BUSINESS CONTINUITY & STRATEGY POLICY

Authorship:	**Chris Wallace, Information Governance Manager**
Committee Approved:	**Integrated Audit and Governance Committee**
Approved date:	**11th March 2014**
Review Date:	**March 2016**
Equality Impact Assessment	Screening
Sustainability Impact Assessment **Target Audience:**	Completed All Staff
Policy Reference No:	
Version Number:	1.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	KGT	Initial structure and headings		
0.2	KGT	Development of content		
0.3	KGT	Development of content		
0.4	KGT	Further content development and formatting		
0.5	KGT	Content and appendices added/updated		
0.6	KGT	Minor content and formatting changes		
0.7	KGT	Changes in response to feedback		
0.8	Chris Wallace	Updated for CSU and amended formatting		
0.9	Barry Jackson	Final draft for approval		
1.0	Barry Jackson	Approved version		

CONTENTS

1   INTRODUCTION

This combined Strategy & Policy provides the high-level framework for the organisation to manage and deliver its Business Continuity responsibilities. These responsibilities arise from a number of sources, and include statutory drivers such as the Civil Contingencies Act (2004), the Data Protection Act (1998), and compliance drivers such as the Information Governance Toolkit (IGT) and the CSS Authorisation and Establishment requirements.

The document sets out the requirements and expectations the organisation will need to remain aware of and in many cases develop from first principles to ensure there is an effective set of arrangements in place covering an array of related issues such as:

- Corporate and personal responsibilities
- Assurance and governance
- Training and development
- Legal requirements and implications
- Managing relationships with third parties
- Budgets and expenditure
- Mutual aid
- Development, testing, maintenance and review of individual BC Plans

This document represents the starting point for a programme of related processes, projects and initiatives that will take time to become embedded within the organisation. As such, this document will be subject to regular review to ensure it continues to support the organisation in the development of Business Continuity Management (BCM) as a key contributor to the corporate governance, assurance and legal responsibilities of the organisation.

2   ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3   IMPACT ANALYSES

3.1 Equality

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

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

4   SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

The development of this document is taking place at a time when the organisation is under-going a period of significant organisational change.

The organisation does not operate in isolation and has extensive networks and relationships with external parties, both NHS and those from the private sector. This document recognises the importance of managing these third party relationships but they are not included within its scope. The organisation is reviewing and progressing the development of its BCM capacity and capability, those third parties relied upon to deliver the organisation's critical services will be expected to have their own BCM frameworks in place.

The document Chapter headings are based on the structure of BS25999-2, the recognised BC Management standard for both the public and private sectors. This Standard is due to be replaced with the International Standard ISO22301 in November 2012. Any future intention to benchmark against or adopt a formal BCM framework should reference ISO22301.

5   POLICY PURPOSE & AIMS

Developing a BCM Strategy & Policy framework from first principles is a challenging programme. This document provides support to both individuals and service teams by setting out what is required at both a strategic, operational and tactical levels within the organisation.

The detailed development of Business Continuity Plans (BCPs) will necessarily take place at team or department level and will need to be owned and maintained at that level. Should they ever be needed (or 'invoked') then it will be the team or department who will initially implement their BCP because they will have identified their core or 'critical' functions, processes and systems and included response, recovery and resumption activities in advance within their BCP.

By implementing this Strategy & Policy, the organisation will be able to maintain the momentum, pace and direction of its BCM programme to ensure that all teams develop together with lessons learned shared across the organisation, and continual improvement delivering shared benefits to all staff.

Understanding the Organisation

5.1 Business Critical Functions, Systems & Processes

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.

5.2 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.

5.3 Legal Requirements & Implications

This Strategy & 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.

5.4   Business Impact Analysis (BIA)

The aim of BIA is to identify, record and assess:

- Critical activities;
- Dependencies required to deliver these activities - these may be internal and external;
- The impact of disruption to these activities, including the financial consequences;
- The timescales for recovery;
- Recovery profile, e.g. resources, equipment, etc;
- Recovery options.

A proforma has been developed to support this process and is available from the BC Manager.

5.5   Risk Management

This Strategy & 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.

5.6   Resource Management

Implementation of this Strategy & Policy will require commitment in terms of staff time and there may be resource implications as a consequence of reducing risk or increasing resilience. It is expected that any such resource implications will be identified whilst completing either the BIA or risk assessment processes.

It is the responsibility of BCP Owners to highlight resource requirements to their line manager so that a decision can be taken on the most cost-effective solutions to be implemented, taking into account the benefits to be delivered.

5.7   Managing relationships with Third Parties

This document aims to ensure the organisation is willing and capable of working with the wide range of Third Parties that either provide 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.

5.8   Mutual Aid

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 Strategy supports a similar approach being adopted for BC Planning.

Determining Business Continuity Strategies

5.9   Business Continuity Strategy Options

This document recognises that not all functions, systems and processes can have an equal amount of protection; neither can they all be recovered at the same time in a BC scenario. Consequently, the document encourages the development of the concept of a 'recovery class' approach when determining risks and recovery priorities.

5.10   Recovery Classes

A Recovery class (as defined below) is determined by the business and relates to business functions, not technical drivers:

- Zero – no reason to recover business function during BC/disaster scenario
- One – regarded as a non-vital and low priority business function
- Two – business functions ordinarily considered 'vital' but not the most important
- Three – considered 'critical / must have' business functions
- Four – business functions that need to be continuously available, absolutely cannot go off-line for any reason or for any amount of time

Where a function, system or process is ceased or considered a low recovery priority, especially if this leads to the suspension of service(s), then the affected parties must be informed at the earliest possible opportunity as part of the Communications Plan, which will form part of the larger BC Plan.

5.11   BC Budget & Expenditure

In a BC scenario, normal operational procedures relating to budget and expenses management may be disrupted either directly (e.g. loss of key systems) or indirectly (e.g. systems are available, but staff cannot access necessary documentation or buildings).

BCP Owners are required to take this into account when completing their BC Plans and put contingency arrangements in place so that budgets can be accessed, especially if the

expenditure is required to support the recovery effort. In some cases, i.e. for those functions that fall within recovery class 4, agreement should be reached about identifying a BC 'reserve' budget, including the budget value, budget holder and budget authorisation and audit procedures.

Developing & Implementing a BCM Response

5.12   BC Plan development and maintenance / structure

The BC Manager will be responsible for co-ordinating the production and maintenance of departmental or service BC Plans. This will include the provision of relevant templates, training support and arranging plan exercises and tests. However, the development and maintenance of the BC Plans remain the responsibility of the BCP Owner as they and their team(s) are familiar with the day-to-day operational environment and will have vital roles to play in any recovery effort.

This will be made explicit in the BC Plans for each department or service.

BC Plans will adhere to an agreed structure and format as developed by the BC Manager. BCP Owners and their teams are responsible for ensuring any supporting procedures are documented and appended to the BC Plan as appropriate.

BC Plans should consider relevant factors across the following areas:

- People – how would your department or service cope with the loss of key staff (numbers) or staff with specialist skills that are difficult to replace?
- Premises – how would your department or service cope with the loss of access to buildings, offices, clinics, wards, equipment?
- Processes - how would your department or service cope with the loss of IT, phones, documentation, data?
- Providers - how would your department or service cope with the loss of supplies, contractors/service providers, power, water?
- Profile - how would your department or service cope with the loss of reputation/organisation by patients, public, partners, stakeholders?

5.13   Invocation arrangements

Each BC Plan will make explicit the arrangements for invoking the plan. In most scenarios, a plan will have its own 'lifecycle' covering the following:

- Prepared – the plan is written but inactive;
- Stand by – something has occurred that raises cause for concern, and the potential for implementing continuity arrangements has increased;
- Invocation – the plan is implemented and staff assume their responsibilities as defined in the plan in aid of the recovery effort;
- Stand down – the recovery aims and objectives within the plan have been achieved and the start of return to 'business as usual' is underway;
- Review – the effectiveness of the plan and any lessons learnt are captured and fed into a revised version.

Of course, in some situations the 'stand-by' stage may be bypassed if the scenario is serious enough or happens at very short notice. In any case, responsibilities for invoking and co-ordinating the BC plan should be made explicit in all departmental or service plans.

5.14   Ownership of BC Plans

BCP Owners are responsible for their departmental or service BC Plans, working with the BC Manager for advice and support as required.

5.15   BC team training and management

Staff filling key roles within their BC Plan are responsible for ensuring they are appropriately trained and capable of fulfilling the roles and responsibilities assigned to them. This could be achieved by completing relevant BC training and/or by taking part in organised plan exercises.

Those with responsibilities for invoking and co-ordinating activities within the plan should ensure that they and their team(s) are equipped to deliver the plan should it be necessary. Support from the BC Manager should be sought if required

5.16   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 include consideration of the following:

- 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;
- Identify 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;
- Identify 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;
- Identify 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.

5.17 Major Incident Planning

This Strategy & Policy has been developed to support the Major Incident Planning process, recognising that a 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 BC Manager is responsible for ensuring there is on-going dialogue and collaboration between the BC function and those teams with Major Incident Planning responsibilities.

5.18 Ensuring BC plan availability and version controls are maintained

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:

- The date the document was changed;
- The person/team making the change(s);
- The person authorising the change(s);
- A brief description of the change(s) made;
- The version number (minor changes should be in the format 0.1, 0.2 etc; major changes should be in the format of 1.0, 2.0, 3.0 etc);
- 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.

BCM Exercising

5.19 Testing Framework and scenarios

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 Strategy & 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.

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

Passive, includes	**Active/Passive**, includes	**Active**, includes
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).

5.20   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 Chief Finance Officer.

5.21   Capturing lessons learned and improving 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.

6   DEFINITIONS

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.

Business Continuity Management (BCM)

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

A series of business continuity activities that, collectively, cover all aspects and phases of the business continuity management programme.

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.

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

An event, whether anticipated or unanticipated, that may cause an unplanned, negative deviation from the expected delivery of critical services according to the organisation's objectives.

Major Incident Planning (MIP)

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. 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.

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 (SoP's)

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.

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.

7 ROLES / RESPONSIBILITIES / DUTIES

For the BCM Programme 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.

The Sections below provide summary details of the responsibilities of key individuals and Committees, and the more general requirements affecting all organisation staff.

7.1 Chief Officer

The Chief Officer Officer (CEO) has overall responsibility for business continuity management within the organisation and is responsible on behalf of the organisations Board for ensuring the implementation of business continuity arrangements throughout the organisation. The CEO has specific responsibility for:

- The implementation of the Business Continuity Strategy & Policy;
- Ensuring that the organisations Board is kept fully informed of significant business continuity risks, and any associated significant developments or issues;

- Ensuring there is specialist advice on business continuity matters and that this is available to the Organisation;
- In conjunction with the Chief Finance Officer ensure financial resources are available, if necessary, to implement relevant Business Continuity Plans;
- Ensuring there is the production of relevant Business Continuity Plans associated with this Strategy;

7.2   Organisation Board

The Organisation Board will be responsible for:

- Ensuring appropriate structures are in place to implement effective business continuity arrangements;
- Setting Key Performance Indicators which will measure the extent and success of BCM implementation and maintenance;
- Monitoring the implementation of the Business Continuity Strategy & Policy through the organisation's IMT Senior Management Team;
- Committing resources necessary to adequately control identified business continuity risks.

7.3   Governance & Quality Committee

This Committee will receive reports from the Chief Finance Officer detailing how it is being implemented and highlighting any areas of concern. Where appropriate, the Committee will seek independent assurances from either Internal or External Audit in the form of an audit report detailing findings and recommendations.

7.4   Chief Finance Officer

This is the Executive Director accountable for the implementation and maintenance of the BC Strategy & Policy, in particular:

- Ensuring there is a Corporate framework for implementing, maintaining and improving the organisation's BC capability and capacity, in collaboration with other members of the Corporate Senior Management Team;
- Appoint a BC Manager for the organisation, and ensure all BC Plans have a nominated Owner.

7.5   Executive [or Associate] Directors

Executive or Associate Directors have a responsibility for ensuring that:

- Systems procedures have been developed, implemented and staff appropriately trained to prevent business interruptions;
- The Business Continuity Strategy & Policy is implemented within their own directorate and in particular that each critical function within the directorate has its individual Business Impact Assessments and appropriate contingency arrangements in place;
- 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;

- Managers and staff co-operate in applying this document throughout their directorate with the involvement of relevant organisation managers;
- Organisation staff are provided with appropriate business continuity management awareness training;
- They cooperate with any requests for information or evidence required for assurance or audit purposes.
- They will retain ownership and responsibility for the plans within their functional areas.

7.6   BC Manager

The BC Manager is responsible for:-

- Meeting with department heads to document and review their Business Impact Assessments on an annual basis or when necessary;
- Identifying training needs associated with this document, including appropriate Induction training and more specialist training for those filling specific roles such as Information Asset Administrators or Owners;
- Providing advice, guidance and instruction on business continuity matters, particularly the production of Business Continuity Plans;
- BCM policy development, maintenance and publication;
- Conducting business continuity exercises in line with national guidance and in liaison with the other organisation Managers, e.g. Emergency Planning Manager;
- Co-ordinating the annual update of departmental Business Continuity Plans;
- Ensuring copies of Business Continuity Plans are made available when required. Copies will be version controlled and held on the intranet, organisation headquarters and designated locations in order that easy access to the plan can be obtained;
- Embedding the culture of business continuity arrangements and responsibilities amongst staff and managers, through appropriate awareness raising campaigns.

7.7   Service Managers

Service Managers are responsible for the day to day implementation of the Business Impact Assessments within their own area and will act as the business continuity representative for their functional area. Specific responsibilities include:

- Ensuring the departmental Business Impact Assessments are updated annually and as and when any responsibilities, procedures or processes change;
- Ensure the Service BCP is maintained and updated, in collaboration with the BC Manager where necessary;
- Develop a reasonable level of staff awareness of this document and the Service Business Continuity Plan;
- Providing active membership of BC testing or review meetings if requested;
- Where they or their staff are filling the role of Information Asset Administrator or Owner, ensure that all relevant training has been completed and take part in any BC exercises that are required.

7.8   All Employees

Employees are expected to act in accordance with the information and instruction they have received on the organisation's business continuity arrangements 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.

8   IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

9   TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

10   MONITORING & AUDIT

This Strategy & Policy will be reviewed and maintained by the BC Manager on behalf of the Chief Finance Officer, in accordance with planned review periods. Strict version control will be maintained, consistent with the scheme at 5.18.

If necessary, e.g. in response to major organisational changes, increased risk levels, occurrence of serious or major incidents, this document may be reviewed ahead of planned review periods to ensure it remains fit for purpose. Any such ad-hoc changes will be notified to the Governance & Quality Committee.

10.1   Internal or external audit

This Strategy & 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.

10.2   Certification / Accreditation

Should the Organisation seek formal external recognition of its BC Strategy and Planning arrangements, this document may need to be revised to ensure it is consistent and compliant with any certification or accreditation standards, e.g. ISO22301. Advice will be sought on the changes that are required and the BC Manager will be responsible for implementing these.

10.3   Self reported assessment (internal)

Should it become apparent that this document is not fit for purpose, staff are encouraged to bring this to the attention of the BC Manager and/or the Executive Director responsible for BC Planning. The BC Manager will be responsible for on-going review of the document in any case.

10.4   Peer review

This document may benefit from peer review to ensure it is consistent with best practice and is providing a relevant framework for BC Planning in the future. The BC Manager will be responsible for identifying opportunities where this could be beneficial. Any such reviews must be endorsed by the EMT and/or the Chief Finance Officer in advance.

10.5 Continual Improvement

This Strategy & Policy promotes an ethos of continual improvement in relation to BC Planning. It is expected that through the combined effects of staff training, plan testing, internal and external review and capturing 'lessons learnt' both this document and individual BC Plans will benefit from increased refinement and improvement.

Recognising that all staff have a contribution to make to this process, they are encouraged to highlight areas where this document could be improved and make an active contribution to their departmental or service BC plans.

11   POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

12   REFERENCES

Supporting resources

1.   NHS Resilience & Business Continuity Management Guidance: Interim Strategic National Guidance for NHS Organisations (June 2008);
http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Consultations/Closedconsultations/DH_085422

2.   Business Continuity & Disaster Planning – Good Practice Guidance (October 2009);
http://nww.connectingforhealth.nhs.uk/infrasec/gpg/disaster.pdf

3.   Information Governance Toolkit;
https://nww.igt.connectingforhealth.nhs.uk/Home.aspx?tk=410426945670569&cb=bd35a72c-a789-46a8-b27e-124cbcdd37e5&lnv=7&clnav=YES

- Relevant Organisation Policies

	1. Equality Impact Analysis
Policy / Project / Function:	Business Continuity & Strategy Use Policy
Date of Analysis:	13/01/14
This Equality Impact Analysis was completed by: **(Name and Department**)	C Wallace - IG Manager – CSU IG Team
What are the aims and intended effects of this policy, project or function ?	This combined Strategy & Policy provides the high-level framework for the organisation to manage and deliver its Business Continuity responsibilities.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

	2. **Equality Impact Analysis: Screening**				
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					

SUSTAINABILITY IMPACT ASSESSMENT

Policy / Report / Service Plan / Project Title:				
Theme (Potential impacts of the activity)	Positive Impact	Negative Impact	No specific impact	What will the impact be? If the impact is negative, how can it be mitigated? (action)
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			x	
Reduce the risk of pollution and avoid any breaches in legislation.			x	
Goods and services are procured more sustainability.			x	
Reduce carbon emissions from road vehicles.			x	
Reduce water consumption by 25% by 2020.			x	
Ensure legal compliance with waste legislation.			x	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			x	
Increase the amount of waste being recycled to 40%.			x	
Sustainability training and communications for employees.			x	
Partnership working with local groups and organisations to support sustainable development.			x	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			x	