Manchester Health & Care Commissioning

A partnership between
Manchester City Council
and NHS Manchester CCG

MANCHESTER
CITY COUNCIL

NHS
Manchester
Clinical Commissioning Group

Corporate Policy

RISK MANAGEMENT FRAMEWORK

Version: 4.1

Date Approved: February 2016

Document Control Sheet

Title of document:	Risk Management Framework		
Supersedes:	Risk Management Framework V3 (June 2015)		
Placement in Organisation:	Corporate Policy		
Consultation/Stakeholders	North, Central and South Manchester CCGs, CCG Corporate Governance Committee, Head of Corporate Services, Risk Leads		
Author(s) name:	David Smith, Corporate Governance Manager		
Department/Team:	Corporate Services Team		
Approved by:	Joint Governance Committee North, Central and South Manchester CCG Governance Committees		
Approval date:	February 2016	Review date:	February 2019
Implementation Date:	Upon Ratification		
Implementation Method:	1. CCG Governance Committees 2. Senior Managers/Service Managers 3. Newsletter (Manchester Matters) 4. CCG Website		
This document is to be read in conjunction with the following documents: North, Central & South Manchester Clinical Commissioning Groups Constitution			

Version Control

Version	Date	Brief description of change
V1.0	Apr 13	First version
Draft.v2.0	July 13	Initial draft issued to CCG Lead for comments
Draft.v2.0	Aug 13	Amended draft sent to CCG Governance Committee
V2.2	Oct/Nov 13	Sent to CCG Board for ratification
V.3	Feb 15	Sent to CCG Joint Governance Committee
V.4	Feb 16	Sent to CCG Joint Governance Committee for ratification to changes on the Information Governance Risks section (Appendix C)

PLEASE NOTE: The formally approved copy of this document is held on North, Central and South CCG's website. Printed copies or electronic saved copies must be checked to ensure they match the current online version.

Contents

Appendices

1.0 Introduction

1.1 The risk management framework is designed to provide a guideline and strategy for the development of a robust risk management system across the organisation. The framework will guide the CCG in its approach to the management of risk in all its activities and provides a structural framework with clear definitions and roles of responsibility.

It is the responsibility of all staff to contribute to the implementation of this policy through effective and appropriate identification and management of all risks to the organisation. The framework identifies how to report risks and how risks are governed within the CCG through an effective committee structure, which feeds up to the Board.

The framework will be reviewed regularly to reflect the changing environment in which the CCG is asked to operate, as well as any change in good practice and legislation.

2.0 Purpose

This document aims to provide all employees and contractors with the guidance to assist in proactively addressing and managing risks.

The risk management framework is in place throughout the organisation, to meet the following objectives:

- To understand risks, their causes, costs and how best to control them.
- To build on and maintain a risk register that details high level, corporate, operational, quality and health and safety risks.
- To provide assurances to the Board that risk management issues are being addressed locally and corporately.
- To establish risk management plans of action based on CCG risk registers.
- To ensure compliance against statutory requirements.

This document is applicable to all employees that work for the CCG.

3.0 Responsibilities

3.1 *CCG Board*

The Board are responsible for overseeing the risks identified within the organisation and for gaining assurance that the CCG is addressing risks which are considered serious to its strategic objectives.

Lay Members for governance will monitor the effectiveness of risk management through the committee structure to ensure that risk management is managed appropriately throughout the organisation.

3.2 *Accountable Officer*

The Accountable Officer is ultimately responsible for ensuring the organisation considers risk management throughout all its activities.

3.3 *Senior Management Team*

The Senior Management Team is responsible for ensuring that the Board, sub committees and departments are sufficiently equipped to be able to report on serious risks that may impact on the organisation's aims and objectives.

Additionally, each senior manager responsible for a committee of the Board will have to ensure the risk is discussed and given appropriate attention at their committee.

3.4 *Managers and Departments*

Managers and Departments are responsible for ensuring information on risks is incorporated into the organisation's risk register in line with this policy.

Individual departments are responsible for implementing management plans and actions connected to risks on the risk register.

3.6 *Corporate Governance Team*

The Corporate Governance Team (working across the three Manchester CCGs) has the responsibility of coordinating the process of risk management and advising the Board on all levels of risk through the appropriate governance arrangements and organisational structures. The team will work closely with employees, departments and stakeholders to proactively address risk management issues.

3.7 *All Staff*

All staff are responsible for identifying risks and implementing the risk management processes outlined in this policy.

4.0 Definitions of Terms Used

4.1 **Assurance** – an evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.

Departments – those working within the Manchester city wide teams to support the commissioning roles and responsibilities of the CCG.

Employee – an individual employed by the CCG directly or is contracted for a specific piece of work on a seasonal or short/ medium term basis.

Internal Control – any action taken to manage risk, these actions may be taken to manage either the impact if the risk is realised, or the frequency of the realisation of the risk.

Residual Risk – the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

Risk – uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance.

Risk Appetite – the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.

Risk Assessment – the evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised.

Risk Management – all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

5.0 Risk Management Framework

5.1 Risk Appetite

The CGG, by way of this framework, has agreed that acceptable and tolerated risks are all risks to the organisation that are graded below 6 on the standardised risk grading matrix. A full explanation of the risk grading matrix and acceptability of risks can be found in Appendix A of this policy.

5.2 Initiation of Risk

It is imperative that the CCG embed the processes for managing risk within all its activities. At the start of every new project, work stream or business plan the risk management framework must be considered and implemented.

Risk management is the priority of all staff and the successful management of risk relies on all staff initiating the risk management process.

5.3 Identification of Risk

5.3.1 *Risk Assessments*

Risk Assessment is a proactive approach to identifying risks within an organisation, department, project or working area. The process involves identifying hazards/risks/uncertainty, evaluating the extent of risks and taking the necessary actions to remove or reduce such risks.

The Corporate Governance Team will provide training to all members of staff who have a responsibility for managing risk, including guidance on undertaking risk assessments and how to use the Datix Risk Management System.

The risk assessment process should be continuously reviewed to maintain an accurate understanding of risk associated to the given area or project.

5.3.2 *Incident Reporting*

Reporting of incidents within the organisation highlights risk. All incidents, regardless of severity can identify risk to the organisation or its employees. 'Near Miss' incidents can act as an early warning indication of potential concerns for the future. 'Harm' or 'No Harm' incidents provide a record of what has already gone wrong. Appropriate analysis and investigation of individual incidents and trends can lead to risks being mitigated and managed in order to prevent further similar incidents.

All staff should be made to feel confident and empowered to report incidents and near misses. The reporting and management of incidents is outlined in further detail in the Incident Management Policy.

5.3.3 *Management of Complaints*

The management of complaints and concerns can help identify risks to organisational objectives. All complaints should be managed in accordance with the Patient Services Policy.

5.3.4 *Management of Claims*

The management of claims can help identify risks to organisational objectives. All claims should be managed in accordance with the Patient Services Policy.

5.3.6 *Management of Quality Issues*

Quality issues reported by member GP Practices concerning provider care can identify risk. These issues should be managed in accordance with the Incident Management Policy.

5.3.8 *Recommendations from Auditors or Inspectors*

Regular inspections and audits of the CCG can identify areas of poor performance or practice, this should result in risk assessments in the given area/department and any risks identified should be recorded and managed on the Datix risk register.

5.4 Control and Reporting of Risk

5.4.1 *Strategic Board Risks*

The Board will receive a high level summary document which brings together the principle strategic risks, their management, controls and subsequent assurances. Its purpose is to provide the Board with assurance that risk to the delivery of organisational objectives has been identified and is being managed.

Additionally the Board will also review all risks graded high (red/15+ on the matrix rating tool) in line with the CCG's risk appetite. These risks will be red risks which are relevant to the CCG as a whole - Project risks rather than red risks related to specific programmes within each project. The Board must assure itself that any unacceptable risk is being managed and any additional resources are made available to mitigate the risk.

The report will be received by the Board on a quarterly basis.

5.4.2 *Corporate Risk Register*

The corporate risk register holds all risks that are attributed to each committee, team or project. Each department/team holds the responsibility for ensuring that their risks on the corporate risk register are maintained and up-to-date. All risks on the corporate risk register will be subject to the agreed risk grading formula outlined in Appendix A.

The risk register will include information on (but not exclusively to):

- Description of risk
- Controls in place
- Risk grading
- Further actions
- Target risk grading
- Review date

Each risk on the corporate risk register will be assigned to a Committee. This Committee will receive a risk register of all their allocated risks at every meeting. Risks that are 'city wide' (e.g. those added to the corporate risk register by teams working across the Manchester conurbation) will be sent to Committees based on their risk type (e.g. risks assigned the type of 'quality' will be sent to the designated committee for quality).

A risk report will be submitted to the Governance Committee on a bi-monthly basis which will include the strategic risks, Governance specific risks and all 15+ risks for each committee. The corporate risk register will be reviewed in its entirety on a six monthly basis by the CGG Governance Committee.

6.0 Document Dissemination and Implementation

6.1 Once ratified this policy will supersede all previous CCG risk management frameworks. In order that this policy is disseminated and implemented correctly the following will occur after ratification:

- The policy will be published on the CCG website and relevant links sent out via the communications and engagement department.
- Manchester Matters will include a dedicated section on risk management including a link to this framework.
- The Datix risk management training is designed to match this framework and attendees are made aware of this framework.
- Senior managers will make their staff aware of this policy when questioned on risk.

7.0 Monitoring and Compliance

7.1 Monitoring

Committee	Report Title	Report Details	Timeframes
CCG Board	Board Risk Report	Strategic risks and risks graded 15+ on the corporate risk register	Quarterly
Governance Committee	Risk Report	Strategic risks, Gov specific risks and risks graded 15+ on the corporate risk register	Every Meeting
Committees of the Board	Risk Register	All open risks assigned to that committee	Every Meeting

7.2 Audit arrangements

An annual policy audit will be conducted and presented to the Governance Committee.

7.3 Training arrangements

Specialist training in the use of Datix is provided by the Corporate Governance Team for all lead persons with responsibilities for maintaining and managing incidents and risks.

8.0 References and Related Documents

8.1 Related Policies

This policy should be read in conjunction with the following policies:

- Incident Reporting Policy
- Patient Services Policy
- Information Governance Policies
- Standards of Business Conduct and Conflict of Interest Policy
- Whistle Blowing Policy
- Anti-Fraud, Bribery and Corruption Policy
- Development and Management of Procedural Documents Policy

Appendix A – Risk Guidance

Risk Rating

It is necessary to rate risk systematically using standard methodology, so that they can be placed into one of the three categories above. This allows prioritisation of remedial action. All incidents should be rated in 2 ways:

Assessment of Consequence

Choose the most appropriate domain for the identified risk from the left hand side of the table then work along the columns in the same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards

Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of <0.1 per cent of the total CCG budget Claim less than £10,000	Loss of 0.1–0.25 per cent of the total CCG budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.25–0.5 per cent of the total CCG budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >0.5 per cent of the total CCG budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Assessment of Likelihood of Reoccurrence
The tool described here provides a simple way of rating the potential risk associated with hazards. It requires an assessment of rating the potential consequences and the likelihood of recurrence of harm from the hazard. (A hazard is anything that has the potential to lead to or cause actual harm, the risk is how likely the hazard will cause harm).

Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur,possibly frequently

Risk Rating = Consequence X Likelihood

Measures of Consequence

Level	Descriptor	Description
1	Insignificant	No adverse outcome or injury
2	Minor	Short term adverse outcome
3	Moderate	Semi-permanent outcome or injury
4	Major	Permanent adverse outcome or Injury
5	Catastrophic	Death; Not meeting Statutory Duties

Measures of Likelihood of Reoccurrence

Level	Descriptor	Description
1	Rare	Can’t reasonably believe that this will ever happen again
2	Unlikely	Do not expect it to happen again but it is possible
3	Possible	May re-occur. Occasionally
4	Likely	Will probably re-occur but is not a persistent issue
5	Almost certain	Likely to re-occur on many occasions, a persistent issue

Risk Grading Matrix

Likelihood	Consequence				
	Insignificant	Minor	Modorate	Major	Catastrophic
Rare	1	2	3	4	5
Unlikely	2	4	6	8	10
Possible	3	6	9	12	15
Likely	4	8	12	16	20
Almost Certain	5	10	15	20	25

Risk Appetite and Grading

The Board is required to agree its strategic and corporate objectives and in doing so is required to identify the risks associated with achieving these objectives. These risks are assessed in regards to the level of controls and assurances that are in place and are scored on the severity (consequence) and likelihood of occurrence. The risk score achieved reflects the urgency and degree of action, if any, required for reducing or eliminating the risk.

These risks, dependant on their score are assessed in regards to severity (Consequence) and likelihood of occurrence and are categorised dependant on their score as ‘acceptable’, ‘manageable’ or ‘serious’ or shared should a risk be jointly owned or transferred should it be the responsibility of a partner organisation. The responsiveness and way in which these categories of risk are managed is depicted below:

Acceptable Risk (Very Low (Green 1–3), Low (Yellow 4-6))

Realistically it is never possible to eliminate all risks. There will always be a range of risks identified within the organisation that would require us to go beyond ‘reasonable’ action to reduce or eliminate them, i.e. the cost in time or resources required to reduce the risk would outweigh the potential harm caused. These risks would be considered ‘acceptable’.

Manageable Risk (Moderate (Orange 8 – 12))

The risk can realistically be reduced within a reasonable time scale through cost effective measures, such as training or new equipment purchase.

Serious Risk (High (Red 15 – 25))

The consequences of the event could seriously impact on the organisation and threaten its objectives. This category might include risks that are individually manageable but cumulatively serious, such as a series of similar incidents or quality issues. Risks identified as serious should be reported to the Senior Management Team.

Appendix B – Equality Impact Assessment Tool

GMCSU Equality Analysis Form

The following questions will document the effect of your activity on equality, and demonstrate that you have paid due regard to the Public Sector Equality Duty. The Equality Analysis (EA) guidance should be used read before completing this form.

	Section 1: Responsibility	
1	Name & role of person completing the EA:	David Smith
2	Service/ Corporate Area	Corporate Governance Team
3	Head of Service or Director (as appropriate):	Nick Gomm
4	Who is the EA for? Select from the drop down box.	Manchester North CCG
4.1	Name of Other organisation if appropriate	All Manchester CCGs
	Section 2: Aims & Outcomes	
5	What is being proposed? Please give a brief description of the activity.	A risk management framework document for all 3 CCGs
6	Why is it needed? Please give a brief description of the activity.	Staff to follow the risk management procedure, namely: to identify, record, control and manage risks to the organisation and themselves
7	What are the intended outcomes of the activity?	A safer organisation
8	Date of completion of analysis (and date of implementation if different). Please explain any difference	Today
9	Who does it affect? Select from the drop down box. If more than one group is affected, use the drop down box more than once.	CCG Staff
	Establishing Relevance to Equality & Human Rights	
10	**What is the relevance of the activity to the Public Sector Equality Duty? Select from the drop down box and provide a reason.**	

	General Public Sector Equality Duties	**Relevance (Yes/No)**	**Reason for Relevance**
	To eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by Equality Act 2010	No	
	To advance equality of opportunity between people who share a protected characteristic and those who do not.	No	
	To foster good relations between people who share a protected characteristic and those who do not	No	

10.1	**Use the drop down box and advise whether the activity has a positive or negative effect on any of the groups of people with protected equality characteristics and on Human Right**			
	Protected Equality Characteristic	**Positive (Yes/No)**	**Negative (Yes/No)**	**Explanation**
	Age	No	No	
	Disability	No	No	
	Gender	No	No	
	Pregnancy or maternity	No	No	
	Race	No	No	
	Religion and belief	No	No	

	Sexual Orientation	No	No	
	Other vulnerable group	No	No	
	Marriage or Civil Partnership	No	No	
	Gender Reassignment	No	No	
	Human Rights	No	No	
	If you have answered No to all the questions above and in question 10, explain below why you feel your activity has no relevance to Equality and Human Rights.			
	The policy asks all staff to act in the same way, using the same procedure, and to be findful of the same principles when undertaking work.			
	Section 4: Equality Information and Engagement			
11	**What equality information or engagement with protected groups has been used or undertaken to inform the activity. Please provide details.**			
	Details of Equality Information or Engagement with protected groups		**Internet link if published & date last published**	
			TBA	
11.1	**Are there any information gaps, and if so how do you plan to address them**	N/A		
	Section 5: Outcomes of Equality Analysis			
12	**Complete the questions below to conclude the EA.**			
	What will the likely overall effect of your activity be on equality?	None		
	What recommendations are in place to mitigate any negative effects identified in 10.1?	N/A		
	What opportunities have been identified for the activity to add value by advancing equality and/or foster good relations?	None		
	What steps are to be taken now in relation to the implementation of the activity?	Policy to be approved.		
Section 6: Monitoring and Review				
13	If it is intended to proceed with the activity, please detail what monitoring arrangements (if appropriate) will be in place to monitor ongoing effects? Also state when the activity will be reviewed.			
	Policy to be reviewed in 2 years or earlier if required.			

Appendix C – Information Governance Risks

Introduction

Information risk is a factor that exists in all areas where information of a personal or confidential nature is used and managed.

Information risk management is a part of Information Governance (IG) and it is acknowledged that IG, including the management of information risks should be part of the culture of the organisation, ensuring that staff are aware of, and work to, good IG (and therefore information risk) practices.

The CCG and their management teams are required to assure the formal introduction and embedding of information risk management into key controls and approval processes of all major business processes and functions of the organisation. Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the CCG continuously manages information risk.

Information Risk Management Processes

The information risk management process will take place using the NHS “5x5 Risk Matrix” as detailed in the NPSA’s “Risk Matrix for Risk Managers”. This document contains guidance on how to interpret the scores that will be attributed to risks and provides the basis for information risk reporting to the Corporate Governance Committee.

Privacy Impact Assessments

Risks to personal and confidential information that arise as a consequence of changes to systems (projects) will be identified via the completion of a Privacy Impact Assessment (PIA). This will be a risk assessment-based questionnaire completed by the Information Asset Owner (IAO) or other suitable project member and will be considered by IG Team and where necessary a report on information risks and actions to be taken will be produced. This will be managed as part of the overall project with oversight and sign off by the IG Team.

The PIA process and proforma are both available on the staff Intranet.

Local Information Risks

It is the Information Asset Owners or Information Asset Administrators responsibility to be aware of, and formally record, information risks for the assets they manage. Many risks will be managed and resolved locally, but higher risks will need to be recorded on Datix and managed jointly in cooperation with IG in order to ensure the CCG is aware of those risks and can be assured that active management of them is in place. Other risks that should also be recorded on Datix are risks identified to Data flow transfers of Personal Confidential Data (PCD) via different modes of communication. The IG team will carry out risk reviews of each asset with Information Asset Owners and at the same time conduct assessments of transfer of information, both ingoing and outgoing.

It is necessary to ensure a consistent approach to risk assessment and risk priority ratings so that all risks can be initially prioritised and ultimately agreed by the appropriate governance group. The use of the following tools will allow a consistent approach:

- Risk Management Process and Action Plans;
- Risk Analysis and Recording
  - Risk Consequence Table
  - Risk Rating Matrix
  - Information Governance Risk Assessment form
  - Risk Register Template
- Information Asset Register
- Privacy Impact Assessment

The CCGs board will be informed of significant risks.

Management of Information Risks

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. All breaches and incidents regarding information assets should be reported using the CCG’s online incident reporting system – Datix.

Information risks will be managed by the Information Asset Owner, unless the risk score attributed to an individual risk is 15 or greater, in these circumstances the Information Governance team should be contacted for additional support and advice.

The Risk Matrix and scoring is available for reference in this policy.
The treatment options for information risk are:

Avoid: not proceeding with activity likely to generate the risk.
Reduce: reducing or controlling the likelihood and consequences of the occurrence.
Transfer: arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint ventures, etc.
Accept: some risks may be minimal and retention acceptable.

Risks will be managed via a standard risk log format that will enable risks managed consistently across organisations ensuring a high quality level of support, where it is necessary.

Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated by the Information Governance team and the Risk Manager and action taken on a risk assessed basis.

All sensitive personal data will be handled as ‘confidential information’, kept securely in locked cabinets and via appropriate permissions on the network. It will be made available on a need-to-know basis and advice provided to staff as appropriate.

Policies are in place to support information risk management including information security, data protection, confidentiality and Records Management on the CCG’s intranet.

All internal staff as well as third parties, contractors, agency staff will be required to sign and follow the CCG's Data Protection Act and Confidentiality clauses.

PIA will be carried out as necessary where new systems have the potential to negatively impact on personal privacy. The PIA Proforma is available on the CCG's intranet.

Escalation of Information Risks

The IAO will be responsible for managing the risks, reporting and ensuring that suitable mitigations are put in place either locally or with support from information governance/risk management.

The Senior Information Risk Owner (SIRO) is responsible for ensuring that this policy is followed and to be aware of all risks.

The Joint Governance Committee is responsible for escalating high risks to the board and ensuring that where relevant they are admitted to the corporate risk register.

Proactive planning will be undertaken for investigating and identifying risks through different scenarios, regular policy reviews, Information Commissioner's Office (ICO) recommendations and assessment of sources of legal weight and admissibility of evidence for reducing risks.

Information Risk Management Training

The Health & Social Care Information Centre's (HSCIC) **- IG Training Tool** is an online training tool focused on all aspects of learning about IG. The aim of the tool is to develop and improve staff knowledge and skills in the IG work area.

It is advised that as a part of the CCG's Information Risk Management approach, SIROs and Information Asset Owners must complete the following online modules: -

SIRO must complete the following annually:-

- Information Risk Management for SIRO and IAO).

Information Asset Owner:-

- Information Risk Management for SIRO and IAO must be completed once every 3 years

As new Information Asset Owners are identified, they will be asked to complete the dedicated training.

Information Asset Register (IAR)

The Information Governance Team will work closely with IAOs to establish and maintain an Information Asset Register to ensure that all Information Assets (IAs) are identified and the information risks managed appropriately:

The IAR process will involve:-

- All IAs will be included on the IAR and their IAO identified. The IAR will also identify business critical assets, Information Asset Administrators (IAA) and risk assessments

- Evidence of Business Continuity Plans and Risk Reviews for all business critical assets.

The Information Governance Team will work closely with IAO's to ensure Business Continuity Plans (BCP) are in place for all critical assets. This will involve the completion of a local BCP Template and the collection of evidence from third party suppliers if required.

The Information Governance Manager will lead a review of the IAR on a six monthly basis to ensure it is kept up to date, complete and robust. The SIRO will sign off the output of the review.

Samples of typical assets are below:

Personal Information Content	**Software**
• Databases and data files • Back-up and archive data • Audit data • Paper records (patient case notes and staff records) • Paper reports	• Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware including PCs, • Laptops, PDA, communications devices e.g. iPhones and removable media
System/Process Documentation	**Miscellaneous**
• System information and documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services e.g. power • Air-conditioning • People skills and experience Shared service including Networks • Printers • Computer rooms and equipment • Records libraries