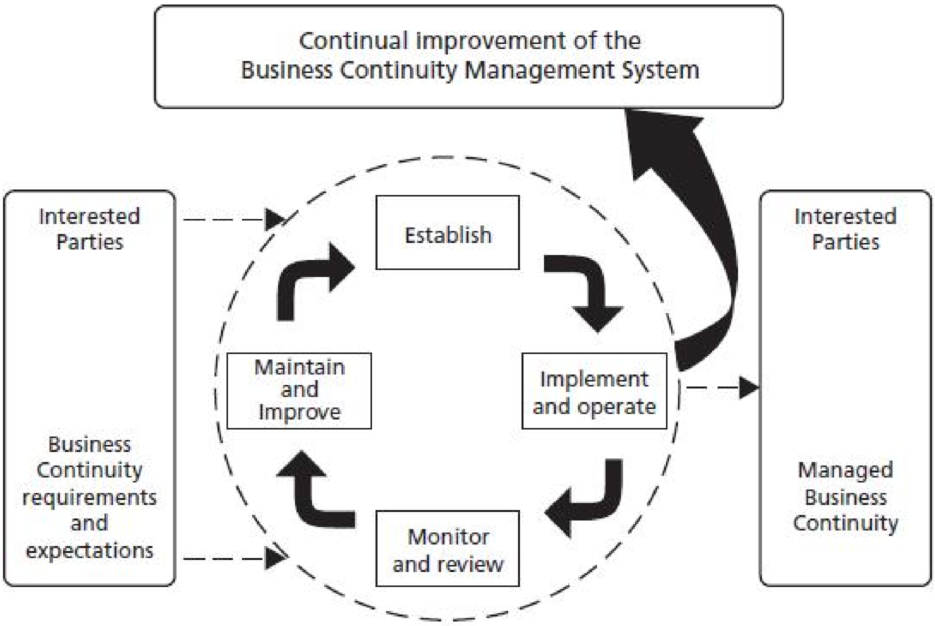
- *Inform, warn and advise the public*
  Inform, warn and advise in preparedness, response and recovery phases of an incident minimising the impact of the incident on staff, service users and stakeholders. Emergency planning communications strategies identify appropriate and effective ways of communicating before emergencies ensuring staff, service users and stakeholders are aware of the risks that CWP may face; having robust arrangements in place to communicate during an emergency including both verbal and non verbal communication methods; and having clear and concise strategies for working with the media in an emergency.

- *Cooperate in resilience activities*
  Maintain the legal duty to cooperate with local responders by sustaining relationships and networks with resilience partners to cooperate in resilience activities in Cheshire, Merseyside and Greater Manchester including but not limited to; training and exercising, and ensuring a resilient approach to preparedness, response and recovery in an emergency.

- *Share information*
  Share information with resilience partners as information sharing is the crucial element of emergency planning, underpinning all forms of cooperation. Through liaison with Cheshire, Merseyside and Greater Manchester partner organisations CWP has raised awareness of the emergencies, threats risks and hazards that the Trust may face. Ensuring that the Trusts emergency and business continuity plans are available in the public domain, and that plans comply with both the data protection act (1998) and freedom of information act (2000) is an essential part of conducting emergency planning.

Each individual NHS organisation must plan to respond and recover from incidents in which its own services may be overwhelmed. The organisation itself may be affected by its own internal incident or by an external incident that impairs the organisations ability to operate normally.

The NHS British Standard for Business Continuity International Standard for Business Continuity Management (ISO 22301) (2012) specifies requirements for setting up and managing an effective business continuity management system. The standard applies the plan-do-check-act cycle to *establish, implement, operate, monitor, exercise, maintain and improve the effectiveness of an organisations business continuity management system.*


Continual improvement of the Business Continuity Management System
Interested Parties
Business Continuity requirements and expectations
Establish
Implement and operate
Monitor and review
Maintain and Improve
Interested Parties
Managed Business Continuity

Plan, Do, Check, Act cycle ISO 22301

It is particularly important for NHS organisations to ensure that they are equipped to work as part of a multi-agency response across geographical boundaries, ensuring the ability to provide and to give mutual aid within the context of Local Resilience Forums (LRF) and their subgroups.

2.2 International Standards Organisation ISO 22301 Societal security – Business continuity management systems

The main guidance for business continuity management, which also applies to BCMS, is contained in: a. ISO 22301 Societal Security - Business Continuity Management Systems – Requirements1 b. ISO 22313 Societal Security - Business Continuity Management Systems – Guidance

2.3 Business Case for BCM

Although it is widely accepted that the protection of brand, reputation and image is paramount for any organisation, other, external drivers have greater influence over the introduction of BCM. Industry regulations and legal requirements are having an increasing impact in driving the establishment of BCM as are insurance companies' requirements.

Other significant drivers are corporate governance and auditors. Auditors will look for evidence of effective BCM being in place to meet regulations and legislation. The current approach is not just to see if plans exist but also to look for evidence that the plan has been rehearsed and that BCM has been promoted within the organisation. It makes sense to put BCM arrangements in place because they help to:

- Develop a clearer understanding of how the organisation works;
- Protect the community and organisation;
- Protect the reputation of the organisation;
- Produce clear cost benefits;
- Ensure compliance with the Civil Contingencies Act 2004 and corporate governance;
- Enable performance standards and key performance indicators to be maintained.

2.4 Benefits of BCM

If correctly introduced, BCM encourages greater staff involvement in the successful running of the organisation. By involving the people who actually do the job, it is possible to eliminate many of the lower level risks that can disrupt an organisation. It is often the frontline staff that can identify where weaknesses and single points of failure exist and how to improve processes and resilience.

Every organisation has a duty of care to its employees, clients, the community and the environment. BCM can be seen as part of a social responsibility agenda, helping to discharge these duties and maintaining employment throughout the period of disruption.

2.5 Definitions

Emergency Planning

Emergency Planning encompasses the planning and preparedness stages; consideration of the impacts of a major incident either external to the trust or internal, which may cause injury, loss of life, or a threat to the overall service provided by the trust; dealing with the impact of the emergency and the recovery phase of returning services to normal. The Major Incident Plan is in place to deal with such emergencies.

NHS Business Continuity Incident;

“A business continuity incident is an event or occurrence that disrupts, or might disrupt, 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. (This could be a surge in demand requiring resources to be temporarily redeployed)” (NHS EPRR Framework 2015).

Business Continuity;

Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at a predefined level.

Business Continuity Management;

A management process that helps manage the risks to the smooth running of an organisation or delivery of a service, ensuring that it can operate to the extent required in the event of a disruption.

For the NHS, BCM is defined as “the management process that enables an NHS organisation:

- To identify those key services (and functions) which, if interrupted for any reason, would have the greatest impact upon the community, the health economy and the organisation
- 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”

Business Continuity Plan;

Documented collection of procedures and information that is developed, compliant and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at a predefined level.

Business Impact Analysis;

Process of analysing business functions and the effort that a business disruption might have upon them.

Recovery Time Objectives (RTO);

Target time set for resumption of product/ service/ activity delivery after an incident. Note this has to be less than the maximum period of tolerable disruption.

Maximum Period of Tolerable Disruption (MTPD);

Duration after which an organisation's viability will be threatened if product/ service/ activity delivery cannot be resumed.

Major incident/emergency;

Any occurrence which presents a serious threat to the health of the community, disruption of the services or cause such numbers or types of casualties to require special arrangements to be implemented by hospitals, ambulance trusts or primary care services and health organisation.

Local Resilience Forum (LRF)
LRF's are multi-agency forums allowing responders to consult, collaborate and disclose information with each other to facilitate planning and response to emergencies.

Each LRF publishes a Community Risk Register, an assessment of the natural hazards and manmade threats that could affect the LRF area enabling organisations to ensure that their response and recovery plans are proportionate to the local risks it may face.

CWP services fall within Cheshire and Merseyside LRF boundaries, arrangements are in place to ensure a consistent and coordinated approach to any incident in any LRF area.

Audit
Systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving objectives.

Debrief
Debriefing is the process in which staff within or across organisations communicate their experience of how the Trust operated during training, exercise or incidents; so that lessons can be identified.

Recovery
Recovery is the process of rebuilding, restoring and rehabilitating the Trust following an emergency.

2.6 BCM Life Cycle

The BCM arrangements at CWP will align with the International Organisation Standard (ISO) for Business Continuity – ISO 22301, issued in 2012.
Thee BCM life cycle is a phased process using the Plan-Do-Check-Act cycle for developing the business continuity management system. These stages are as follows: Table 1 and diagram below shows the ISO 22301 'Plan, Do, Check, Act' (PDCA) cycle, as applied to the BCM processes.

Table 1: Explanation of PDCA Model

Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organisations overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review and determine and authorise actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the Business Continuity Management Systems (BCMS) by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Stage 1 – Understanding the organisation
The first stage in the process of creating an effective BCM is to fully assess the organisation needs and the current situation in order to determine the actions necessary to put together and maintain effective protection of the critical business services

Stage 2 –Determining BCM strategies

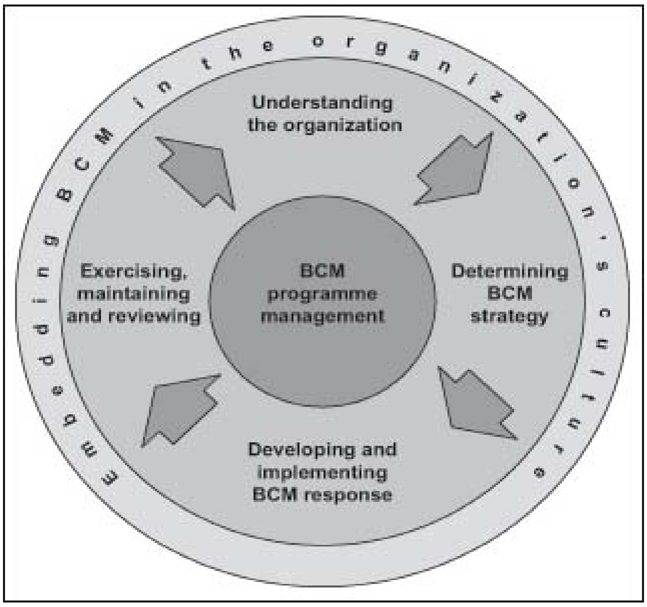
The second stage is to determine how the organisation will recover each critical activity within the specified recovery time; determine the allocation of resources; how to manage relationships with key stakeholders and continue to manage non-critical activities

Stage 3 – Developing and implementing a BCM response
The third stage is to develop and implement plans detailing how to manage the incident and how to maintain business continuity based on previously agreed timescales and levels of service

Stage 4 – Exercising, maintaining and auditing BCM
The fourth stage is to review and exercise the BCM arrangements by self-assessment and encouraging staff to continually look for improvements

Overall – BCM Programme Management and Building and Embedding a BCM culture
The overall process is to gain Board acceptance of the value of the BCM process and encourage a management approach which will raise awareness of and promote ownership of the BCM process.

The BCM model – the BCM Wheel below illustrates the life cycle. The hub (BCM programme management) and the tyre (embedding BCM in the organisation's culture) relate to Plan, Check and Act. The spokes – Understanding the organisation, Determining BCM Strategy, Developing and implementing BCM response and exercising, maintaining and reviewing) represent the Do element of the cycle.


Embedding BCM in the organization's culture
Understanding the organization
Determining BCM strategy
Developing and implementing BCM response
Exercising, maintaining and reviewing
BCM programme management

2.7 BCM Procedure

A separate BCM procedure has been drafted to ensure that BCP Leads have a process to follow. This is included in Section 4. When following the procedure, it is important to ensure that all plans are aligned with the organisation's vision, strategic goals and key priorities.

For further detailed procedures addressing: severe shortage of staff, loss of building, loss of data, key systems infrastructure failure, telecoms failure, threat to wellbeing of staff and disruption to the supply chain, please refer to the Business Continuity Plan template (Appendix 3) for Action Plans and Procedures.

3. Risk Assessment

The following risk assessment methodology will be used to understand the threats to services and departments within the Trust.

Levels of Likelihood of Impact

Level	Likelihood of Impact
1	Rare (1)
2	Unlikely (2)
3	Possible (3)
4	Likely (4)
5	Almost certain (5)

Levels of Impact

Risk Level	Risk Weighting	Actual or potential Event Consequences	Event detail / description
A RED	5	Catastrophic	– International / National adverse publicity – Severe loss of confidence in the organisation as a result of loss of servers/contracts – Death – Extensive injuries to patients and staff – Substantial disruption of service provision – Litigation – Substantial financial impact
B RED	4	Major	– National adverse publicity/Major loss of confidence in the organisation – Temporary service closure – Serious injury to patients and staff – Serious property damage – Litigation / major financial loss / cost
C AMBER	3	Moderate	– Local adverse publicity / moderate loss of confidence in the organisation – Medical treatment required – Reduced capacity to deliver service(s) – Litigation – High financial loss / cost – Minor disruption to service delivery
D GREEN	2	Low	– No medical treatment or intervention required as a result of injury – First Aid treatment delivered as a result of injury – Minimal or no disruption to service delivery – Litigation – Low-medium financial loss or cost
E GREEN	1	Minimal	– No service disruption – No injury – Minimal financial impact

Risk Rating Matrix

	Consequence				
LIKELIHOOD OF OCCURRENCE	**Catastrophic A (5)**	**Major B (4)**	**Moderate C(3)**	**Low D (2)**	**Minimal E (1)**
Almost certain (5)	25	20	15	10	5
Likely (4)	20	16	12	8	4
Possible (3)	15	12	9	6	3
Unlikely (2)	10	8	6	4	2
Rare (1)	5	4	3	2	1

Risk ratings of 16 or above will be captured on the Emergency Planning risk register, an overview maintained by the Emergency Planning Sub Committee and additional risk treatment measures put into place.

4. BCM Procedure and Actions for signposting and developing a BCP

There are five key stages to be followed to implementing BCM processes successfully into NHS organisations. This procedure and action plan has been developed for each stage to ensure the implementation of Business Continuity Management within the trust (see Appendix 1).

Stage 1: Programme Management

This enables the business continuity capability to be established and maintained in a manner appropriate to the size and complexity of the trust.

Action

1. Producing a Business Continuity Policy and ensure ratification through the usual procedure;
2. Achieving 'top down buy in' from Chief Executive and Executive Directors to introduce a Business Continuity Management Policy;
3. Establishing the scope of the programme;
4. Establishing how the programme will be financed and resourced;
5. Establishing a programme of awareness raising to embed within the culture of the organisation and through governance arrangements;
6. Developing a timetable for implementation with timescales for completion.

Stage 2: Understanding the business

CWP will be aware of its full range of services and determine the impact of a disruption to its key services by means of a Business Impact Analysis (BIA) and risk assessments. These will ensure the identification of critical services, evaluation of recovery priorities and the assessment of risks that could lead to a disruption of service.

Action

1. Each Service and Corporate Department to identify a Business Continuity Lead;
2. Business Continuity Leads to undertake appropriate training;
3. Each Service and Corporate Department to undertake a BIA for each activity (see Appendix 2);
4. BIAs are to be reviewed annually;
5. Each Service and Corporate Department to undertake a risk assessment of major threats to continuity of service (via corporate, Service and community risk registers);
6. Senior management sign off of the BIA and risk assessments for each Service and Corporate Department.

Stage 3: Determining the BCM strategies

Having identified the critical activities, processes and resources that support the key services of the organisation, completed the impact and risk assessments and agreed the recovery time objectives, together with the minimum level of service required, consideration must be given to how the services will continue.

Action

1. Each Service and Corporate Department to determine how it will recover each key service. This will include ensuring full availability of the service, recovery of the service within Recovery Time Objective (RTO) at an agreed minimum level or suspension of the service;
2. Determining how relationships with key stakeholders will be managed at the time of disruption;
3. Agreeing the incident response structure to be developed and implemented in the event of a disruptive event;
4. Determining how the restoration of suspended services is implemented;
5. Senior management sign off of the BCM strategies.

Stage 4: Developing and implementing a BCM response

By completing the processes in stages 1 to 3, the trust will be able to develop realistic and appropriate business continuity plans:

1. Develop a Business Continuity Plan template (see Appendix 3);
2. Business Continuity Plans are to be reviewed 2 yearly;
3. Business Continuity Plans to be developed for each Service/Unit and Corporate Department;
4. Strategic Business Continuity Plan to be developed for the organisation;
5. Ensure all staff are aware of their role in the event of a disruption to service;
6. Ensure all other stakeholders are aware of the plans and their role.

Stage 5: Exercising, maintaining and reviewing

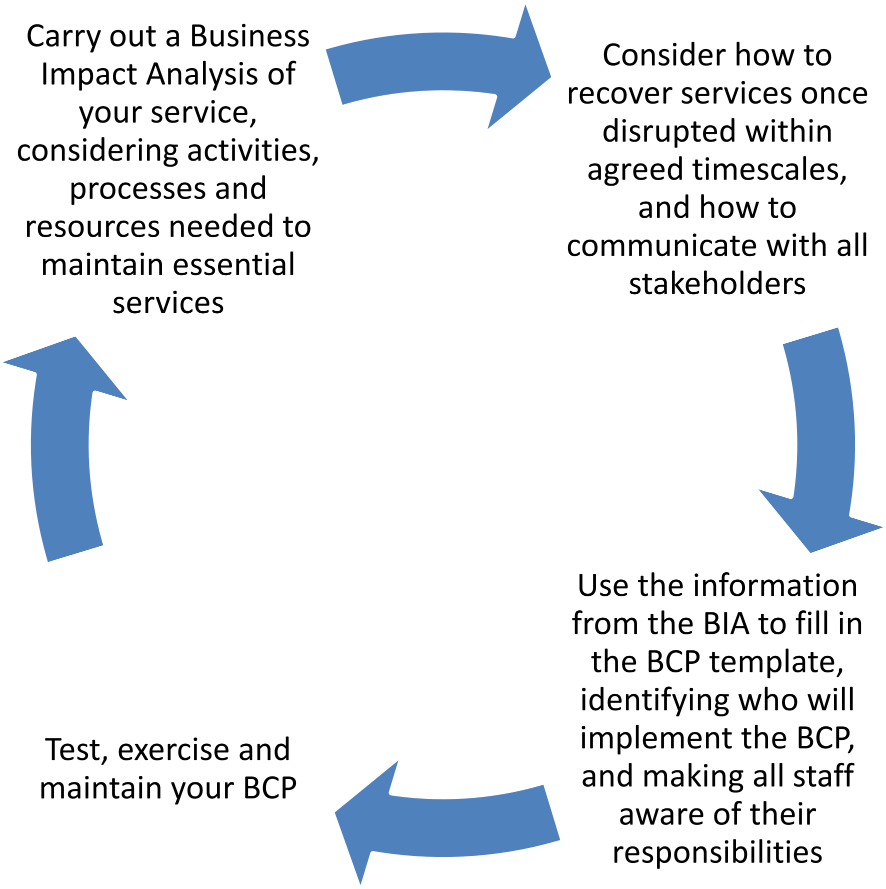
The exercising of plans is essential to ensure that the plan is robust. Exercises should not ‘risk’ the trust by causing disruptions; they must be practical and cost effective, be appropriate to the trust and designed to build confidence in the plan. It is important that all plans are maintained regularly to take account of any changes and that they are reviewed to ensure that they continue to be suitable, adequate and effective.

Action

1. Design an exercise programme to ensure plans can be tested;
2. Identify lessons learned from exercises and incidents and develop action plans to implement improvements;
3. Review plans on a regular basis to ensure that any changes are taken account of
4. Communicate any changes to staff and stakeholders;
5. Audit of plans to be undertaken on a regular basis.

How to write a BCP Stages 2-5.

5.



Carry out a Business Impact Analysis of your service, considering activities, processes and resources needed to maintain essential services

Consider how to recover services once disrupted within agreed timescales, and how to communicate with all stakeholders

Use the information from the BIA to fill in the BCP template, identifying who will implement the BCP, and making all staff aware of their responsibilities

Test, exercise and maintain your BCP

Preventive and Corrective Actions

The Trust will improve the Business Continuity Management System through the application of preventative and corrective actions.

Preventative and corrective actions are to be documented in.

5.1 Preventive Actions

The Emergency Planning Sub Committee (EPSC) will take action to guard against potential nonconformities in order to prevent their occurrence documenting the following;

- Potential nonconformities and their causes;
- Determining and implementing preventive action needed;
- Recording results of action taken;
- Reviewing preventive action taken;
- Identifying changed risks and ensuring that attention is focused on significantly changed risks;
- Ensuring that all those who need to know are informed of the nonconformity and preventive action put in place;
- The priority of preventive actions based on the results of the BIA.

5.2 Corrective Actions

The Emergency Planning Sub Committee (EPSC) will take action to eliminate the cause of nonconformities associated with the implementation of BCMS in order to prevent their recurrence documenting the following;

- Identifying the nonconformities
- Determining the causes of non conformities
- Evaluating the need for actions to ensure that nonconformities do not recur;
- Determining and implementing corrective action needed;

- Recoding the results of action taken;
- Reviewing corrective action taken.

6. Ratification Process

The process for consultation, approval and ratification of Business Continuity Plans has been approved by the Emergency Planning Sub-Committee. A copy of the approval and ratification process can be found in Appendix 6.

7. Implementation

The Emergency Planning Officer is responsible for making sure that awareness is raised regarding the policy once it has been ratified. Implementation will involve discussion at team meetings and briefing sessions will be organised for Business Continuity Plan Leads who will be responsible for ensuring the implementation of this policy locally within each service and department.

8. Procedures for monitoring compliance and effectiveness

The Emergency Planning Sub Committee (EPSC) will be responsible for monitoring and reviewing the effectiveness of this policy and its deployment across the organisation.

Each Service/unit and department will be responsible for writing, approving and implementing BCPs locally. Plans must be approved by the corporate governance structure locally by the appropriate General Manager and local emergency planning group before being sent to the EPSC to be filed centrally and uploaded onto the emergency planning intranet page (see Appendix 6).

Furthermore, the EPSC will manage a rolling programme of quality checking local BCPs to monitor and review their quality, to ensure compliance with this policy and to offer assurances to employees, stakeholders and partner agencies that the Trust is resilient and able to maintain essential services.

Monitoring will also include an evaluation of BCP Leads' activity, and the workplan and arrangements undertaken by them to comply with this policy. This will be reported to the EPSC on an annual basis and to the Operations Board in the Emergency Planning annual report.

In the event that improvements are required, this will be escalated to the Emergency Planning Officer to ensure that corrective action is taken. Any nonconformity with this policy will be escalated and reported through the Operations Board and added to the risk register if unresolved.

Any learning from exercises and incidents will be formally reported to the EPSC by means of a debrief report to enable lessons learned to be disseminated across the Trust (Appendix 4).

9. Key Performance Indicators (KPIs)

There are a number of key performance indicators which will help to provide assurance that the policy has been implemented effectively. These KPIs include:

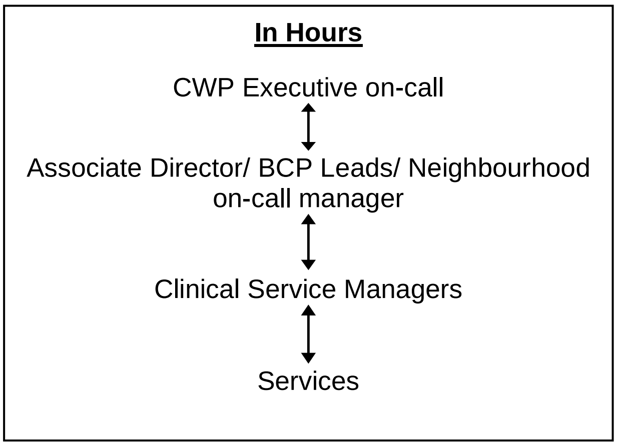
- BCP Leads to be nominated by each Service and Corporate Department;
- Awareness sessions for all BCP Leads to be undertaken;
- Business Impact Analysis undertaken by all Services and Corporate Departments and Mission Critical Activities identified for each;
- Development of BCPs for each Service and Corporate Department;
- Development of Strategic Business Continuity Plan;
- Exercises to be undertaken to test BCPs and Strategic BCP.

10. Business Continuity Incident Response

Staff are advised to refer to the Trust Major Incident Plan for further information on emergency command control structures.

On activation of this plan, command and control arrangements will be activated.

10.1 Internal Command and Control



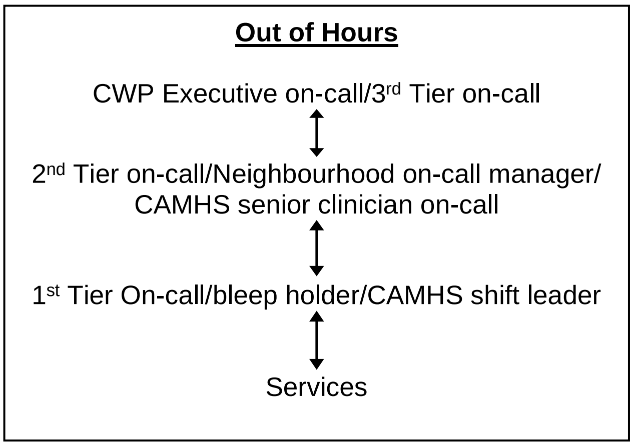
In Hours

CWP Executive on-call

Associate Director/ BCP Leads/ Neighbourhood on-call manager

Clinical Service Managers

Services



Out of Hours

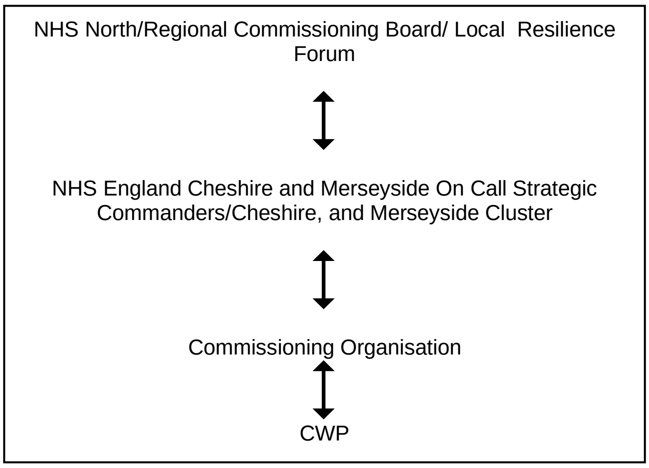
CWP Executive on-call/3rd Tier on-call

2nd Tier on-call/Neighbourhood on-call manager/ CAMHS senior clinician on-call

1st Tier On-call/bleep holder/CAMHS shift leader

Services

10.2 External Command and Control



NHS North/Regional Commissioning Board/ Local Resilience Forum

NHS England Cheshire and Merseyside On Call Strategic Commanders/Cheshire, and Merseyside Cluster

Commissioning Organisation

CWP

11. Roles and responsibilities

This section identifies the groups, or individuals having specific roles with respect to this Business Continuity Policy; determining resources to establish, implement, operate and maintain the Business Continuity Management System.

11.1 Chief Executive and Executive Team

The Chief Executive has overall responsibility for ensuring that the organisation complies with the statutory duties under the Civil Contingencies Act 2004 and complies with other associated Business Continuity legislation.

All members of the Executive Team have a responsibility to be familiar with the Business Continuity Policy and to ensure that BCM becomes part of the everyday culture for the organisation. The Executive Team will also ensure that contracts with suppliers of critical goods and services must include a requirement for the suppliers' business continuity processes to be approved and exercised to the satisfaction of this organisation.

The Chief Executive is responsible for nominating spokespersons and approving press releases, statements and stories to be used in media handling.

The CWP Executive On-call is responsible for;

- Activating the arrangements within the Business Continuity Management System;
- Confirm Major Incident stand down where required;
- Emergency response and recovery on activation of this plan;
- Confirming the nature and extend of a Trust wide business continuity incident;

- Activating a major incident team to support response and recovery.

11.2 Director of Operations

The lead Director for Emergency Planning, supported by the Executive Team, must ensure that the policy is implemented and to nominate a responsible officer, to be known as the Emergency Planning Officer, and adequate resources from within the organisation to ensure that business continuity plans are developed. The lead Director for Emergency Planning is to be accountable for Business Continuity Management policy and implementation Trust wide.

11.3 Emergency Planning Coordinator

The Emergency Planning Coordinator leads on the development of Emergency Planning and Business Continuity Planning and is supported by the Emergency Planning Sub-Committee to ensure that emergency preparedness and business continuity arrangements are in place and are robust across Services and Corporate Services.

The Emergency Planning Officer and Emergency Planning Sub-Committee are responsible for:

- Developing, implementing and maintaining the Business Continuity Management System;
- Developing, reviewing and updating this Policy in line with statutory, legislative and best practice guidance;
- Developing, reviewing and updating the Strategic Business Continuity Plan and its distribution;
- Ensuring that the organisation complies with the statutory duties under the Civil Contingencies Act 2004 and the good practice guidance Department of Health Emergency Planning Guidance 2005;
- Ensure that key performance indicators are set and are met;
- Highlight any areas of concern relating to business continuity to the Operations Board;
- Providing leadership, advice and training to all Business Continuity Leads;
- Co-ordinating the development and implementation of action plans to address points of vulnerability identified by the risk assessment process;
- Ensuring that suppliers have the required business continuity arrangements in place;
- Ensuring that training of key staff is undertaken;
- Ensuring that a programme of business continuity exercises is developed and undertaken on an annual basis;
- Conducting adequate risk assessments to the infrastructure operations of the organisation;
- Responsible for defining and executing policy regarding Crisis Management of Incidents and Situations impacting Infrastructure Operations.

11.4 Business Continuity Planning Leads and deputies

Each Service and Corporate Department must have a designated Business Continuity Planning Lead (BCP Lead). It is suggested that each BCP Lead will have one day per month protected for Emergency Planning work. Each BCP Lead will be responsible for the following:

- Attend CWP Emergency Planning Sub Committee meetings;
- Ensuring that risk assessments and business impact analysis are undertaken for each service and risks entered onto the organisational/departmental risk register;
- Attend emergency planning and business continuity training annually to maintain a level of competence;
- Ensuring that the training of key staff within each Department is undertaken, including giving a documented localised induction to staff involved in the BCM process;
- Completing the Business Continuity Plan template and ensuring that it is reviewed 2 yearly or following any major change; is tested and maintained;
- Cascading Business Continuity information to staff where required;
- Collating information on behalf of each respective department in order to complete business continuity incident debriefs as required;
- Responding to requests for information from the major incident team;
- Activating local Business Continuity arrangements;

- Ensuring that staff are aware of the need to escalate to the appropriate on-call Manager in the event of any disruption to service and that a report incorporating lessons learned is completed and forwarded to the Emergency Planning Team within a week of the event. (See Appendix 4).

11.5 Associate Directors

Associate Directors are responsible for the following:

- Overall ownership and co-ordination of crisis management and business operational recovery for the relevant Service;
- Plan maintenance, policy, review and testing activities relevant to the Service, together with BCP Lead;
- Implementing the BCP in response to incidents affecting the Service, together with BCP Lead;
- Ensuring that the BCP Lead has a suggested minimum of one day per month protected time for Emergency Planning work, for some services, to be agreed within the PDP and to be reviewed annually;
- Ensuring all relevant departments within the Service are able to discharge their individual responsibilities to normal service levels.

11.6 Heads of Operations

Each Care Group is managed by a Head of Operations who is responsible for the following:

- Defining, communicating and implementing policy to ensure resilience of service provision against potential threats to normal service;
- Defining the operational response to an incident;
- Minimising the impact and duration of an incident affecting the service;
- Ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal service following all anticipated business disruptions;
- Communicating policy and plans with existing employees together with Line Managers during supervision;
- Policy and plans to be highlighted during local induction for all new employees by the relevant manager.

11.7 Director of Finance

The Director of Finance is responsible for the following:

- Outline a process for authorising additional expenditure in an emergency;
- Ownership and responsibility for ensuring that revenue-generating and cash collection activities are maintained at the normal level in the face of threats;
- Establishing effective Business Continuity Planning to combat threats to these operations, so as to reduce, or remove the impact and/or duration of such threats;
- Ensuring the people, processes and technology required are in place to maintain normal services for revenue and cash generation;
- Defining and executing policy of managed communication with customers and prospects, in the event of a threat, incident, or situation deemed to require it;
- Defining, communicating and implementing policy to ensure resilience of Finance activities against potential threats to normal service;
- Defining the operational response to an incident in this service;
- Minimising the impact and duration of an incident affecting this service;
- Ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal service following all anticipated business disruptions;
- Establishing and maintaining necessary arrangements to enable financial commitments to be met in a situation;
- Re-negotiating financial facilities and arrangements as necessary to minimise the effects of the situation on the organisation;
- Managing all exceptional financial transactions during a situation, including all insurance and banking matters arising.

11.8 Director of Organisational Development and People Services

The Associate Director of Workforce is responsible for the following:

- Defining, communicating and implementing policy to ensure resilience of Human Resources activities against potential threats to normal service;
- Defining the operational response to an incident in this area;
- Minimising the impact and duration of an incident affecting the service;
- Ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal service following all anticipated business disruptions;
- Ensuring the welfare needs of staff are met during a situation;
- Sourcing interim or replacement staff as appropriate to the situation.
-

11.9 Associate Director of Communications

The Head of Communications is responsible for the following:

- Providing a nominated spokesperson;
- Providing press releases, statements and stories to be used in media handling to the Chief Executive;
- Ensuring staff, service users and other stakeholders are informed of situations, as directed by the Major Incident Management Team;
- Notifying stakeholders when normal services will be/has been restored and what (if anything) will be done to avoid the same scenario happening in the future;
- Defining key messages for staff, service users and partners.

11.10 ICT Services

ICT Services are responsible for the following:

- Defining, communicating and implementing policy to ensure resilience of Information and Communications Technology (ICT) activities against potential threats to normal service;
- Defining the operational response to an incident in this area;
- Minimising the impact and duration of an incident affecting the service;
- Ensuring effective operational practices are in place and well-rehearsed to ensure swift restoration of normal service following all anticipated business disruptions;
- Ownership of all policy, plans and activities to ensure the staff can follow required processes using suitable technology and infrastructure to maintain and recover normal service for the organisation;
- Minimise potential threats and impact of those threats to the organisation through technical operations, including those arising from infrastructure, staff and suppliers, as well as other external threats;
- Providing all necessary enabling technical facilities to allow staff to be productively employed as soon as possible, in the event of an incident, or situation;
- Ensuring all reasonable precautions are in place to protect staff in technical operations, in accordance with prevailing Health and Safety legislation and published best practice;
- Ensuring all necessary plans, processes and technology are in place to minimise the likelihood of a threat to the organisation, through loss, or underperformance of a supplier to technical operations;
- Ensuring effective and timely communications with key suppliers before, during and after incidents and situations;
- Engage necessary support from suppliers before, during and after incidents and situations to minimise their impact and duration.

11.11 All Employees

- All employees should be familiar with the Business Continuity Policy and must be aware of the plans that affect their service and their role following invocation of the business continuity plan;

- Understand the importance of meeting Business Continuity Management objectives, confirming to the policy and continual improvement;
- Communication with existing employees will be by the Clinical Service Manager and Line Managers via supervision;
- Policy and plans will be highlighted during local induction for all new employees by the relevant manager;
- Any staff who are sub-contracted; bank or agency workers; volunteers; trainee students etc. (NB this list is not exhaustive) will be supported to comply with the policy and plans by the relevant manager.

12. Communications and Engagement

The main aim of the Communications Team is to ensure information is clear, reliable, timely and reaches all intended recipients Trust wide.

In order to achieve this high level of communications, the communications team will work closely with the emergency planning sub committee, major incident team and business continuity leads during incident response, proactively agreeing a strategy for effectively communicating with staff, service users and other key stakeholders that will follow national, regional and local communications guidelines.

CWP will have pre-planned messages for internal and external distribution. The following communications methods will be utilised in the event of a disruption to road fuel supplies;

- CWPEssential – weekly e-newsletter
- CWP communications bulletins – urgent daily emails if necessary
- CWPeople – quarterly printed staff newsletter
- CEO blog – fortnightly
- CWP Fuel intranet page
- CWP internet
- Social networking sites including @cwpnhs twitter account
- Emails direct to Trust BCP leads

Media handling

Any direct Trust media contact however will be managed as part of the Trust's Media Policy.

Appendix 1 - Workplan for Business Continuity Management System

Stage No	Action Required (give detail)	Responsibility	Timeframe	Progress Update	Current Status
1	Maintain a Business Continuity Policy and ensure ratification through the usual procedure.	EPSC			
1	Achieve ‘top down buy in’ from Chief Executive and Executive Directors to introduce a Business Continuity Management Policy.	EPSC			
1	Establish and maintain the scope of the programme	EPSC			
1	Establish and maintain how the programme will be financed and resourced.	EPSC			
1	Establish and maintain a programme of awareness raising to embed within the culture of the organisation and through governance arrangements.	EPSC			
2	Each Service and Corporate Department to identify a Business Continuity Lead.	EPSC			
2	Business Continuity Leads to undertake appropriate training and continued professional development.	All			
2	Each Service and Corporate Department to review and maintain a BIA for each activity.	All			
2	Each Service and Corporate Department to review and maintain a risk assessment of major threats to continuity of service (via corporate, Service and community risk registers).	All			
2	Senior management sign off of the BIA and risk assessments for each Service and Corporate Department.	Board			
3	Each Service and Corporate Department to determine how it will recover each key service. This will include ensuring full availability of the service, recovery of the service within Recovery Time Objective (RTO) at an agreed minimum level or suspension of the service	All			
3	Determining how relationships with key stakeholders will be managed at the time of disruption.	All			
3	Agreeing the incident response structure to be developed and implemented in the event of a disruptive event.	All			
3	Determine and maintain how the restoration of suspended services is implemented.	All			
3	Senior management sign off of the BCM strategies.	Board			
4	Develop, maintain and review a Business Continuity Plan template.	EPSC			

4	Business Continuity Plans to be developed for each Service/Unit and Corporate Department.	All			
4	Strategic Business Continuity Plan to be reviewed.	EPSC			
4	Ensure all staff are aware of their role in the event of a disruption to service.	BCP Leads			
4	Ensure all other stakeholders are aware of the plans and their role.	BCP Leads			
5	Maintain a training and exercise programme to ensure plans can be tested.	BCP Leads and Local Groups			
5	Identify lessons from exercises and incidents and develop action plans to implement improvements.	BCP Leads and Local Groups			
5	Review plans on a regular basis to ensure that any changes are taken account of.	Local Groups and EPSC			
5	Communicate any changes to staff and stakeholders.	BCP Leads			
5	Audit of plans to be undertaken on a regular basis.	EPSC			

Green - Target achieved or assurance completed. Plan expected to deliver desired outcome within timescale without further resource or re-planning. Measures fall within agreed tolerances (acceptable levels of risk - Risk rating 1-5) which can be dealt with at workstream / group level.

Amber -Target or assurance requires intervention for achievement or a measure has temporarily deviated outside tolerance limits. Remedial plan is in place or will be initiated through governance structure (moderate level of risk - Risk rating 6-14) which must be dealt with at sub-committee level.

Red - Target missed or assurance not available within timescale, or intervention on amber traffic light not achieving planned improvement. Significant risk of failure (high levels of risk - Risk rating 15-25) which must be dealt with at committee and therefore executive level- decision will be made regarding elevation to Trust Board.

Appendix 2 - Business Impact Analysis (BIA)

Date of BIA	
Service / Unit / Department / Team	
Version number and type	*(e.g. draft, final etc)*
Responsible offices	
Date of BIA Review	

Details of Staff Involved in BIA Process:

Name	**Role**	**Email**

Are any changes expected in the service that might impact on the BIA data?		**Yes / No** **If Yes, please give further details**	
Name and title of officer signing off BIA:			
Signature		**Date**	

Assessment of essential activities

Service / unit / department	
Essential service activity consider also access	
Is the service a statutory requirement?	
Minimum resources required e.g. staff / critical information / documentation	
List of minimum equipment requirements e.g. beds and linen, PCs / lap tops / printers / photocopier.	
Accommodation required: e.g. office space / car parking	
Do you have an up to date contact list of your staff? Where is it kept?	
What alternative accommodation have you identified?	
Can any of your staff work from home, have you considered implications?	

Who and what do you depend upon to deliver your essential services?	**What do they deliver?**

Single point of failure of service

Are there any **'single points of failure'** for your service which will require adequate contingency measures to be put in place, e.g. **processes; activities; key personnel or equipment**

Name of Activity	**Carried out by (job role)**	**Resource e.g. specially trained staff, a supplier, a piece of equipment etc which your service depends on in order to operate**	**Back up arrangements in place (state whether formal or informal)**	**Suggestions for improving resilience**

Key timed deliverables

There may be aspects of your service that are essential and **must** be delivered; these functions may also be more crucial at certain times of the month/year etc. Please indicate below where there are any such requirements. This helps identify where you might want to see recovery priorities focused and/or changed in your BC plan.

Examples might include where there is a statutory duty for you to deliver a service or an activity that only takes place at a certain time of year and to **not** deliver these duties would create a serious issue for your service to cope with.

Key Deliverable e.g. Financial month/year end 7 Day Follow-Up (contract data) **Mental Health Act considerations** **Payroll**	**Activity responsible for key deliverable**	**Day and Time Due**	**Impact if <u>not</u> delivered (Low/Medium/High + rationale)**

Business Impact Analysis

For the Business Impact Analysis on the following pages please consider:

- Types of threat, including fire, power cut, flood, loss of data/IT systems or telecoms failure, industrial action. Please consider the **likelihood of the impact** of occurring;
- Non-financial and financial impacts such as: security and safety; service user impact; staff morale; legal issues; regulatory impact; loss of reputation; loss of operational capacity; loss of revenue; bad debts; additional costs; input on cash flows. Please consider the **level of impact.**

Table 1 Levels of Likelihood of Impact

Level	Likelihood of Impact
1	Rare (1)
2	Unlikely (2)
3	Possible (3)
4	Likely (4)
5	Almost certain (5)

Table 2 Levels of Impact

Risk Level	Risk Weighting	Actual or potential Event Consequences	Event detail / description
A RED	5	Catastrophic	– International / National adverse publicity – Severe loss of confidence in the organisation as a result of loss of servers/contracts – Death – Extensive injuries to patients and staff – Substantial disruption of service provision – Litigation – Substantial financial impact
B RED	4	Major	– National adverse publicity/Major loss of confidence in the organisation – Temporary service closure – Serious injury to patients and staff – Serious property damage – Litigation / major financial loss / cost
C AMBER	3	Moderate	– Local adverse publicity / moderate loss of confidence in the organisation – Medical treatment required – Reduced capacity to deliver service(s) – Litigation – High financial loss / cost – Minor disruption to service delivery
D GREEN	2	Low	– No medical treatment or intervention required as a result of injury – First Aid treatment delivered as a result of injury – Minimal or no disruption to service delivery – Litigation – Low-medium financial loss or cost
E GREEN	1	Minimal	– No service disruption – No injury – Minimal financial impact

Table 3 Risk Rating Matrix

	Consequence				
LIKELIHOOD OF OCCURRENCE	**Catastrophic A (5)**	**Major B (4)**	**Moderate C(3)**	**Low D (2)**	**Minimal E (1)**
Almost certain (5)	25	20	15	10	5
Likely (4)	20	16	12	8	4
Possible (3)	15	12	9	6	3
Unlikely (2)	10	8	6	4	2
Rare (1)	5	4	3	2	1

Use this scale to allocate a priority to each activity / function

Recovery Priority Scale

Priority 1 Very High	Services must be provided as soon as practicable or will definitely result in loss of life, infrastructure destruction, loss of confidence or significant financial impact These services normally require continuation within 0 – 24 hours.
Priority 2 High	Services must be provided within 1 – 3 days or will likely result in infrastructure destruction, loss of confidence or financial impact with disproportionate recovery costs.
Priority 3 Medium	Services must be resumed within 4 – 14 days or could result in loss of confidence, considerable loss, further destruction or disproportionate recovery costs

Business Impact Analysis

List in order of priority your service's ***main functions*** and the implications in the short and long term if they were disrupted

Priority Level	Service Main Functions	Impact / Implications *(e.g. stakeholders / vulnerable groups)*	Loss of staff			Loss of workspace			Loss of ICT			Loss of equipment			Loss of critical data			Loss of supplies/ supply chain issues			Maximum Period of Tolerable Disruption
			Likelihood of Impact	Level of Impact	Risk Score	Likelihood of Impact	Level of Impact	Risk Score	Likelihood of Impact	Level of Impact	Risk Score	Likelihood of Impact	Level of Impact	Risk Score	Likelihood of Impact	Level of Impact	Risk Score	Likelihood of Impact	Level of Impact	Risk Score	What is the maximum length of time after which the viability of your service will be irrevocably threatened if services cannot be resumed? *NB this must be longer than the RTO*
1, to be restored within 0-3 hours (Recovery time objective) Very High																					
2, to be restored within 4-24 hours (Recovery time objective) Very High																					

3, to be restored within 3 days (Recovery time objective) High																					
4, to be restored within 14 days (Recovery time objective) Medium																					

Minimising Risks

Using the business impact analysis and the risk register data, describe how you will mitigate against the risks you have identified.

Priority 1

Core Activity Priority 1 – Restored within 0-3 hours	Risk Analysis Score	Minimising Risk Measures

Priority 2

Core Activity Priority 2 – Restored within 4-24 hours	Risk Analysis Score	Minimising Risk Measures

Priority 3

Core Activity Priority 3 – Restored within 3 days	Risk Analysis Score	Minimising Risk Measures

Priority 4

Core Activity Priority 4 – Restored within 14 days	Risk Analysis Score	Minimising Risk Measures

Risk assessment and the Risk Register
The purpose of this section is to link business continuity planning and the impact assessment and risks you have identified and scored with existing risk management systems e.g. local risk registers and trust risk register.

Do any risks present a business continuity issue?

High Risks 16 and above: List the risks that have been identified as high for your service/department and how these have been managed or treated

Description of risk	**Details of how the risk has been managed/treated**

Existing Business Continuity Planning

What is the current position with business continuity planning in your service?
(e.g. plan up to date, needs revision etc)

Describe the current position with Business Continuity Plan testing/exercising in your service?
(E.g. date plan test carried out, recommendations implemented etc)

ICT Programmes to be restored as a priority
Please contact Servicedesk on 0300 303 8182 for all matters relating to ICT.

Priority Application e.g. Electronic patient record, Microsoft Outlook, Telephone network, Fax, ESR, Datix	Hours needed e.g. 24/7, Monday-Friday 9-5	Priority rating 1 very high, 2 high, 3 medium

Action plan

Number	**Recommendation**	**Actioned by whom**	**Actioned by when**	**Open/ Closed/ Ongoing**

Once your BIA has been completed, senior management should be involved in reviewing the BIA within a specific timescale.

- Any excesses are moderated e.g. 'under-selling' or 'over-selling' certain functions in terms of their importance;

- Relative priorities are considered;
- A priority list for the whole organisation is agreed;
- A timetable for Business Continuity Planning can be produced.

In the ‘sign-off’ stage of the BIA, both IT and Estates requirements should also be discussed i.e. the required timescales for recovery of key IT systems/alternative accommodation arrangements. Both the organisation and the IT provider need to have a clear understanding of timescales and expectations so that a mutual agreement can be developed.

Resource planning prompt sheet

Continuity Planning Prompt Sheet	
For each of the following resource categories identify where they can be sourced from elsewhere within the business stream, elsewhere within the Trust and from outside of the Trust, a number of prompt questions are given within each category to assist with that analysis.	
People	• What skills and qualifications are required to carry out the job? • Are any specific qualifications or attributes are needed? • Is any formal training or other checks needed (e.g. CRB check)?
Equipment	• What equipment that is needed to carry out the service element? • Why is the equipment needed? • What purpose does it serve? • What is the impact of not having access to the equipment?
Environment	• What sort of physical environment is needed to provide the service element? • How long can the service element be provided from an alternative location? • Would any restrictions apply if the service element was provided from another location? • Are there any specific requirements needed for the physical location (e.g. security, access, capacity etc)? • What risks are associated with providing the service element from another location?
Materials	• What materials are used when providing the service element? • Why are those materials used? • Are there any special handling or storage requirements when using those materials? • What risks exist if the materials are not available?
Methods	• What working methods are used to provide the service element? • Why are those particular working methods used? • Could other working methods be used? • What risks are associated with changing working methods/practices for service element delivery? • What impact would changing working methods have upon the situation?

Appendix 3 - Business Continuity Plan (BCP) template
Business Continuity Plan (BCP)

The business continuity plan for	

Version	
Ratified by	
Date ratified	
Author(s)	
Responsible committee / officers	
Date issue	
Review date	
Intended audience	
Impact assessed	
Emergency Planning Lead	

Further information about this document

Document name	
Author(s) - Contact(s) for further information about this document	
This document should be read in conjunction with	CWP Major Incident Plan CWP Strategic Business Continuity Plan Individual business impact analysis

Version Control

Version History		
Version Number	Reviewing Committee / Officer	Date
	General Manager / Members of the Emergency Planning Sub- Committee	

Introduction

Business continuity

In the event of any major disruption to the Trust's internal function, it is essential that business continuity is maintained and that contingency plans are activated. The following events may threaten the business continuity of the Trust (this list is not exhaustive):

- **Loss of staff**; for example, staff sickness, lottery syndicate, industrial action
- **Loss of workspace**; for example, fire, evacuation of buildings, terrorism/hostage situation/security incident/bomb threat, adverse weather events including flooding
- **Loss of ICT, telephony & critical data**; for example, ICT failure, communications breakdown – systems telephones/ computer/ bleep, cyber attack, loss of access to patient records
- **Loss of equipment and supplies/ supply chain issues**; for example, medical equipment failure, for example, utility failure/ shortage, disruption to road fuel supplies

Each Trust service needs to establish individual contingency plans which detail arrangements for maintaining each of the services in the event of major disruption.

Name of ward / department
Location
Role of ward / department

If you need to invoke your Business Continuity Plan:
You should consider who needs to be informed of this. As a starting point, the following teams, areas, third parties etc. should be contacted as soon as possible based upon you assessment of the incident and the impact:

- If it is an IT or facilities / estates outage then the relevant Service desk
- Line Management – as a minimum, your Clinical Service Manager
- Locality Emergency Planning Lead (either West, Central and East or Wirral)
- The Communications Team based in Redesmere – *it is important that other areas in CWP are aware of the outage asap*
- Other CWP teams or areas who rely on you / or you rely on them to help you provide services
- Third Parties – external organisations/ suppliers / other Hospital Trusts etc.
- The Emergency Planning team

Note: your Business Continuity Plan should include these details.

If your service is provided from a number of locations it may be relatively simple for you to identify an alternative temporary location within your own service area. Possible alternatives will be identified through the production of your business continuity plans.

Thought now needs to be given to:

- How continuity of highly critical functions can be protected;
- How quickly less critical functions can be resumed;
- Where possible, through which other means can services temporarily be provided;
- Recording the arrangements made that will facilitate the above;
- A method to ensure that records are updated.

For planning purposes, it may be helpful to think about three separate phases:

1. **The initial impact**
   - The procedures
   - What to do
   - Who to notify

2. **The immediate future**
   - Temporary arrangements for staff and clients
   - The giving and explaining of information to both clients and staff

3. **Longer term**
   - Resume normal working practices
   - Debrief staff to learn from any mistakes made
   - Update the plan to reflect lessons learnt
   - Periodic test of evacuation procedures and plan

Business Continuity Questions

Event/scenario that would disrupt/stop normal Ward/Departmental services
<u>Loss of staff</u>
1. What would be the impact if this level of service/s were not available?
2. How would you know if the service had failed? (What would trigger you to take action)?
3. What would you do if the service had failed? (What is your alternative?)
4. Is your alternative contingency plan vulnerable to the same risk as the service?
5. What structure needs to be in place for the contingency plan to work?
6. What actions would actually be taken, and by whom?
7. How long could you carry on in this state?
8. How would you find out that the service is available again?
9. Would you have to do anything else to get your service working again?
10. What specific actions would be taken, and by whom?
11. What checks would be required?

The appropriate manager must be notified immediately of any incident that affects the usual working practice of the service, along with the on-site supervisor (where applicable).

Event/scenario that would disrupt/stop normal Ward/Departmental services
Loss of building/workspace
1. What would be the impact if this level of service/s were not available?
2. How would you know if the service had failed? (What would trigger you to take action)?
3. What would you do if the service had failed? (What is your alternative?)
4. Is your alternative contingency plan vulnerable to the same risk as the service?
5. What structure needs to be in place for the contingency plan to work?
6. What actions would actually be taken, and by whom?
7. How long could you carry on in this state?
8. How would you find out that the service is available again?
9. Would you have to do anything else to get your service working again?
10. What specific actions would be taken, and by whom?
11. What checks would be required?

Event/scenario that would disrupt/stop normal Ward/Departmental services
Loss of ICT, Telephony & Critical Data
1. What would be the impact if this level of service/s were not available?
2. How would you know if the service had failed? (What would trigger you to take action)?
3. What would you do if the service had failed? (What is your alternative?)
4. Is your alternative contingency plan vulnerable to the same risk as the service?
5. What structure needs to be in place for the contingency plan to work?
6. What actions would actually be taken, and by whom?
7. How long could you carry on in this state?
8. How would you find out that the service is available again?
9. Would you have to do anything else to get your service working again?
10. What specific actions would be taken, and by whom?
11. What checks would be required?

Event/scenario that would disrupt/stop normal Ward/Departmental services

Loss of equipment and/or supplies

1. What would be the impact if this level of service/s were not available?

2. How would you know if the service had failed? (What would trigger you to take action)?

3. What would you do if the service had failed? (What is your alternative?)

4. Is your alternative contingency plan vulnerable to the same risk as the service?

5. What structure needs to be in place for the contingency plan to work?

6. What actions would actually be taken, and by whom?

7. How long could you carry on in this state?

8. How would you find out that the service is available again?

9. Would you have to do anything else to get your service working again?

10. What specific actions would be taken, and by whom?

11. What checks would be required?

Implementing the BCP

1. Who would make the decision to put the contingency plan into action?
2. How long would it take to put the contingency plan into action?
3. Who would make the decision to move from the alternative contingency plan back to the normal way of running?
4. Are there any training requirements in order to be able to operate the above contingency plans?

Key Services to protect
Provide details of the key services you provide. Including if these are "9 – 5" or "24/7" and Monday – Friday etc. Also, what would you need to continue with immediately, slight delays, put on hold etc.

Key service	**Description. *Including*** *"9 – 5" or "24/7".*	**How quickly must this continue?** *Immediately, slight delays, put on hold*:

Alternative accommodation arrangements
Where staff are to report to until they can return to their regular work base:

Alternative location	**Number of staff that can be accommodated?**	**Contact name / number**

Telephony Arrangements
What are you key* phone numbers within the service and what will be done if your phone system goes down?

Key* Numbers	**What service does this provide?**	**Where and how can this be diverted?**

***a key telephone number might be for:**

- A Switchboard,
- A Reception area,
- To contact a team who provide urgent care,
- 24/7 care and support,
- For a Ward

You should also consider any **fax numbers** and what continuity / resilience is required.

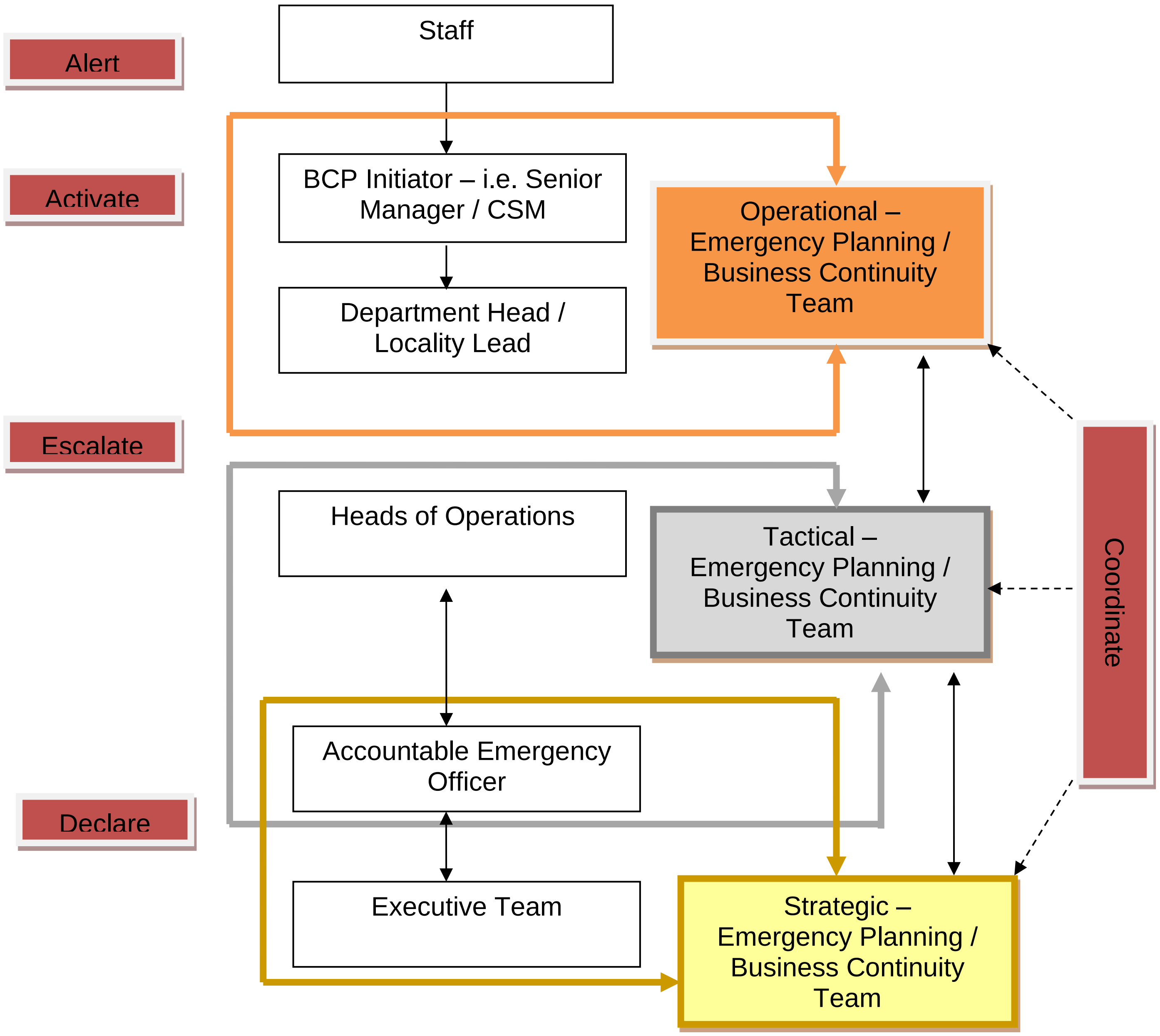
Note: If you invoke BCP plan you must complete a “Report following a business continuity incident” pro-forma and forward to the Emergency Planning team within 7 days of the outage.

This is essential for any debriefing, learning lessons and providing feedback across the Trust via the Local Emergency Planning Forums. Copies of these can be located on the CWP intranet via the Emergency Planning pages.

Resource Requirements for Recovery – *to be completed at the time of an incident*

Time	No. of Staff required?	Relocation required?	Divert Telephony?	Any other resources required
Immediately				
2 – 4 hours				
First 24 Hours				
2 – 3 days				
Up to a week				
Up to 2 weeks				

Business Continuity Escalation Process


Alert
Activate
Escalate
Declare
Staff
BCP Initiator – i.e. Senior Manager / CSM
Department Head / Locality Lead
Operational – Emergency Planning / Business Continuity Team
Heads of Operations
Tactical – Emergency Planning / Business Continuity Team
Coordinate
Accountable Emergency Officer
Executive Team
Strategic – Emergency Planning / Business Continuity Team

Key contact numbers in the event of a business continuity incident

IT Service Desk	**0300 303 8182** or extension **8182** from a CWP Cisco phone
Facilities	**Central & East** – (in hours) 01625 663 084 **West** – (in hours) 01244 397271 **Wirral** – (in hours) 0151 604 7605
Estates	**Chester & Wirral –** in hours 01244 397 737, out of hours 01244 365 000 (ask for CWP Duty Engineer/ On-call engineer) **Central & East Cheshire–** in hours 01625 663 737, out of hours 07917 228 099
HR	**01244 393128**
Emergency Planning Team	0300 303 4582 / 01244 397 642
2nd tier on-call	**See intranet (rotas)**
In hours 3rd tier on-call - Redesmere Switchboard	**01244 397 397**
Out of hours 2nd & 3rd tier on-call (Via Switchboards)	**CoCH:** 01244 365 000**, Macclesfield:** 01625 421 000, **Arrowe Park:** 0151 678 5111, **Leighton:** 01270 255 141

This plan was completed by

Print name			
Position			
Signature			
Date		Ext	

This plan was reviewed annually by

Print name			
Position			
Signature			
Date		Ext	

Staff (out of hours) contacts

A pre-arranged call out/contact system is necessary to ensure that the right people are mobilised to their place of duty and in the minimum time.

The manager is			
Based at			
Contactable at		Extension	
Home		Mobile	

The officer / supervisor with direct responsibility for the service is

The manager is			
Contactable at		Extension	
Home		Mobile	

The officer / supervisor with deputy responsibility for the service is

The manager is			
Contactable at		Extension	
Home		Mobile	

Staff (out of hours) contact list

Note: full departmental contact list should be stored outside of your BC plan.

Service		**Location**	

Name and address	Function	Tel ext	Mobile

Appendix 4 – Debrief report following a business continuity incident

Section A

Datix form ID	
Incident name	
Reported date	
Department	

Section B

Please give a brief description of the incident to include nature and cause, or attach the relevant Datix Form

Please describe the impact the incident had on the Service, to include effectiveness in meeting Recovery Time Objectives (RTO's)

1.
2.
3.
4.

Was the BCP implemented?

□ Yes
□ No

Who decided to implement the BCP?

Name	
Job title	

What were the lessons identified from the incident relating specifically to business continuity/ emergency planning?

1.
2.
3.
4.

Is there a requirement to update the business continuity plan following the incident?

□ Yes
□ No

Action plan following the incident:

Action	By whom	By when	Status	Comments

Section C

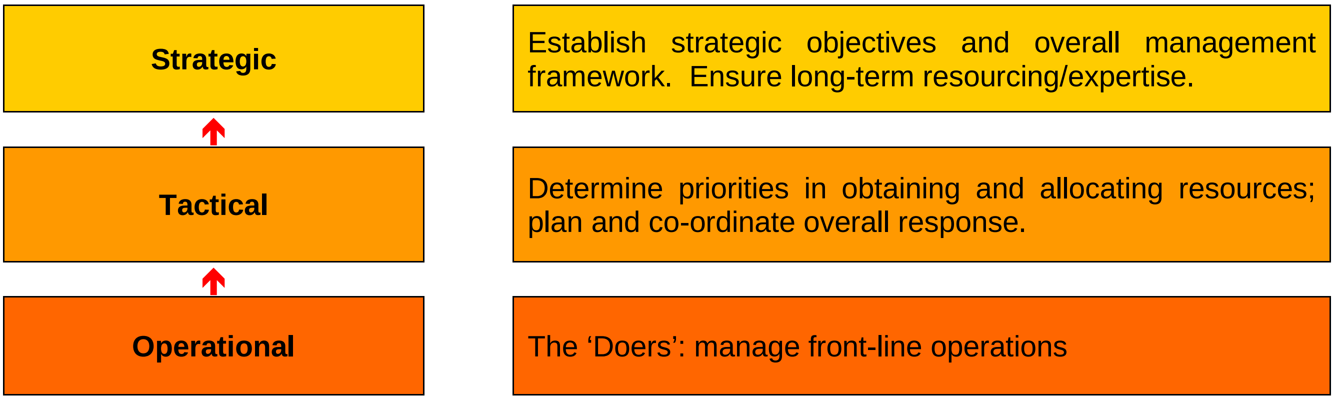
Signed		**Dated**	

FOR OFFICE USE ONLY

Emergency Planning Reference	
Date quality checked by Emergency Planning Team	
Quality checked by the Emergency Planning Team?	□ Yes □ No
Date taken to Emergency Planning Sub-Committee	
Approved by Emergency Planning Sub-Committee?	□ Yes □ No

Please complete and return to the Emergency Planning Team within one week of the incident

Appendix 5 - Framework of command / management



Strategic

Establish strategic objectives and overall management framework. Ensure long-term resourcing/expertise.

Tactical

Determine priorities in obtaining and allocating resources; plan and co-ordinate overall response.

Operational

The ‘Doers’: manage front-line operations

Appendix 6- Process for consultation, approval and ratification of Business Continuity Plans

New Business Continuity Plan

Reviewing existing Business Continuity Plan
Document author to determine if the document is still needed

Yes continue to **step 1** | **No** continue to **step 6**

↓

Step 1 – Write / review Plan
Business Continuity lead develops / reviews the Business Continuity plan using the approved template – see Business Continuity Management System Policy and Procedures and CWP emergency planning intranet page for template.
It can be advised that this is done in partnership with the emergency planning team

↓

Step 2 – Consultation
Business Continuity leads send the working document for feedback to;

- Members of your team/ department/ service;
- General managers and service managers;
- Related services/ departments.

Business Continuity leads send to the Emergency Planning Team for consultation ahead of approval.

↓

Step 3 - Approval
Emergency Planning Team to send the final version of the document to the approving meeting

Trust wide documents	**Approving meeting**
Adult Mental Health West/ Wirral/ Central & East	West/ Wirral/ Central & East local emergency planning group respectively
CAMHS	West, Wirral and Central & East emergency planning local groups
Learning Disability	West, Wirral and Central & East emergency planning local groups
Substance Missue	West, Wirral and Central & East emergency planning local groups
Neighbourhood	West local emergency planning group
Clinical and Corporate support (all)	Emergency Planning Sub Committee

Business Continuity lead to make agreed amends as per meeting minutes and progress to step 4

↓

Step 4 – Ratification
Send approved document to the Emergency Planning Team for the Emergency Planning Sub Committee (EPSC) agenda for ratification.

↓

Step 5 – Dissemination
Emergency Planning Team disseminates to all staff via CWP emergency planning intranet page.
Business Continuity leads will disseminate to their own teams/ department/ service.

↓

Step 6 – Control and archive
Emergency Planning Team archives all previous issues of documents. The archived document **must** include a watermark stating 'not current issue'

↓

Step 7 – Reviewing document
Business Continuity lead and Emergency Planning Team ensure that the document review is conducted before the stated review date (default 2 years or following significant changes)