NHS
Barnsley Clinical Commissioning Group

Putting Barnsley People First

Business Continuity Policy

Version:	2.0
Approved By:	Governing Body
Date Approved:	August 2015 – Reviewed October 2016
Name of originator / author:	Jamie Wike, Head of Planning, Delivery and Performance and Ricard Walker, Head of Assurance
Name of responsible committee/ individual:	Governing Body
Name of executive lead:	Jamie Wike, Head of Planning, Delivery and Performance
Date issued:	13 October 2016
Review Date:	2 years from date of implementation
Target Audience:	All employees

DOCUMENT CONTROL

Version No	Type of Change	Date	Description of change
V 0.1	New Policy	November 2014	Replaces previous PCT policy and reflects CCG responsibilities as identified in the NHS Commissioning Board Business Continuity Framework and Guidance
V 1.0	New Policy	20 December 2013	Approved version incorporating minor changes requested by Governing Body on 12 December 2014 in relation to emergency powers and urgent decisions (para 1.4), and, testing of Business Continuity arrangements (para 12.1)
V 1.1	Review	August 2015	Minor changes following routine review including changes to reflect structural arrangements and regional configuration of NHS England
V 2.0	Review	October 2016	Minor changes to add a definition of a Business Continuity Incident (2.3), add an additional incident for Loss of Fuel (6.6 and Appendix 1) and update accountabilities to reflect the change to the Emergency Accountable Officer from the Chief of Corporate Affairs to the Head of Planning, Delivery and Performance

Contents

1. Introduction

1.1 The CCG along with its partners has a duty to protect and promote the health of the community, including in times of emergency. We are committed to complying with legislation and guidance in relation to emergency preparedness and business continuity management. Detailed in the '*NHS Emergency Preparedness Framework 2015'* and the '*NHS England Business Continuity Management Framework 2013'*

1.2 The role of the Clinical Commissioning Group (CCG) is to commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will develop, maintain and continually improve the business continuity management systems. This means having suitable plans which set out how the organisation will maintain continuity in its services during a disruption from identified local risks and how the organisation will recover delivery of key services in line with ISO22301. This policy is important because it will help the CCG make sure that it can continue to deliver its business on behalf of patients in times of disruption.

1.3 The CCG recognises the potential operational and financial losses associated with a major service interruption, and the importance of maintaining viable recovery strategies.

1.4 This policy statement is intended to provide a framework for the CCG to follow in the event of an incident such as fire, flood, bomb or terrorist attack, power and/or communication failure or any other emergency that may impact upon the daily operations of the CCG. It describes the proposed policy for implementing and maintaining a suitable business continuity process within the CCG, including the roles and responsibilities of the officers with the responsibility for implementing it. In extreme circumstances, the CCG's Emergency Powers and Urgent Decisions arrangements, as set out in the Standing Orders incorporated within the Constitution, will apply.

1.5 This policy statement will support the organisation to think ahead in order to avoid or mitigate risk, take corrective action and be in control of the outcome of an emergency.

1.6 The Cabinet Office standard, ISO 22301 lays out the requirements for business continuity management. The business continuity plan (BCP) is designed to meet the requirements of this standard.

2 Definition - Business Continuity Management (BCM):

2.1 An holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause and which provides a framework for building organisational resilience with the capability for an effective response that

safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

2.2 The diagram (figure 1) illustrates the Business Continuity Management (BCM) Cycle to develop a robust BCM culture across the organisation.

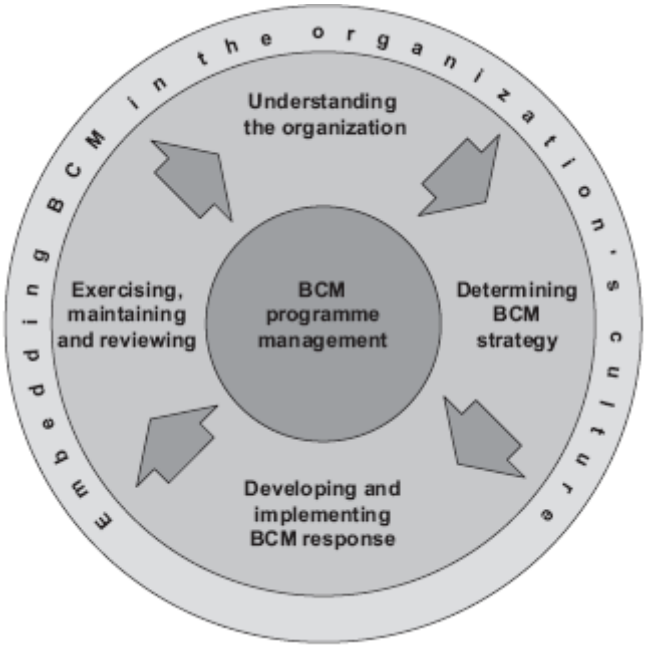

Fig 1

2.3 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.

3. Aims and objectives of the Policy

3.1 The aim of this policy is to enable the response to business disruptions to take place in a co-ordinated manner, in order to continue key business operations at the highest level achievable in the circumstances.

3.2 The key objectives of the policy are:

- To identify key services which, if interrupted for any reason, would have the greatest impact on 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 maintain and / or resume key services in the shortest possible time.

3.3 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

4. What should be included in the Business Continuity Plan?

- **Business Impact Analysis / Hazard identification – Local Risk Assessment**
  The process of identifying business functions and the effect a business disruption will have on them. Risk assessment is the process of risk identification, analysis and evaluation using a risk matrix.

- **Critical Activities**
  Those activities whose loss would have the greatest impact in the shortest time and need to be recovered most rapidly.

- **Communications Strategy**
  Internal and external communications and how the CCG cascades information.

5. Where the organisation may need a Business Continuity Plan

5.1 The list below provides examples of what might be considered an event to invoke a BCP. The list is not exhaustive and judgement will be applied in each case:

- loss of workplace short and long term;
- loss of information and communications technology infrastructure services for up to five days;
- loss of key staff short and long term;
- significant national or international incident impacting on the CCG, such as pandemic;
- any requirement as identified by the business impact analysis process;

6. Risk Analysis of the Business Continuity Plan

6.1 The response to an emergency incident does not necessarily or automatically translate into the declaration of a major incident and the implementation of a full recovery operation.

6.2 Incidents may cause a temporary or partial interruption of activities with limited or no short term or longer term impact. It will then be the responsibility of the CCG Executive team, as available, to evaluate and declare the appropriate

level of response.

6.3 The Severity of an incident will be identified as follows:

- Insignificant;
- Minor;
- Moderate;
- Major and
- Catastrophic.

6.4 The severity level will indicate the urgency of recovering the business service, and also the order in which services should be reinstated.

6.5 The CCG is not responsible for the direct provision of health services, however it is responsible for some functions that have a direct impact on providers of health services, for example safeguarding. Therefore the risks to our stakeholders resulting from a Major incident affecting the CCG could be significant.

6.6 A series of robust plans and mitigation actions have been developed for the following priority incidents:

- unavailability of premises for more than five working days caused by fire, flood or other incidents;
- major electronic attacks or severe disruption to the IT network and systems;
- terrorist attack or threat affecting transport networks or the office locations;
- denial of access to key resources and assets;
- significant numbers of staff prevented from reaching CCG premises, or getting home, due to bad weather or transport issues;
- theft or criminal damage severely compromising the organisation's physical assets;
- significant chemical contamination of the working environment;
- illness/epidemic striking the population and therefore affecting a significant number of staff;
- simultaneous resignation or loss of a number of key staff;
- widespread industrial action;
- significant fraud, sabotage or other malicious acts; and
- Loss of fuel due to industrial action, terrorism or other causes.

7. Cascade process

7.1 Immediate response and management functions required to handle an incident will be led by the most Senior CCG Officer on site/on call. A cascade

structure will be developed to ensure key individuals within and external to the organisation have been informed.

7.2 The CCG Officer will lead any business continuity incident and if necessary utilise the Incident Response Plan to provide any resources required.

8. Accountability

8.1 In order for the CCG to develop a good long-term business continuity capability, it is essential that all staff take on an appropriate level of responsibility.

8.2 Governing Body

BCM is an important part of the organisations risk management arrangements. The Governing Body will ratify this Policy.
Governing Body members need to assure themselves that up to date policies and plans are being implemented effectively in the event of an incident.

8.3 Chief Officer / Executive Team

- Will oversee the implementation of the business continuity policy and standards;
- Will review the business continuity status and the application of the policy and standards in all business undertakings;
- Will enforce compliance through assurance activities; provision of appropriate levels of resource and budget to achieve the required level of business continuity competence;
- Will co-ordinate the overall management of a crisis, providing strategic direction of service recovery plans; and
- Ensure information governance standards continue to be applied to data and information during an incident.
- Will decide when to escalate to the area team.
- Will lead the recovery plan after the incident.

8.4 Emergency Accountable Officer (Head of Planning, Performance and Delivery)

- Will determine the criteria for implementing the Business Continuity Plan;
- Will manage training and awareness of the plan; and maintaining the plan.
- Will be responsible for change control, maintenance and testing of the plan.
- Will ensure the BCP is reviewed and updated at regular intervals to determine whether any changes are required to procedures or responsibilities.

8.5 Team managers

Individual managers will be required to assess their specific area of expertise and plan actions for any necessary recovery phase, setting out procedures and staffing needs and specifying any equipment or technical resource which may be required in the recovery phase.

8.6 All CCG staff

- Achieve an adequate level of general awareness regarding business continuity;
- Being aware of the contents of their own business areas disaster recovery plan and any specific role or responsibilities allocated;
- Participate actively in the business continuity programme where required; and ensuring information governance standards continue to be applied to data and information during an incident.

9. Communications strategy

9.1 Good communication is essential at a time of crisis. A communications strategy/plan is included within the Business Continuity Contingency plan out describes the arrangements for appropriate internal and external communication and processes for ensuring communication to all staff in the case of an emergency. This strategy will be the same across all plans.

10. Business Continuity and Incident Response

10.1 A Business Continuity Contingency Plan has been developed and shared with Senior Managers and employees as appropriate to ensure awareness of the plan and the roles and responsibilities. The Plan is accessible on the CCG website. The contents of the Plan will be reviewed, checked for completeness and updated regularly to reflect changes to business continuity guidelines, frameworks and processes, or whenever there is a change in this policy which may affect its contents.

11. Training and awareness

11.1 Appropriate levels of training and awareness sessions will be developed and put in place for all CCG staff to ensure business continuity becomes part of CCG culture and daily business routines, improving the organisations resilience to the effects of emergencies.

12. Testing

12.1 The on-going viability of the business continuity program can only be determined through continual tests and improvements. The Chief of Corporate Affairs will be responsible for ensuring regular tests and revisions are made to the BCP to ensure they provide the level of assurance required. Testing will cover potential scenarios based on the areas included at section 6.6 of this policy and will include cascade arrangements, communication plans and response.

12.2 If there is a major change to the CCG's role and structure, plans will be tested and revised once a 'settling-in' period has been achieved, to allow for a confident level of response and recovery.

13. Appendices

- Business Impact Analysis

Business Impact Analysis / Hazard Identification – NHS Barnsley Clinical Commissioning Group

Hazard	Likelihood	How the hazard affects business	Impact	Risk Score	Controls in Place	Short Term (under 72 hours) action	Longer term action	Action Card number
Fire	1	Loss of use of some or all of premises	4	**4**	Fire Procedures	Staff work at home or hot desk at other sites where they have access	Temporary alternative work base for key staff, to enable point of contact and email/internet access	1,3,4,5
Flood	1	Loss of use of some or all of premises	4	**4**		Staff work at home or hot desk at other sites where they have access	Temporary alternative work base for key staff, to enable point of contact and email/internet access	1,3,4,5
Terrorist or criminal attack	1	Loss of use of premises. Possible loss of staff	4	**4**	Emergency response plan	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.	1,2,3,4,5
Significant chemical contamination	1	Loss of use of premises. Possible loss of staff.	4	**4**	Emergency response plan	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.	1,2
IT failure/loss of data	2	No access to email, electronic files, telephones	4	**8**	IT back-up systems	Remote working through NHSNet. Access to paper files.	As short term	3

Hazard	Likelihood	How the hazard affects business	Impact	Risk Score	Controls in Place	Short Term (under 72 hours) action	Longer term action	Action Card number
Loss of power	2	No access to email, electronic files, telephones Loss of use of premises	3	**6**	Back-up generator?	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary generator? Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.	1,3,4,5
Loss of water	2	Access to Toilets and beverages Cleaning functions	3	**6**		Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected	Temporary portable loos Bottled water Water brought in / Stand pipes	1,4
Loss of Telephone (landline)	2	Limited telephone communication. Possible impact on email/internet?	3	**6**		Use of mobile phones. Staff work from home?	Temporary alternative work base for key staff, to enable point of contact and email/internet access	1,4
Simultaneous resignation of a number of key staff	1	Loss of leadership function	4	**4**	Notice period in contracts	n/a	Accelerate normal recruitment processes. Seek secondments to cover gap and provide continuity.	2
Staff Illness/epidemic	2	Loss of significant number of staff	4	**8**		Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.	2

Hazard	Likelihood	How the hazard affects business	Impact	Risk Score	Controls in Place	Short Term (under 72 hours) action	Longer term action	
Commissioning support unable to deliver appropriate support	2	Loss of support staff or business functions	4	**8**	Provisions of the SLA with the CSU	Use directly employed staff and/or agency staff to deliver critical functions CSU action	eMBED / host to remedy. If it cannot, seek alternative sources of support and compensation from supplier.	2,3
Travel disruption preventing staff getting to base	2	Loss of significant number of staff	3	**6**		Staff work at home or at other premises or organisations	As short term, if necessary (long term impact less likely)	1
Travel disruption preventing staff getting home	2	Staff wellbeing affected. Disruption to work due to need to accommodate staff.	3	**6**		If possible, obtain food and blankets to enable staff to stay overnight.	As short term, if necessary (long term impact less likely)	1,2
Widespread industrial action	1	Loss of significant number of staff	4	**4**	Staff engagement and HR policies	Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.	2,3,6
Theft or damage to assets	2	Loss of use of e.g. computers, furniture	3	**6**	Security policies	Staff work at home. Bring old equipment into use?	Purchase or hire replacements	1,3,4,5
Significant fraud or other criminal act	1	Loss of access to funds? Restriction placed on business activities?	4	**4**	Security policies	Suspend transactions or seek assistance from partner organisations.	Seek assistance from partner organisations.	2
Loss of Fuel due to industrial action, terrorism	1	Staff unable to get to work or travel to meetings	4	**4**		Staff work at home or at other premises or organisations	As short term, if necessary (long term impact less likely)	6

Risk Scoring		
No	**Probability Scores**	**Impact Scores**
1	Rare	Negligible
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost Certain	Catastrophic

Risk Matrix
Low 1 - 3
Moderate 4 - 6
High 8 – 12
Extreme 15 - 25