BUSINESS CONTINUITY STRATEGY
Version 1

Authorship:	Clare Hedges, Head of Quality and Performance
Committee Approved:	Governing Body, HaRD CCG
Approved date:	
Review Date:	
Equality Impact Assessment: **Sustainability Impact Assessment:** **Target Audience:**	Screening completed Screening completed All Staff
Policy Reference No:	N/A
Version Number:	One (New Strategy)

A hard copy of this and the above document can be found in the on-call file.

However the on-line version is the only version that is maintained. Any printed copies should therefore be viewed as 'uncontrolled' and should be checked that the version corresponds with the on-line version.

CONTENTS

REVISIONS/AMENDMENTS SINCE LAST VERSION

Date of Review	Amendment Details

1. GLOSSARY

The definitions below are included to provide a commonly understood terminology and support a shared understanding of the aims and objectives of this document. They are not exhaustive but do cover the main issues of interest.

Activity
Processes or sets of processes undertaken by the CCG, or on behalf of the CCG, that supports delivery of services.

Business as Usual
Pre-defined acceptable levels of service delivery.

Business Continuity Management (BCM)
A process for identifying potential threats to the organisation and impacts upon critical operations, and which provides a framework for building organisational resilience with the capacity for an effective response. Includes strategic and tactical capability of the CCG to plan for and respond to business interruptions in order to support continued delivery of 'business as usual'.

This process needs to link closely with the corporate risk management system to ensure all risks are recorded and risk mitigation plans developed

Business Continuity Plan (BCP)
A documented collection of procedures that is developed, compiled and maintained in readiness for use in an incident to enable the organisation to continue to deliver its critical services at an acceptable, pre-defined level.

Business Continuity Planning
The development of strategies, plans and management structures to ensure continuity of critical services at acceptable, pre-defined levels. Business Continuity Planning is the next logical step in the Business Continuity Management Lifecycle after Business Impact Analysis.

Business Impact Analysis (BIA)
A survey and analysis process to determine the differentiation between critical and non- critical organisational services and processes. A service may be considered critical if the implications of probable damage to the organisation are regarded as unacceptable.

Critical Activities
Those activities which have to be performed in order to deliver the key products and services which enable the organisation to meet it most important and time-sensitive objectives. These activities have a maximum tolerable period of disruption of less than twenty-four hours.

Disaster Recovery Planning (DRP)
A disaster is an occurrence or scenario that disrupts the functioning of the organisation resulting in the loss of data, loss of personnel, loss of business or loss of time. DRP is the related set of processes which identify and consider likely scenarios and proactively prepares for how these will be contained, managed and recovered from in a way that minimises the impact or loss.

Disruption
Any event, planned or unplanned, which causes an interruption to the CCG's ability to continue business as usual.

Emergency

Is defined in Part 1 of the Civil Contingencies Act 2004 as "an event or situation which threatens serious damage to human welfare in a place in the UK, the environment of a place in the UK, or war or terrorism which threatens serious damage to the security of the UK." The definition of emergency is concerned with consequences, rather than cause or source. Therefore, an emergency inside or outside the UK is covered by the definition, so long as consequences of such are experienced within the UK.

Essential Activities

Those activities carried out by the CCG which are sensitive and important, but not critical to life and death of patients. These activities have a maximum tolerable period of disruption of less than forty-eight hours.

Major Incident

A Major Incident is any occurrence that presents serious threat to the health of the community, disruption to the service or causes (or is likely to cause) such numbers or types of casualties as to require special arrangements to be implemented by hospitals, ambulance organisations or primary care organisations. For the NHS, a major incident is defined as:

"Any occurrence which presents a serious threat to the health of the community, disruption to the service or causes (or is likely to cause) such numbers or types of casualties as to require special arrangements to be implemented by hospitals, ambulance trusts or primary care organisations"

Major incidents for NHS organisations are defined as one of three levels. These are 'major', 'mass', or 'catastrophic'.

i.   Major – each individual NHS organisation must plan to handle incidents in which its own facilities – or neighbouring ones – may be overwhelmed. Planning successfully for these wider disruptive challenges will require more than simply scaling up the current plans of individual agencies.

ii.   Mass - much larger scale events affecting potentially hundreds rather than tens of people, possibly also involving the closure or evacuation of a major facility (eg because of fire or contamination) or persistent disruption over many days; these will require a collective response by several or many neighbouring trusts.

iii. Catastrophic - events of potentially catastrophic proportions that severely disrupt health and social care and other functions (power, water etc) and that exceed even collective capability within the NHS.

Major Incident Planning

MI Planning is the related set of processes which identify and consider likely scenarios and proactively prepares for how these will be contained, managed and recovered from in a way that minimises the impact or loss.

Resilience

The ability of an organisation to prevent its critical services being disrupted by an incident and/or to promptly recover them to pre-defined and acceptable levels of delivery.

Resources

Resources are all assets, people, skills, information (electronic and manual), technology (including plant and equipment), premises and supplies that the organisation must have available in order to meet its critical service delivery objectives.

Risk Management (RM)

The structured development and application of management culture, policy, procedures and

practices to the tasks of identifying, analysing, evaluating and controlling the response to risks. This must be managed and recorded through the corporate risk management system.

Routine Activities

Those activities carried out by the CCG which support business delivery on a daily basis and are not critical or essential. These activities have a maximum tolerable period of disruption of less than two weeks.

Service Continuity Plan (SCP)

A set of actions and procedures required by local management which details the response to the loss of one or more activities or resources which a critical service depends upon. The SCP should define recovery to at least a pre-defined minimum level of service delivery.

Standard Operating Procedures (SoPs)

A procedure is an established or official way of doing something; a series of actions conducted in a certain manner. A procedure is a set of detailed step-by-step instructions that describe the appropriate method for carrying out tasks or activities to achieve a stated outcome to the highest standards possible and to ensure efficiency, consistency and safety. In the context of this policy, procedures should be defined to a level necessary to reduce the likelihood of the procedure contributing to a business continuity disruption, and also detailed enough to support any recovery effort. Staff should be trained to follow the procedure as intended.

Service Recovery

The process through which business as usual is reached, following an interruption or disruption event.

Trigger Points

Significant milestones or anticipated events during the planning, exercising and execution of a BC Plan. One or more prepared actions should be taken in response to a Trigger Point being reached, usually regardless of impact upon the organisation or its critical services, although impact may determine which options are selected within certain action plans.

2. INTRODUCTION

The Chief Officer of the CCG has the statutory responsibility for the Emergency Preparedness Resilience and Response arrangements of the CCG under the Civil Contingencies Act 2004 (CCA), Health and Social Care Act 2012, NHS England, Emergency Planning Framework and other central Government Guidance.

The CCG Accountable Emergency Officer (AEO) is responsible for '*ensuring that the organisation is properly prepared and resourced for dealing with a major incident or civil contingency event*' (Emergency Officers for Emergency Preparedness, Resilience and Response (EPRR) 2012). CCGs must assure their Board, NHS England and Local Health Resilience Partners that suitable arrangements are developed, tested and maintained.

The Accountable Emergency Officer is the Executive Nurse and Director of Quality and Governance.

Category of Responder

Category 1 Responders (main NHS providers and NHG England) have a legal obligation under the Civil Contingencies Act 2004 (CCA) to assess the risk of, plan, and exercise for emergencies, as well as undertaking Business Continuity Management. Category 1 Responders are also responsible for warning and informing the public in relation to emergencies.

CCGs are Category 2 Responders. This means that the CCG has a legal obligation under the Civil Contingencies Act 2004 (CCA) to support the Category 1 Responders.

The CCG also has a statutory duty to deliver essential functions to meet its commissioning responsibilities for the CCG population.   The purpose of this plan is to map these key functions and consider alternative ways of delivery in the short term until normal service is restored. Any long term disruption would need further discussion by the CCG's Governing Body.

For the NHS, business continuity management is defined as the management process that enables a 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 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.

This Policy has been developed to support the Major Incident Planning process, recognising that a Business Continuity (BC) scenario could provide the 'trigger' for a major incident response (such as loss of one or more Organisation HQ sites) or, alternatively, a major incident (such as widespread and prolonged flood affecting the ability of staff to travel and work) may require one or more departmental or service BC plan to be invoked.

The Head of Quality and Performance is the BC Manager

They are responsible for ensuring there is on-going dialogue and collaboration between the BC function and those teams with Major Incident Planning responsibilities.

Pandemic Flu

As a Category 2 Responder, the CCG has a role in supporting NHS England and providers of NHS funded care in planning for and responding to an influenza pandemic.

3. SCOPE

3.1 Within Scope

This policy relates to the business continuity management of the business functions within the CCG. It addresses those services which are provided by the Teams of Harrogate and District Clinical Commissioning Group:

- Corporate Services
- Quality and Performance
- Commissioning
- Finance and Contracting
- Medicines Management

3.2 Out of Scope

This plan does not outline the arrangements for business continuity management of services and business functions carried out by the CCG's providers and service suppliers, such as:

- HDFT
- NYCC
- eMBED
- North of England Commissioning Support
- Harrogate Borough Council
- Other CCGs where Memorandum of Understandings are in place for the hosting of services
- NHS England (co-commissioning Primary Care Services)

The CCG is heavily reliant on the services provided by the above organisations. Contractually these organisations are required to ensure arrangements for business continuity are in place and assurance is given to the CCG that the processes are robust.

4. POLICY PURPOSE

The purpose of this document is to ensure the organisation's business critical functions, systems and processes are identified. This will be achieved through partnership working between the BC Manager, Information Asset owners and relevant BCP owners to undertake risk assessments and business impact analysis, and then taking action to reduce risks and/or produce BC Plans covering those areas identified as high or medium risk.

The policy will help the CCG to anticipate, prepare for, prevent, respond to and recover from, disruptions, whatever their source and whatever part of the business they affect.

4.1 Objectives of the Business Continuity Policy

- to ensure a comprehensive Business Continuity Management System is established and maintained;
- to ensure key services, together with their supporting critical activities,
- processes and resources, will be identified by undertaking business impact analysis;
- to ensure risk mitigation strategies will be applied to reduce the impact of disruption on key services;
- to ensure plans will be developed to enable continuity of key services at a minimum

acceptable standard following disruption;

- to outline how business continuity plans will be invoked and the relationship with the CCG Major Incident Plan;
- to ensure plans are subject to on-going exercising and revision;
- to ensure the Clinical Commissioning Group Governing Body is assured that the Business Continuity Management System remains up to date and relevant.

4.2 Outcomes of the Business Continuity Policy

The outcomes of this policy aim to ensure:

- key products and services are identified and protected, ensuring their continuity
- the organisation's understanding of itself and its relationships with other organisations, relevant regulators or government departments, local authorities and the emergency services is properly developed, documented and understood
- staff are trained to respond effectively to an incident or disruption through appropriate exercising
- staff receive adequate support and communications in the event of a disruption
- the organisation's supply chain is secured
- the organisation's reputation is protected
- the organisation remains compliant with its legal and regulatory obligations

5. ROLES / RESPONSIBILITIES / DUTIES

5.1 Legal and Statutory Duties and Responsibilities

The Civil Contingencies Act (CCA) 2004 places a duty on CCGs to have business continuity plans in place to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable. The duty relates to all functions, not just emergency response functions.

The model adopted aligns with best practice expectations placed upon all NHS organisations in the NHS England's 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).

5.2 Specific duties and responsibilities within the CCG

For the BC policy to be effective and become embedded in the organisation, responsibilities from the Chief Officer downwards need to be agreed and communicated so that everyone is aware of what is expected from them.

5.2.1 Strategic

Chief Officer

Has overall statutory responsibility for the strategic and operational management of the CCG, including ensuring that the CCG has in place robust arrangements for business continuity management and service recovery. They should ensure that Governing Body is kept fully informed of significant business continuity risks and any associated significant developments or issues.

Accountable Emergency Officer – Head of Quality & Governance

Is responsible for ensuring that the CCG is prepared and resourced for dealing with a major incident or event.

Executive Directors

Have a responsibility for ensuring that:

They hold up to date copies of the Business Continuity Plans and Business Impact Assessments relevant to their individual directorates and circulate as appropriate to identified managers.

CCG Governing Body

Is responsible for setting the strategic context in which business continuity and service recovery procedures are developed, and for the formal review and approval of this Policy and the BC Plan. The Governing Body is also responsible for determining the accepted levels of 'business as usual', through monitoring service delivery and approving suggested developments.

Corporate Risk Review Group

Acts as the CCG's risk management steering group, tasked with establishing and maintaining robust risk management and business continuity systems within the CCG on behalf of the Governing Body.

Business Continuity Manager – Head of Quality & Performance

Is responsible for ensuring that business continuity management plans to support the core business functions are completed and updated as necessary. They are responsible for ensuring:

- Directorate leads document and review their Business Impact Assessments on an annual basis or when necessary;
- Training needs are identified, including appropriate induction training and more specialist training for those filling specific roles
- Advice, guidance and instruction on business continuity matters is available, particularly the production of Business Continuity Plans
- Business continuity exercises are conducted in line with national guidance and in liaison with the other organisation managers
- That awareness and knowledge of the business continuity plan is embedded among staff.

CCG Heads of Service

Will support the Business Continuity Manager ensuring that

- Critical services and resources are identified across their team ensuring that their element of the BC plan is reviewed at six monthly intervals and updated as necessary to maintain good quality control of document information.
- Any revisions are notified to the Business Continuity Manager
- Encourage and participate in training or exercises.
- Contribute to the review and updating of the BC plan regularly in light of lessons learned from exercises or incidents, research or changes in staff.
- Support business continuity awareness and acceptance amongst staff and ensure that all of their staff are aware of their responsibilities within the BC plan.

All CCG Staff

Are responsible for ensuring familiarity and co-operation with this policy and their Business Continuity Plan and in particular are required to report any risks to the delivery of the organisation's strategic aims and related objectives via normal reporting arrangements.

6. ACTIVATING THE PLAN

Director on Call

Is responsible for activating and coordinating the plan following discussion with the Head of Service on call and other Directors. However, it should be noted that there may also be a major incident which they will be leading on behalf of the organisation. In this scenario it is possible to delegate the leadership of the business continuity plan to the senior manager on call or other suitable delegate. If there is an incident that requires evacuation of Grimbald Crag Court and the Director on call is not on site they should delegate the responsibility to an individual who is in on site.

Heads of Service on-call

Is the key link with the Director on-call. They are responsible for ensuring that the business continuity plan is activated and that all staff are kept informed and updated.

Triggers for activation of plan

The Business Continuity Plan will also be activated by the Director on Call when the major incident plan has been activated or is on standby, and there is an incident that has the potential to cause business disruption and affect critical activities. Depending on the type of disruption, it is possible that not all teams will need to activate their business continuity plan.

Action Cards

Action Cards can be found in the Business Continuity Policy and should be used to initially address any potential threat to business continuity. They cover:
1. Partial loss of staff
2. Complete loss of staff (>40%)
3. Loss of access to Unit 1 or 2 Grimbald Crag Court (or the surrounding business park or roads) for longer than the maximum acceptable downtime.
4. Loss of telephone communication
5. Loss of network connectivity for an anticipated prolonged period
6. Loss of email
7. Loss of electrical supply for longer than the maximum acceptable downtime
8. Loss of gas supply for longer than the maximum acceptable downtime
9. Loss of water supply for longer than the maximum acceptable downtime
10. Loss of security
11. Transportation issues
12. Fuel shortage
13. Adverse weather conditions

It should be borne in mind that these events may not be mutually exclusive, e.g. extreme weather leads to loss of electricity, disruption to transport, staff unable to get to work.

7. BUSINESS CONTINUITY PLANNING

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. 7.2.

Figure 1 below demonstrates that steps 1 - 4 are cyclical and these should 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

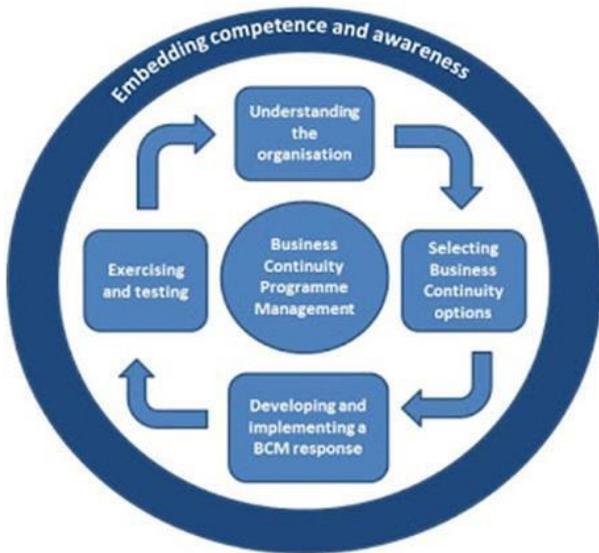and grow as incidents happen, exercises are held and risks are reassessed.

Figure 1: Business continuity programme elements (Source: ISO 22313)

7.1 Understanding the Organisation

The CCG is responsible for commissioning a wide range of patient services for the local population and in the event of an emergency or business interruption it is essential that critical services can be restored and maintained as soon as is practically possible.

7.2 Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is the process of analysing business functions and determining the effect that a business disruption might have upon them, and how these vary over time. The aim of the BIA is to ensure Harrogate and Rural District Clinical Commissioning Group has identified those activities that support its key services in advance of an incident, so that robust business continuity plans can be put into place for those identified critical activities.

The BIA process:

- Defines the function and its supporting processes.
- Determines the impacts of a disruption.
- Defines the recovery time objectives
- Determines the minimum resources needed to meet those objectives.
- Considers any statutory obligations or legal requirements placed on the CCG.

Within the BIA, functions within the CCG have been categorised as critical, essential and routine. The functions by category are summarised in Appendix 1.

7.2.1 Risk Assessment

This Policy will link to the risk management framework to identify and validate the potential risks to critical business functions. The criticality of the risks may be assessed according to impact on the organisation in terms of service delivery, finance, operations management or reputation.

Not all services will be deemed critical. The framework will therefore help identify the high, medium and low risk factors so that effort can be applied where it will have most value.

The NYCC community risk register is considered when undertaking business impact analysis in order to enable the organisation to understand the threats to, and vulnerabilities of, critical activities and supporting resources. It can be found at:
http://www.emergencynorthyorks.gov.uk/node/10
and https://www.northyorks.gov.uk/resilience-and-emergencies-unit
Any risks identified by the CCG with regards to the Business Continuity Plan will also be recorded on the Harrogate and Rural District CCG risk register.

7.2.2 Maximum Acceptable Downtime (MAD)

The Maximum Acceptable Downtime (MAD) is the timeframe during which the recovery of systems, processes and activities must be achieved to prevent the risk of a significant impact arising if the downtime is exceeded, i.e. what is the maximum down time which could be tolerated without incurring one or more of the consequences below.

For the purposes of business continuity, Harrogate and Rural District Clinical Commissioning Group defines a 'significant impact' as any situation that could give rise to one or more of the following situations:

- An unacceptable risk to the safety and/or welfare of patients and staff
- A major breach of a legal or regulatory requirement
- A major breach of a contract, service level agreement or similar formal agreement
- The risk of significant financial impact, and/or
- A threat to the reputation of the CCG as a competent NHS organisation.

For the purposes of business continuity, Harrogate and Rural District Clinical Clinical Commissioning Group defines the following scale of maximum acceptable downtimes:

	Timeframe	Rationale
A	Immediate restart	Typically used only for clinical and in-patient services where any interruption raises an immediate and unacceptable risk to people
B	One working day	An unacceptable risk will arise if this activity is not fully restored within 24 hours
C	Three working days	The norm for service recovery - recovery within this timeframe will not jeopardise patient safety or welfare
D	One working week	The timeframe for most non-clinical activity
E	Seven days plus	Typically training and similar activities that can be suspended without significant impact in the short term

7.3 Non-Critical Functions, Systems & Processes

For those areas of organisation business deemed 'non-critical' as a consequence of completing the BIA and risk assessment processes, it will be the responsibility of the relevant BCP Owner to ensure these areas are kept under review and take account of any changes which may have an impact on their status. If a BC scenario occurs, these areas will be recovered as a lower priority and according to agreed recovery time objectives. In some scenarios, it may be justified to stop these functions altogether so that all available resources can focus on recovering the

critical functions within agreed timescales. Where services are put 'on hold' it is essential that affected users or other stakeholders are notified as part of the recovery effort.

7.4 Legal Requirements & Implications

This Policy aims to ensure the organisation meets its legal obligations both as an employer, e.g. health and safety, and as the 'custodian' of sensitive and personal information relating to both the local population and staff.

Under the Data Protection Act (2000) the organisation is a legally accountable 'data controller' and will ensure there are appropriate safeguards in place to protect sensitive and personal data as part of on-going business practices, and ensure this data is protected and recoverable in a BC scenario.

Therefore, this document requires that appropriately detailed Disaster Recovery Plans are in place and maintained relating to the technical infrastructure, assets and systems the organisation is responsible for. Overall responsibility for this area rests with the Head of IMT. These responsibilities will cover areas such as:

- Identifying and assigning Recovery Classes to technical assets
- Arranging off-site support and recovery
- Security of critical & vital electronic records
- Recovery of critical & vital systems, assets & infrastructure.

7.5 Selecting business continuity options

A number of areas affecting service resilience have been considered for each function to ensure effective service resilience. These include:

a) People - Information on services and supporting resources, key staff, skills, equipment and contact information.

b) Premises - In the event that CCG premises are unavailable or inaccessible for an extended period alternative accommodation will be sought to house all critical/essential processes. The minimum office amenity requirements (desks, phones, fax, PCs, etc.) have been identified for each function.

In the event of an incident, alternative accommodation will be sought. If further accommodation is required the CCG will approach partner agencies including other Clinical Commissioning Groups, NHS England Yorkshire and Humber Area Team, adjacent Mental Health Trusts and Acute Trusts.

NB: It is, however, extremely unlikely that this level of response will be required as the majority of CCG personnel responsible for carrying out critical / essential processes will be equipped to work from home or any other base.

c) Processes – Information on IT equipment, software and documentation/records requirements.

d) Providers – The CCG relies upon the products and services of the following organisations to be able to deliver its commissioning responsibilities:
   - eMBED

- North of England Commissioning Support
- Harrogate Borough Council
- NHS Harrogate and Rural District CCG

The BIA identifies the support dependencies provided by other organisations such as those listed above. The BIA also identifies those functions provided entirely by other organisations and where recovery of these services would be undertaken through that supplier's business continuity arrangements.

7.6 Developing and implementing a business continuity response

7.6.1 Triggers for activation of plan
The CCG Business Continuity Plan is likely to be activated in the following circumstances although the list is not exhaustive and the need to activate the plan will be decided by the Director on Call for the CCG.

- Loss of access to Grimbald Crag Court (due to fire, flood or other incident affecting either the building, surrounding business park or roads) for longer than the determined maximum acceptable downtime (MAD)
- Loss of amenities that support Grimbald Crag Court including power, water or gas for longer than the determined MAD
- Loss of network connectivity at Grimbald Crag Court
- Complete or near complete loss of staff
- Loss of telephone communication
- Loss of email
- Transportation issues
- Fuel shortage

It should be borne in mind that these events may not be mutually exclusive, e.g. extreme weather leads to loss of electricity, disruption to transport, staff unable to get to work.

7.7 Exercising and Testing

BC Plans are more likely to be effective in a real life situation if they have previously been tested under simulated and controlled conditions. This gives staff the opportunity to practice their roles and responsibilities and for any assumptions or omissions to be identified and corrected.

This Policy promotes the development of a formal and robust testing framework for all BC Plans so as to provide on-going assurance to the organisation that plans have been placed under some 'stress' and are fit for purpose, and reassurance to BCP owners that they are well prepared to manage what might otherwise be a very stressful and highly-charged set of circumstances.

7.7.1 Training
On call directors and Team Business Continuity Leads will be provided with business continuity training appropriate to their role. All other staff will require business continuity awareness training in relation to continuity plans for each service and this will be provided by the staff member's line manager.

7.7.2 Exercising

Teams will be expected to undertake business continuity exercises on a regular basis. These may take the form of self-directed exercises by individual services using scenarios on the emergency planning intranet, team table top exercises facilitated by the Associate Director of Corporate Services and multi- agency exercises.

Exercising can take various forms, from a test of the communications plan, a desk-top walk through, to a live exercise. However in all cases, exercises should be realistic, carefully planned and agreed with stakeholders, so that there is minimum risk of disruption to business processes.

The organisation will aim to support our key partners (NHS and others) in a BC scenario. This could include loss of a key building or an environmental incident such as flooding. The practice of mutual aid is already firmly established as part of Major Incident Planning and this policy supports a similar approach being adopted for BC Planning.

7.7.3 Testing Programme

The BC Manager in collaboration with the BCP Owner will determine the frequency, scope and level of testing – it is expected that any testing will reflect prevailing risks and take account of any recent or planned changes. In any case however, all plans should be subject to some form of testing at least once per calendar year.

Wherever possible, testing of plans will take place according to a timetable, agreed in advance between the BCP Owner and the BC Manager. In exceptional circumstances, the BC Manager reserves the right to carry out an unannounced test. However, documented authority for this will have to be granted by the Accountable Emergency Officer.

In all cases, exercises should be realistic, carefully planned and agreed with stakeholders, so that there is minimum risk of disruption to business processes.

Whilst details of the testing will be made locally, the following continuum provides a framework within which these decisions should be made:

Passive	Active/Passive	Active
Procedures Review: ensure procedures needed in a recovery are available, understandable and current. Can be tested as a table-top exercise.	Simulation Testing: involves a disruptive scenario, but without actually disrupting normal operations. Could include an evolving scenario, rather than having a pre-determined 'end point'.	Notification: determines adequacy of call lists and notification procedures; needs to be carried out regularly otherwise it can become out of date quickly (similar to Communication Cascades).
Structured Walk-Through: involving a given scenario, with team members assuming their roles and carrying out actions in chronological order as detailed in the BCP.		Inventory / Checklists: Verifies key resources needed for a recovery, those that should be and actually are available. Should consider resources held elsewhere (if appropriate).

		Parallel Testing: usually involves working with IT to ensure data is recoverable, and accurately reflects known values/outputs using historical data as a comparator.
		Full Interruption: invocation of the BCP, only carried out if there is a sound business case for doing so as it disruptive and expensive (may form part of a wider Major Incident Plan testing exercise).

For HaRD CCG the following will occur:

	Frequency	Timing	
Notification	6 months	Q1 & Q3	Admin Team
Procedures review every 12 months	12 months	Q3	Heads of Service
Inventory checklists	6 months	Q1 & Q3	Head of Finance
Parallel Testing	12 months	Q3	Head of Finance
Simulation test 12 months	12 months	Q2	CCG
Full simulation test (part of LHRP operation)	24 months	Usually Q3	Heads of Service

7.7.4 Capturing lessons learned and improvement plans
All testing sessions should be followed by an immediate de-brief with the staff concerned with the aim of providing answers to the following questions:

What went well?
What needs improving?

The outcomes and results of plan tests and de-briefs will be recorded by the BC Manager and made available to auditors, the Chief Finance Officer and/or the IMT Senior Team if requested. The BCP Owner is responsible for amending the plan to reflect the testing outcomes and lessons learnt.

This may also require amendment to standard operating procedures and consideration of risks reported to be reviewed and updated.

7.7.5 Records
A record of training and exercising undertaken will be kept by the Business Continuity Manager so that the organisation has a central record of training undertaken.

7.7.6 Audit and Monitoring Criteria
The Business Continuity Manager is responsible for ensuring policy and guidance on all business continuity arrangements is developed, including the production and maintenance of

the Harrogate and District Clinical Commissioning Group Business Continuity Policy and Plan which is approved by Governing Body.

The Associate Director of Corporate Services is responsible for ensuring the policy and plan is reviewed on an annual basis or earlier as a result of changes to legislation or changes to CCG structures and/or procedures. Each team will undertake an annual business impact analysis and review the team business continuity plan accordingly.

Within Harrogate and District Clinical Commissioning Group, the Business Continuity Manager will ensure that annual assurance reports are submitted to the Governing Body outlining the current status of Harrogate and District Clinical Commissioning Group's emergency preparedness.

7.7.7 Continuous Improvement

Business Continuity Plans will be updated in light of feedback from:

- actual incidents and disruptions to business activities;
- exercises and audits;
- re-assessment of risks;
- organisational, facility or systems changes;
- external change including change to partner organisations;
- Management reviews of the effectiveness of the business continuity process.

8. AWARENESS

This policy will be made available to all Members and staff via the CCG's website. Notice of all approved policies placed on the website will be included in CCG briefing processes. The policy will be brought to the attention of all new Members and staff via the induction process.

Advice on this policy can be obtained from the Accountable Emergency Officer or the Business Continuity Manager.

Specific training and awareness have been identified in Section 7.7

9. IMPACT ANALYSES

7.2 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing an Equality Impact Analysis, this policy does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage.

7.3 Sustainability

As a result of performing a Sustainability Impact Assessment, this policy does not appear to have any positive or negative impacts on any of the CCG's sustainability themes

10. IMPLEMENTATION

Following approval by Governing Body, this policy will be distributed to the CCG Heads of Service for dissemination to all their staff.

11. MONITORING & AUDIT

This Policy and any associated BC Plans may be subject to review by the organisation's Internal or External Auditors as part of their annual audit plan, to ensure it is being implemented effectively. Any such reviews will be carried out with the full support of staff requested to contribute to the audit. The findings and recommendations arising from the audit will be considered using standard audit reporting procedures.

The Audit and Governance Committee will keep under review the arrangements for the Business Continuity Plans, annually review the plans and Business Impact analysis and provide an annual assurance report to the Governing Body.

Individual Teams will review the Business Impact Analysis for their areas 6 monthly.

12. POLICY REVIEW

This policy will be reviewed in two years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance, as instructed by the senior manager responsible for this policy. Any interim amendments will be tabled at Senior Management Team meetings.

13. REFERENCES
- Civil Contingencies Act 2004
- NHS Commissioning Board Emergency Preparedness Framework 2013
- NHS Commissioning Board Business Continuity Management Framework (service resilience) (2013)
- ISO 22301 Societal Security – Business Continuity Management System

Associated Documentation
- On Call Policy
- Surge and Escalation Plan
- Flexible Working Policy

14. KEY PARTNERS

This document aims to ensure the organisation is willing and capable of working with the wide range of Third Parties that either provides services to the organisation, or where the organisation has a dependency on them in order to deliver its own critical functions, systems or processes.

This will be achieved by:

- active co-operation and collaboration with relevant Third Parties on strategic or inter-agency BC initiatives
- ensuring our critical suppliers and providers have appropriate BC Plans in place; ensuring

any contracts entered into include BC requirements
- reviewing our supplier and provider arrangements to reduce the possibility of a 'single point of failure' being created
- ensuring Third Parties are considered during Departmental BIA, risk assessment and BC Planning processes.

14.1 Key partners include

Outsourced Activities	Supplier Name	Date Business Continuity Plan reviewed
IT Services & Support (inc. telephony and networks)	eMBED	Reviewed August 2017
BI Services	eMBED	Reviewed August 2017
HR Support	eMBED	Reviewed August 2017
Procurement Support	eMBED	Reviewed August 2017
Referral Support Services & Choose and Book	NHS Vale of York CCG	Current plan under review. Feb 2015 plan in use
Serious Incident reviews	NHS Vale of York CCG	Current plan under review. Feb 2015 plan in use
Community Infection, Prevention & Control	Harrogate & District NHSFT	Reviewed July 2017
Research & Development	NHS East Riding of Yorkshire CCG	Reviewed January 2018
Legal Services	NHS Scarborough & Ryedale CCG	Reviewed January 2018
CHC/FNC/VP Teams	NHS Scarborough & Ryedale CCG	Reviewed January 2018
Children's Services	Hambleton, Richmondshire & Whitby CCG	Reviewed February 2017

15. COMMUNICATIONS & MEDIA STRATEGY

In all but the most localised and short-term scenarios, it is highly likely that both internal and external stakeholders and partners will need to be notified that a BC Plan has been invoked and 'business as usual' has been disrupted.

All departmental or service plans should identify:

- **WHO** needs to be consulted with and who needs to be informed; the former implies a more active relationship (e.g. this may be a key supplier or internal 'customer') while the latter may be the general 'all user' staff population;
- **WHEN** to communicate; this is likely to be at the point of invocation and at key points whilst the plan is active, e.g. at checkpoints identified in the BCP Action Cards;
- **HOW** to communicate; this may be affected by the nature or source of the incident (e.g. email system is down) so judgement will have to be used as to the most effective and efficient way of letting others know that the BC plan has been invoked. All BCPs should contain Contact Details of key stakeholders, that must be kept up to date if they are to be effective;
- **WHAT** to communicate; depending on the incident, it may be possible to provide detailed updates or it may be more feasible to provide summary details. Consult with Communications experts to support you when making these decisions if required.

16. AVAILABILITY & VERSION CONTROL

BCP owners are responsible for ensuring their BC Plan is subject to regular review and update, either as part of a planned review, to reflect significant changes or as part of the post-invocation process. Support and advice should be sought from the BC Manager as required.

In any case, all reviews of BC Plans should be subject to version control identifying the following:

- Date the document was changed
- Person/team making the change
- Person authorising the change
- Brief description of the change made
- Version number
- Date of next planned review

The BC Manager is responsible for maintaining copies of the current library of plans in a central repository and for retaining previous versions in an archive. BCP owners are responsible for ensuring that current copies of their BC Plan are available both electronically and in hard copy at designated and secure locations.

Appendix 1 – CCG Functions RAG rating

CATEGORY 1 **Critical - resume** **within 24 hours**	Emergency Preparedness - Planning and Response
	Oversight, Management and Monitoring of communications and Engagement
CATEGORY 2 **Essential- Resume** **within 24 – 48** **hours**	Authorisation of payments to NHS provider organisations
	Authorisation of payments to essential suppliers and independent contractors
	Authorisation of payments to non-essential suppliers and independent contractors
	Financial external returns to NHSE, including monthly finance information and financial plan returns etc.
	Quality and Performance - Statutory/external activity return
	Continuing Healthcare Decision making
	Safeguarding
	Serious Incidents
	Authorisation of payments to NHS provider organisations
	Authorisation of payments to essential suppliers and independent contractors
	Authorisation of payments to non-essential suppliers & independent contractors
	Individual Funding Requests
CATEGORY 3 **Routine - Resume** **as soon as** **practical (ideally 2** **weeks)**	Complaints Management
	Freedom of Information request processing
	Maintenance of Assurance Framework and Risk Register
	Manage the business agendas for the CCG Governing Body, Executive Team and subcommittee meetings; minute taking process delivery and supervision
	Overseeing the delivery of the HR, corporate governance and information governance functions of the CSU.
	Corporate Health and Safety
	QIPPs relating to Primary Care
	Primary Care activity / quality
	Service Redesign - Primary Care Element
	Development of QP pathways and establishment of monitoring systems
	Support of Primary Care Contracting
	Financial and contract management function including, preparation of finance and contracting reports for CCG Governing Body etc.
	Financial and contract management function including, preparation of finance and contracting reports for CCG Governing Body etc.
	Financial and contract management function including, preparation of finance and contracting reports for CCG Governing Body etc.
	Key Provider Contract Management meetings Planning and Forecasting
	Ad hoc data analyses
	Management, development and ongoing monitoring of compliance and performance against the quality expectations within main provider contracts, assessment of performance on quality schedule
	KPIs and CQUIN delivery
	Management of the GP Feedback System
	Strategic Planning - coordinating the processes required to deliver strategic and operational plans
	Organisational Development - liaise with team in ACS to enable and monitor delivery of SLA
	Equality and Diversity - liaise with ACS lead to ensure CCG compliance and commitment to this agenda