NHS Rotherham Clinical Commissioning Governing Body

Governing Body – 6th December 2017

Information Governance Policy and Management Framework and Information Security Policy

Lead Executive:	Ian Atkinson, Deputy Chief Officer
Lead Officer:	Andrew Clayton, Head of Informatics
Lead GP:	

Purpose:

Approval of the following policies:

- Annual review of the CCGs Information Governance Policy and Management Framework
- Information Security Policy

Background:

It is a mandatory requirement for compliance with the Information Governance Toolkit for the CCG to have an Information Governance Policy and Management Framework. This document should be reviewed on an annual basis and signed off at a Senior Management level at the CCG.

Effective information security management is essential to NHS Rotherham CCG. The objectives of the Information Security policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned, used or held by NHS Rotherham CCG

Analysis of key issues and of risks

The CCG's Information Governance Policy and Management Framework has been reviewed by the eMBED's Senior Information Governance Specialist to ensure that the mandatory elements of the documented have been included. There have been no major changes to the content of the policy from that of last year. All the mandatory requirements are included. Changes made include:

- References to new DPA/GDPR added
- Included role of Data Protection Officer as defined by GDPR (although not required in post until 25th May 2018)
- Training section amended to include new mandatory Data Security training

The CCG has not previously had an Information Security Policy in place. This policy takes into account of the NHS Information Governance aims and expectations set out within the Information Security Management: Code of Practice for the NHS and the Health and Social Care Information Centre (HSCIC) guidance relating to cyber security incidents. The purpose of information/cyber security is to ensure business continuity, to minimise the impact of security related incidents and to ensure the integrity of the information and data held by NHS Rotherham CCG. Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to that security.

Patient, Public and Stakeholder Involvement:
Both policies have been reviewed by IG Group
Equality Impact:
Equality Impact Assessment completed at the end of the policies – neutral impact
Financial Implications:
N/A
Human Resource Implications:
N/A
Procurement:
N/A
Approval history:
Approved at: - IG Group: 22 September 2017 - Operational Executive: 27 October 2017 - AquA: 7 November 2017
Recommendations:
Approval of the revised information Governance Policy and Management Framework and new Information Security policy.

NHS
Rotherham
Clinical Commissioning Group

Title:	**Information Governance Policy And Management Framework**
Reference No:	004-IT
Owner:	Deputy Chief Officer (SIRO)
Author	Author: IG Associate – eMBED Health Consortium
First Issued On:	March 2013
Latest Issue Date:	
Operational Date:	
Review Date:	October 2018
Consultation Process	IG Group to OE to AQuA
Ratified and approved by:	AQuA 7th November 2017 Governing Body 6th December 2017
Distribution:	All staff and GP members of the CCG.
Compliance:	Mandatory for all permanent and temporary employees of Rotherham CCG.
Equality & Diversity Statement:	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

Approvals

This document requires the following approvals.

Name	Signature	Title	Date of Issue	Version
Robin Carlisle		Deputy Chief Operating Officer (SIRO)	25th March 2013	6.0

Revision History

Date of this revision: 07/10/2014
Date of Next revision: 07/10/2015

Revision date	Previous revision date	Summary of Changes	Version
26/10/2010	NA	Revision of IG Policy version 3 to incorporate IG Management Framework	V4.0
27/10/2010	26/10/2010	Second appendix added to cover policy approval and review dates	V4.1
01/03/2012	27/10/2010	Revised to reflect Cluster IG responsibilities and local organisational changes	V5.0
19/03/2013	01/03/2012	Revised to reflect NHS reconfiguration.	V6.0
28/03/2013	19/03/2013	Revised following review at OE to include CSU IG obligations and new reporting arrangements for IG	V6.1
07/10/2014	28/03/2013	Changed trust to CCG, WSYCSU to YHCS, updated training to reflect IG Refresher and IAO training. Deleted duration of modules	V6.2
13/10/2015	07/10/2014	Annual review – incorporation of the framework into the body of the policy - incorporated new incident reporting rules	V7.0
22/07/2016	07/10/2014	Annual review – changes made to reflect commissioning support move from YCHS to eMBED Health Consortium, added details of the new CCG IG Group, updated references to legislation to include the new Health and Social Care (Safety and Quality) Act 2015	V7.1
02/08/2017	22/07/2016	Annual review – references to the new DPA/GDPR legislation including DPO role and new mandatory training modules added	V7.2

Contents

	Page
1. Introduction	4
2. Aims	4
3. Scope	4
4. Organisational Roles and Accountability	5
5. Resources	9
6. Governance Arrangements	10
7. Key Principles and Procedures -Openness and Transparency -Legal Compliance -Information Security -Clinical Information Assurance, Quality Assurance and Records Management	 10 11 11 12
8. Training	12
9. Incident Management	13
10. Monitoring Compliance and Effectiveness of the Policy	13
11. Associated Documents	13
12. Relevant Legislation	14
13. Implementation and Dissemination	15
14. Review	15
Appendix 1: Policy Approval Schedule	16
Appendix 2: Equality Impact Assessment	17

NHS Rotherham CCG

Information Governance Policy and Management Framework

1. Introduction

NHS Rotherham CCG recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCG also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which it processes, stores, shares and disposes of information.

This overarching Information Governance Policy and Management Framework sets out how NHS Rotherham CCG will meet its information governance obligations and outlines the underlying operational policies and procedures which will enable the CCG to fulfil its information governance responsibilities.

The policy provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information.

2. Aims

The aim of this policy is to ensure that all staff understand their obligations with regard to any information which they come into contact with in the course of their work and to provide assurance to the Governing Body that such information is dealt with legally, securely, efficiently and effectively.

The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation (GDPR) which comes into force on the 25th May 2018), and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit.

This policy supports the CCG in its role as a Commissioner of Health Services and will assist in the safe sharing of information with its partner agencies.

3. Scope

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students, partner CCGs and eMBED Health Consortium staff working on behalf of the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy and framework covers all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information

- Organisational information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transferring of information – fax, e-mail, post, telephone and removable media such as laptops and memory sticks, etc.
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

Information governance within an independent contractor's premises is the responsibility of the owner/partners. However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and the Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate regulatory bodies including the police and professional bodies.

4. Organisational Roles and Accountability

Key staff involved in the Information Governance Agenda, below those at Executive Team level, will be provided to the CCG through a contract between the CCG and eMBED Health Consortium.

4.1 Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy. It has responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, and IG Lead

4.2 Audit and Quality Assurance Committee (AQuA)

The Information Governance agenda will be led by the Deputy Chief Officer supported by staff of eMBED Health Consortium and will report through IG Group to AQuA.

The IG work programme, and new or significantly amended strategies and policies are escalated to the IG Group for their consideration and onward approval by AQuA.

4.3 Information Governance Group

The IG Group meets on a monthly and consists of the CSU IG Lead, SIRO, Caldicott Guardian, eMBED Health Consortium IG Associate, and appropriate representation. The IG Group will:

- report to the Audit and Quality Assurance Committee;
- support the CCG SIRO and CCG Caldicott Guardian in their roles;
- monitor information governance performance annually using the Information Governance Toolkit hosted by the Health and Social Care Information Centre (HSCIC);
- be responsible for overseeing operational information governance issues;
- develop and maintain policies, standards, procedures and guidance;
- co-ordinate and monitor the implementation of the information governance strategy, framework and policy across the CCG

4.3 Senior Information Risk Owner

The role of the SIRO will be carried out by the Deputy Chief Officer. The SIRO is responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO will:

- Understand how the strategic business goals of the CCG may be impacted by information risks, and how those risks may be managed.
- Implement and lead the CCG information governance risk assessment and management processes within the organisation.
- Own NHS Rotherham's Information Risk Policy
- Undertake training as necessary to ensure they remain effective in their role as SIRO.

4.4 Caldicott Guardian

The role of the Caldicott Guardian will be carried out by the Head of Quality/Lead Nurse. The Caldicott Guardian will oversee the arrangements for the use and sharing of patient information and will:

- act as the 'conscience' of the CCG
- represent and champion Information Governance requirements and issues at a senior management level
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS
- undertake training as necessary to ensure they remain effective in this role

4.5 Data Protection Officer (from 25th May 2018)

Under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. The role of Data Protection Officer is to facilitate the CCG's compliance with GDPR and will:

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Privacy Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

4.6 Information Governance Lead

The role of the IG Lead will be carried out by the Deputy Chief Officer.

The IG Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. This role includes but is not limited to:

- Providing direction in formulating, establishing and promoting IG policies
- Ensuring that the approach to information handling is communicated to all staff and made available to the public
- Ensuring that appropriate training is made available to staff and completed as necessary to support their duties
- Monitoring information handling activities to ensure compliance with the law and guidance and
- Providing a focal point for the resolution and/or discussion of IG issues

The management of the annual IG work programme will be delegated from the IG Lead to the IG Service provided by eMBED Health Consortium.

4.7 Information Asset Owners and Administrators

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems undergo a privacy impact assessment.

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

4.8 Managers

All Managers within the CCG are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

4.9 Employees

Information Governance compliance is an obligation for all staff. Staff should note that there is Non-Disclosure of Confidential Information clause in their contract and that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues.

Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported to the SIRO and (in the case of health or social care records), the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to the Data Protection Act 1998 and the Common Law Duty of Confidentiality.

4.10 Third Party Contractors

Contracts with third parties providing services to Rotherham CCG must include appropriate, detailed and explicit requirements regarding confidentiality and information governance to ensure that Contractors are aware of their IG obligations.

Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract in place to form a joint data controller relationship regarding the information required to effectively monitor commissioned services
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office
- Complete the annual Information Governance Toolkit and if requested, undertake an independent audit, to be disclosed to the CCG in order to provide further assurance they have met expected requirements.
- Ensure privacy notices make individuals aware of a CCG's role in commissioning and the personal and sensitive data it may receive to undertake such a role
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract.
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. Passing on data/deletion/ retention of data at end of the contract

Support services

All support services that process information on behalf of the CCG will be required to:

- Ensure a suitable contract/SLA and or as a minimum a confidentiality agreement is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG

- Ensure that the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office

- Complete the annual Information Governance Toolkit (if applicable) and at the request of the CCG undertakes a compliance check/ audit, in order to provide assurance they have met expected requirements.

- Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity

- Report any known incidents or risks in relation to the use or management of information owned by the CCG

- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act

- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. Passing on data / deletion/ retention of data at end of the contract

5. Resources

The key roles and responsibilities for the delivery of the Information Governance agenda in Rotherham CCG are identified in the table below:

Rotherham CCG Role	Information Governance Responsibilities
Deputy Chief Officer	• Information Governance lead • SIRO (Senior Information Risk Owner) • Chair of the Rotherham CCG Information Governance Steering Group
Head of Quality/Lead Nurse	• Caldicott Guardian • Confidentiality lead officer
Assistant Chief Officer	• FOI lead officer
Head of Health Informatics	• Information Governance Toolkit lead officer • Data Quality Lead officer Records Management lead officer •
IT Programme and Service Delivery Manager	• Assists Head of Health Informatics with IG responsibilities

IG Assurance and Security Manager (TRFT)	• Information Security lead officer
eMBED Health Consortium	• eMBED provide Information Governance support and can be contacted via the CCG IG

6. Governance Arrangements

The following governance arrangements have been agreed:

- The CCG Governing Body will receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by IG updates within the Corporate Assurance report.
- The CCG will obtain Information Governance Support through a contract with eMBED Health Consortium.
- Responsibility and accountability for Information Governance will be cascaded through the organisation via staff contracts, contracts with third parties, Information Asset Owner arrangements and departmental leads.

7. Key Principles and Procedures

7.1 Openness and Transparency

- The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and where appropriate kept confidential underpinning the principles of Caldicott, legislation and guidance.
- Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCG will establish and maintain a Publication Scheme in line with legislation and guidance from the Information Commissioner.
- There will be clear procedures and arrangements for handling queries from patients, staff, other agencies and the public concerning personal and organisational information.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Legislation, national and local guidelines will be followed.
- The CCG will undertake annual assessments and audits (through the Information Governance Toolkit) of its policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under the Data Protection Act 1998 (expected to be Data Protection Act 2017 in line with GDPR by 25th May 2018) using the CCG's Data Protection and Access to Records policy.

- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

7.2 Legal Compliance

- The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.
- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the Annual Assessment against the Information Governance Toolkit Standards and in line with changes and developments in legislation and guidance.
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principles of the Human Rights Act and in the public interest
- The CCG will establish and maintain policies to ensure compliance with the Data Protection Act (expected to be the Data Protection Act 2017 in line with GDPR by 25th May 2018), Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance.
- The CCG will work with partner NHS bodies and other agencies to establish Information Sharing Protocols to inform the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation Information Governance training will be mandatory for all staff. This will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. Information Governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be Personal Development Review (PDR) based.
- The CCG will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

7.3 Information Security

- The CCG will establish and maintain policies for the effective and secure management of its information assets and resources
- The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements as part of the Annual Assessment against the Information Governance Toolkit Standards and in line with changes and developments in legislation and guidance.
- The CCG will promote effective confidentiality and information security practice to its staff through policies, procedures and training.
- The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- The CCG will appoint a Senior Information Risk Owner and assign responsibility to Information Asset Owners to manage information risk.

- The CCG will use pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information.

- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns a Privacy Impact Assessment (PIA) must be used. Under GDPR Data Protection Impact Assessments are mandated for high risk processing.

7.4 Clinical Information Assurance, Quality Assurance and Records Management

- The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve of, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- The CCG will promote data quality through policies, procedures, user manual and training
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards
- The CCG will establish a Records Management policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

8. Training

8.1 Mandatory IG Training

The CCG includes Information Governance as part of its mandatory training for all staff annually. All new staff are required to complete the Data Security Awareness Level 1 training module via the Electronic Staff Record (ESR) or eLearning for Health website, https://nhsdigital.e-lfh.org.uk/ ,when they first join the organisation unless they have completed appropriate Data Security Training within the last year and can evidence this.

The CCG also requires all existing staff to complete online Data Security Training annually.

8.2 Role Specific Training

The CCG has identified other recommended training for staff members whose role has information governance responsibilities and requires further role specific training. This can be delivered through the eLearning for Health website when available or suitable alternatives such as workshops, face to face training and keeping up to date through briefing materials and newsletters.

8.3 Adhoc Training

In addition to the above any member of staff involved in an Information Governance related incident may be required to undertake further training via the eLearning for Health website, the modules to be taken will depend on the type of incident and the outcomes of any investigations into the incident.

In addition to the mandatory and additional training delivered formally, the IG Toolkit also requires organisations providing health and social care services to have a documented action plan to promote staff awareness of information governance standards, inform staff of their responsibilities and the consequences of misconduct and advise staff their compliance with IG requirements will be checked and monitored.

Staff may be informed through formal raining, team meetings, awareness sessions or staff briefing materials. In all cases, 'staff' refers to all staff (new and existing), including new starters, locum, temporary, student and contract staff members.

9. Incident Management

Information Governance and IT related incidents, including cyber security incidents must be reported and managed through the CCG Incident Policy. Under GDPR, where a data breach is likely to result in a risk to the rights and freedoms of the individual, incidents must be reported to the Information Commissioners Office within 72 hours. An information governance incident of sufficient scale or severity to be classified as a Level 2 Serious Incident Requiring Investigation (SIRI) or cyber SIRI will be:

- Notified immediately to the CCG's SIRO and Caldicott Guardian
- Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the HSCIC Incident reporting tool
- Investigated and reviewed in accordance with the guidance in the HSCIC checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

10. Monitoring Compliance and Effectiveness of the Policy

An assessment of compliance with the requirements in the Information Governance Toolkit (IGT) will be undertaken each year. Annual assessments and proposed action/development plans will be presented to the CCG's Operational Executive. The requirements are grouped into the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

11. Associated Documents

Rotherham CCG will maintain the following key policies to support effective Information Governance:

- Information Governance Policy and Management Framework
- Data Protection /Access to Health Records Policy
- Network Security Policy
- Records Management Policy
- Freedom of Information Policy.

Supplementary to the key policies listed above, Rotherham CCG will also maintain the following policies and guidelines:

- Confidentiality Code of Conduct
- Email Policy
- Information Risk Policy
- Internet Acceptable Use Policy
- Portable Data Security Policy
- Safe Haven Policy
- Smartphone and Tablet Policy.

Details of all the above polices, including where the policy was last approved and the date of last approval are detailed in appendix 1.

Each policy will be subject to an implementation plan:

- All policies will be maintained on the Rotherham CCG Intranet.
- Policies will be incorporated into induction and training sessions as appropriate.

12. Relevant Legislation

There are many different standards and legislation that apply to IG and information handling, including, but not limited to:

- Data Protection Act 1998 (expected to be superseded by the Data Protection Act 2017 in line with GDPR by 25th May 2018)
- Health and Social Care Act 2012
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Confidentiality NHS Code of Practice
- Human Rights Act 1998
- International Information Security standard: ISO/IEC 27002: 2005
  Access to Health Records Act 1990
- Information Security NHS Code of Practice
- Caldicott Guidance
- Computer Misuse Act 1990
- Mental Capacity Act 2005
- Public Records Act 1958
- Records Management Codes of Conduct for Health and Social Care 2016
- Care Act 2014
- Health and Social Care (Safety and Quality) Act 2015.

13. Implementation and Dissemination

All the Information Governance policies and procedures will be made available in electronic format and will be located on the CCG Intranet. Any updates/new policies/procedures are approved by the Audit and Quality Assurance Committee (AQuA) following consideration at the IG Group and are communicated to staff via the intranet and staff briefings.

Every new member of staff will be directed to the policy pages on the intranet as part of the induction process.

14. Review

This policy will be reviewed every year or in line with changes to relevant legislation or national guidance. The policy will be reviewed in August 2018.

Appendix 1: Policy Approval Schedule
(This schedule is maintained by Andrew Clayton of RCCG)

Policy Name	Owner	Responsible Organisation	Last Approved By	Last Issued Date	Review Date
Information Governance Policy and Management Framework	Andrew Clayton	RCCG	RCCG GB	Feb 2017	October 2018
Freedom of Information Policy	Ruth Nutbrown	RCCG	RCCG GB	April 2017	January 2019
Records Management Policy	Andrew Clayton	RCCG	RCCG GB	Feb 2017	October 2018
Safe Haven Policy	Andrew Clayton	RCCG	RCCG GB	Feb 2017	October 2018
Email Policy	Derek Stowe	TRFT	RCCG GB	March 2015	December 2016
Portable Data Security Policy	Derek Stowe	TRFT	RCCG GB	March 2015	January 2017
Data Protection and Records Access Policy	Andrew Clayton	RCCG	RCCG GB	Feb 2017	April 2018
Information Risk Policy	Andrew Clayton	RCCG	RCCG GB	Feb 2017	October 2018
Internet Acceptable Use Policy	Andrew Clayton	RCCG	RCCG GB	Feb 2017	October 2018
Smartphone and Tablet Policy	Derek Stowe	TRFT	RCCG GB	March 2015	January 2017

NHS
Rotherham
Clinical Commissioning Group

APPENDIX 2

Equality Impact Assessment

Title of policy or service:	Information Governance Policy and Management Framework	
Name and role of officer/s completing the assessment:	Andrew Clayton – Head of Health Informatics	
Date of assessment:	25.09.17	
Type of EIA completed:	**Initial EIA 'Screening'** ☐ ***or*** **'Full' EIA process** ☐	*(select one option - see page 4 for guidance)*

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	It is a mandatory requirement for compliance with the Information Governance Toolkit for the CCG to have an Information Governance Policy and Management Framework. This Framework supports the current and evolving Information Governance agenda across the organisation and describes the framework for managing Information Governance that extends to cover all those working on behalf of the organisation. This document should be reviewed on an annual basis and signed off at a Senior Management level at the CCG.

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is either justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.					
(Please complete each area)	**What key impact have you identified?**			**For impact identified (either positive and or negative) give details below:**	
	Positive Impact	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐	N/A	
Age	☐	☒	☐	N/A	
Carers	☐	☒	☐	N/A	
Disability	☐	☒	☐	N/A	
Sex	☐	☒	☐	N/A	
Race	☐	☒	☐	N/A	
Religion or belief	☐	☒	☐	N/A	
Sexual orientation	☐	☒	☐	N/A	
Gender reassignment	☐	☒	☐	N/A	
Pregnancy and maternity	☐	☒	☐	N/A	
Marriage and civil partnership (only eliminating discrimination)	☐	☒	☐	N/A	
Other relevant groups	☐	☒	☐	N/A	
HR Policies only: Part or Fixed	☐	☐	☐	N/A	

term staff					

IMPORTANT NOTE: *If any of the above results in '**negative**' impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	**Andrew Clayton**	**Date of next Review:**	**August 2018**

Once completed, this form **must** be emailed to Alison Hague, Corporate Services Manager for sign

off: Alison.hague@rotherhamccg.nhs.uk

Alison Hague signature:	

EQUALITY IMPACT ASSESSMENT: Initial EIA 'Screening' and 'Full' EIA Processes

EIA FLOWCHART

STEP 1

SCREENING EIA

Lead Manager/Person to identify the policy or process (revised or new), strategy, business case or decision for EIA screening

If you require assistance, please contact Elaine Barnes, Equality & Diversity Manager: elaine.barnes3@nhs.net

Carry out an Initial Screening EIA to determine if a Full EIA (STEP 2) is required

Screening identifies whether the policy or process (revised or new), strategy, business case or decision is relevant to equality.

It outlines the purpose/aim of the policy, gives information or evidence relating to equality groups that may be affected and reviews type of impact (positive, neutral or negative) on equality and other relevant groups.

OUTCOME

POSITIVE OR NEUTRAL IMPACT: impact can be rectified by small actions being taken to the policy, strategy, business case or decision. Therefore **no Full EIA required.**

Forward completed EIA template to Elaine Barnes for sign off.

End of Process

Ensure any identified actions are completed and reported

NEGATIVE / ADVERSE IMPACT: where this is identified and impact cannot be rectified without significant changes to the policy, strategy, business case or decision, then a **Full EIA required needs to be considered (STEP 2).**

STEP 2

FULL EIA

If you require assistance, please contact Elaine Barnes, Equality& Diversity Manager: elaine.barnes3@nhs.net

Carry out Full EIA to explore the negative/adverse impact identified. Complete EIA form (same as screening form) showing actions to justify/minimise impact and promote equality.

(a) Assess likely impact in detail by collating information/evidence such as reports, quantitative and qualitative baselines, national or local data, consultations and engagement processes, focus groups, surveys, groups, discussions with relevant community or working groups, etc.
(b) Consider actions to mitigate discrimination, minimise negative/adverse impact and promote equality.
(c) Forward completed EIA template to Elaine Barnes for monitoring and quality assurance.

End of Process

Ensure any identified actions are completed and reported