NHS Rotherham Clinical Commissioning Group

Information Governance Group – 05 March 2021

OE – 16 April 2021

Audit Quality and Assurance Committee (AQuA) – 04 May 2021

Governing Body – 02 June 2021

Information Governance Policy and Management Framework

Lead Executive:	Andy Clayton
Lead Officer:	Claire McInnes
Lead GP:	N/A

Purpose:
IG Policy and Management Framework (IGMF) due for review in December 2020.
Background:
Routine review of the IGMF
Analysis of key issues and of risks
Updated to reflect the in-house IG provision, including DPO following the end of the eMBED contract Updated references to UKGDPR following the EU Exit. Section 8 – Training – this section has been expanded to reflect the requirements of the DSPT and now includes Specialist/Advanced Training New Appendix 2 – Detailed training needs analysis for various roles within the CCG – DSPT requirement for the CCG to undertake regular training needs analysis
Patient, Public and Stakeholder Involvement:
N/A
Equality Impact:
N/A
Financial Implications:
N/A
Human Resource Implications:
N/A
Procurement Advice:
N/A
Data Protection Impact Assessment:
DPIA not required
Approval history:
Reviewed at the IG Group 05 March 2021 and approved by AQuA 04 May 2021 for ratification at Governing Body
Recommendations:
Governing Body are asked to ratify the changes to the IG Policy and Management Framework
Paper is for Ratification

NHS
Rotherham
Clinical Commissioning Group

Title:	**Information Governance Policy And Management Framework**
Reference No:	004-IT
Owner:	Deputy Chief Officer (SIRO)
Author	Author: Senior IG Specialist – eMBED Health Consortium
First Issued On:	March 2013
Latest Issue Date:	January 2021
Operational Date:	April 2021
Review Date:	April 2023
Consultation Process	IG Group to OE to AQuA
Ratified and approved by:	AQuA 04 May 2021 Governing Body TBC
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.

Revision History

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
03/10/2018	02/08/2017	Review changed to 2 yearly Updated references to new DSP Toolkit and new DPA/GDPR legislation	V7.3
20/01/2021	03/10/2018	Updated to reflect the in-house provision of the IG service and the UK GDPR following the EU Exit. Training section expanded and the addition of a Training Needs Analysis document as an appendix	V8.0

Contents

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 legislation, and other related legislation and guidance, contractual responsibilities and to support the ten Data Security standards of the Data Security and Protection 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 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 – 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

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, Head of IG and Data Protection Officer

4.2 Audit and Quality Assurance Committee (AQuA)

The Information Governance agenda will be led by the Deputy Chief Officer supported by the Head of IG 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 Head of IG, SIRO, Caldicott Guardian, IG Officer, Head of Digital, Head of IT, Head of BI, Assistant Chief Officer 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 Data Security and Protection toolkit hosted by NHS Digital;
- 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

4.4 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.

4.5 Caldicott Guardian

The role of the Caldicott Guardian will be carried out by the Chief 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

4.6 Data Protection Officer

Under the General Data Protection Regulation (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 held by the Head of IG 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

4.7 Head of Information Governance

The Head of IG 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

4.8 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.

4.9 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.

4.10 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 2018, the UK General Data Protection Regulation and the Common Law Duty of Confidentiality.

4.11 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 controller relationship regarding the information required to effectively monitor commissioned services

- Ensure the services commissioned meet the requirements of the Data Protection Act 2018 and UKGDPR when providing services including, but not limited to, fair processing and maintaining a Data Protection notification with the Information Commissioners Office

- Complete the annual Data Security and Protection 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 Controller to 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 2018 and UKGDPR when providing services including, but not limited to, fair processing and maintaining a Data Protection notification with the Information Commissioners Office

- Complete the annual Data Security and Protection 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
Chief Nurse	• Caldicott Guardian • Confidentiality lead officer
Assistant Chief Officer	• FOI lead officer
Head of IG	• Data Protection Officer • Data Security and Protection Toolkit Lead Officer • Data Quality Lead officer • Records Management lead officer
Head of IT	• Assists Head of IG with IG responsibilities
IG Assurance and Security Manager (TRFT)	• Information Security lead officer
Data Protection Officer	• Position held by the Head of 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.

- 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 Data Security and Protection Toolkit) of its policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under Data Protection legislation 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 Data Security and Protection 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 legislation, 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 Data Security and Protection 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 Data Protection Impact Assessment (DPIA) must be used. Under UKGDPR 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) when they first join the organisation. In the event of unresolvable difficulties with ESR and for all specialised Information Governance E-learning, this can be accessed via the eLearning for Health website https://portal.e-lfh.org.uk/

The mandatory Data Security Awareness training is split into four learning modules with an additional "Welcome module". Each learning module concludes with an assessment. The modules can be taken in any order and the system will record the assessment pass mark and issue a certificate on successful completion (a score of 80% or more).

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

Written training materials and class room training can be provided to staff locally once they have completed the Data Security Awareness e-learning module online (and will meet the mandated training requirement) as long as it is equivalent to the learning materials they provide.

8.2 Specialist/Advanced Training

The Data Security and Protection Toolkit (DSPT) requires that staff with specialist roles receive data security and protection training suitable to their role and that Leaders and Board members receive suitable training. Caldicott Guardian and SIRO training will therefore also be made available to the relevant CCG staff.

The SIRO and Caldicott Guardian will be able to complete the training either online, once available on the eLearning for Health website, or by attending a face to face, SIRO/Caldicott Guardian specific, training session.

8.3 Role Specific Training

The CCG has identified in Appendix 2 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, accredited course providers and keeping up to date through briefing materials and newsletters.

8.4 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.

9. Incident Management

Information Governance and IT related incidents, including cyber security incidents must be reported and managed through the CCG Incident Policy. Under UKGDPR, 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 (ICO) within 72 hours. An information governance incident of sufficient scale or severity to be reportable to the ICO 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 Incident reporting tool on the Data Security and Protection toolkit
- Investigated and reviewed in accordance with the guidance within the Data Security and Protection toolkit
- 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 Data Security and Protection toolkit will be undertaken each year. Annual assessments and proposed action/development plans will be presented to the CCG's Operational Executive.

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
- Information Security Policy
- Records Management Policy

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

- Confidentiality Policy
- Email, Digital Collaboration and Videoconferencing Policy & Procedures
- Information Risk (incorporated in the CCG's Integrated Risk Management Framework)
- Internet Acceptable Use Policy
- Portable Data Security and Smartphone & Tablet Policy
- Safe Haven Policy
- Data Protection by Design Procedure
- Data Protection Impact Assessment Procedure
- Information Asset and Dataflow Review Procedure

Details of 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 2018
- UK General Data Protection Regulation (UKGDPR)
- 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 two years or in line with changes to relevant legislation or national guidance. The policy will be reviewed in April 2023.

Appendix 1: Policy Approval Schedule
(This schedule is maintained by the Head of IG)

Policy Name	Last Approved By	Review Date
Information Governance Policy and Management Framework	RCCG GB	May 2023
Records Management Policy	RCCG GB	March 2022
Safe Haven Policy	RCCG GB	June 2022
Email, Digital Collaboration and Videoconferencing Policy & Procedures	RCCG GB	April 2023
Portable Data Security and Smartphone and Tablet Policy	RCCG GB	December 2021
Data Protection and Records Access Policy	RCCG GB	March 2022
Internet Acceptable Use Policy	RCCG GB	March 2022
Information Security Policy	RCCG GB	December 2021
Confidentiality Policy	RCCG GB	August 2022

Appendix 2 – IG Training Needs Analysis

Staff Group	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
New starters	Data Security Standard 3 in the Caldicott Review requires that all staff undertake appropriate annual data security training and pass a mandatory test. To achieve compliance with the requirements of the Data Security and Protection Toolkit	IG Policies and procedures and completion of Induction checklist Data Security Awareness Level 1 – via ESR or e-learning for health	Policies available on the CCG Intranet E-learning - 55 minutes (knowledge chapters) 15 minutes (eAssessment)	Once within 2 months of starting in role
All staff	Data Security Standard 3 in the Caldicott Review requires that all staff undertake appropriate annual data security training and pass a mandatory test. To achieve compliance with the requirements of the Data Security and Protection Toolkit	Data Security Awareness Level 1 – via ESR or e-learning for health	E-learning - 55 minutes (knowledge chapters) 15 minutes (eAssessment)	Annually
Staff who manage Access and other Rights Requests	Subject Access and Individual Rights Requests training To achieve compliance with the requirements of Data Protection legislation	Online or face to face training sessions	Classroom or individual sessions	3 yearly or as required
Staff who commission services and Project Managers	Data Protection Impact Assessment Training – understanding when DPIAs are required and successful completion. To achieve compliance with the requirements of the Data Security and Protection Toolkit	Online or face to face training sessions	Classroom or individual sessions	3 yearly or as required

Information Asset Owners (IAOs)	Describes key responsibilities for IAO roles, and outlines the structures required within organisations to support those staff with IAO duties. To achieve compliance with the requirements of the Data Security and Protection Toolkit	Online or face to face training sessions Information Asset Owner Handbook	Classroom or individual sessions Hard copy	3 yearly or as required Once only (unless updated)
SIRO	To assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties. To achieve compliance with the requirements of the Data Security and Protection Toolkit	Online or face to face sessions provided by external accredited training providers	E-learning or classroom/individual sessions	3 yearly
Caldicott Guardian	To assist staff whose role involves responsibility for the confidentiality of patient information To achieve compliance with the requirements of the Data Security and Protection Toolkit	Online or face to face sessions provided by external accredited training providers E-learning provided by the Office of the National Data Guardian when available	E-learning or classroom/individual sessions	3 yearly
Head of Information Governance/DPO	In depth understanding of the Data Protection Act, UK General Data Protection Regulation (and associated legislation) and information security. To achieve compliance with the requirements of the Data Security and Protection Toolkit	British Computer Society (BCS) Data Protection and Information Security courses	Specialist accredited providers	Once only

APPENDIX 3

Equality Impact and Engagement Assessment Form					
Complete this section **Please retain one copy, and pass one copy to both the Equalities and Engagement leads**					
Section one – Project or plan details					
1.1	**Project Title: Information Governance Policy and Management Framework**				
1.2	**Project Lead: Andrew Clayton**		**Contact Details:**		
1.3	**This activity /project is:**				
	Policy				
1.4	**Describe the activity/project**				
	Historically it has been a mandatory requirement for compliance with the Information Governance Toolkit for the CCG to have an Information Governance Policy and Management Framework with the expectation that this be reviewed on an annual basis; it has therefore been reviewed prior to its review date. The new Data Security and Protection Toolkit (DSPT) does not include the same requirement of an annually reviewed IG Policy and Management Framework the review date has therefore been changed to two yearly in line with the CCG's other policies.				
1.5	**Timescales**				
	2 yearly review				
2	**Equality Impact Assessment**				
2.1	**Gathering of Information:** This is the core of the analysis; how might the project or work impact on protected groups, with consideration of the General Equality Duty. Please add any general information here.				
2.2	**Screening**				
	Please complete each area)	**What key impact have you identified?**			**Information Source**
		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.**	What action, if any, is needed to address these issues and what difference will this make? For example: *At this point no action is required. Further EIA screenings will be developed in future once there are recommendations to assess.*
	Human Rights	**Y/N**	**Y**	**Y/N**	
	Age	**Y/N**	**Y**	**Y/N**	
	Carers	**Y/N**	**Y**	**Y/N**	
	Disability	**Y/N**	**Y**	**Y/N**	
	Sex	**Y/N**	**Y**	**Y/N**	
	Race	**Y/N**	**Y**	**Y/N**	
	Religion or belief	**Y/N**	**Y**	**Y/N**	
	Sexual Orientation	**Y/N**	**Y**	**Y/N**	
	Gender reassignment	**Y/N**	**Y**	**Y/N**	
	Pregnancy and maternity	**Y/N**	**Y**	**Y/N**	

	Marriage/civil partnership (only eliminating discrimination)	**Y/N**	**Y**	**Y/N**	
	Other relevant groups	**Y/N**	Y	**Y/N**	
	NEXT ACTIONS? See 3.4 below				

3 Engagement Assessment	
3.1	**What is the level of service change**? – see diagram 3 above Ongoing Development – Category 1 **If your project is classed as a 'significant variation' (level 3) or 'major change' (level 4)** please contact england.yhclinicalstrategy@nhs.net for a preliminary discussion to support planning and agree whether the service change needs to follow the NHS England Service Change Assurance process. The assurance process generally looks at the 'case for change' The key players in the process include overview and scrutiny teams, and the clinical senates. You can also refer to the DH guidance: (please note that level 4 changes will require considerable long term planning and this DH guidance is mandatory for all level 4 changes) http://www.healthwatch.co.uk/sites/healthwatch.co.uk/files/nhs_public_involvement_-hempsons_stp.pdf DH 2013
	Circle or highlight the appropriate level of service change Level 1 Level 2 Level 3 Level 4
	Add additional information and rationale for this scoring below
	Regular policy review
3.2	**Who are your stakeholders?** Consider using a mapping tool to identify stakeholders - who is the change going to affect and how? Complete below or attach or link to a mapping document
	N/A
3.3	**What do we already know?** What do you already know about peoples' access, experience, health inequalities and health outcomes? Use intelligence from existing local, regional or national research, data, deliberative events or engagements.
	N/A
	Describe any existing arrangements to involve patients and the public which are relevant to this plan/activity and/or provide relevant sources of patient and public insight? How will the insight available to you help to inform your decision?
	N/A
	Briefly describe how the existing or proposed engagement will be 'fair and proportionate', in relation to the activity?
	N/A

3.4	**Reaching out to overlooked communities** Are additional arrangements for patient and public involvement required for this activity and in particular will you ensure that 'seldom-heard' groups, those with 'protected characteristics' under the Equality Act, those experiencing health inequalities are involved • Seldom-heard groups No • Nine Protected Characteristics No • Health inequalities No If yes, please provide a brief outline of your approach and objectives for any additional patient participation targeted at these groups
	Do you need to make any of your resources accessible (i.e. for people with learning disabilities, sight impairments, or alternative languages?)
	N/A
3.5	**What resources do you need for this?** Consider the sections above • The timescales • The need to reach overlooked communities • Accessible materials • Gaps in knowledge
	N/A
4	**Feedback and Evaluation**
4.1	How will you use the feedback – who does it need to be shared with?
	N/A
4.2	Provide a brief outline of how the information collected through patient and public participation will be used to influence the plan/activity.
	N/A
4.3	How will the outcomes of participation be reported back to those involved?
	N/A
4.4	How will you assess the ongoing impact of the change on patients and the public after it has been completed?
	N/A

5	**Engagement and Equality Impact Plan**				
	Action	**Approx. Timescale**	**Lead**	**Deadline**	**Comments/ progress**

6	rm details	
	Completed by:	Claire McInnes
	Job title:	Head of IG
	Date	08.03.2021
	Reported to	Alison Hague