NHS
Wakefield
Clinical Commissioning Group

Information Governance Policy and Framework

Version: 8.0

Committee Approved by: Integrated Governance Committee

Date Approved: 16th January 2020

Author: Information Governance Manager

Responsible Directorate: Corporate Affairs

Date issued: 16th January 2020

Review date: July 2020

Review and Amendment Log / Control Sheet

Responsible Officer:	Director of Corporate Affairs /SIRO
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager
Date Approved:	16th January 2020
Committee:	Integrated Governance Committee
Version:	8.0
Review Date:	July 2020

Version History

Version no.	Date	Author	Description	Circulation
1.0	December 2014	IG Associate / Governance & Board Secretary	Approved	Policy approved by Integrated Governance Committee 18 December 2014
2.0	December 2015	IG Associate / Governance & Board Secretary	Presented to IGC for approval	Approved by IGC December 2015
3.0	December 2016	Information Governance Manager	Approved	Approved policy added to Skyline
4.0	September 2017	Information Governance Manager	Approved	Approved policy added to Skyline
4.1	January 2018	Information Governance Manager	Approved	Amendment to policy to reflect a revised next review date, as agreed by the IGC in December 2017
4.2	January 2018	Information Governance Manager	Amendments to reflect the requirements of the General Data Protection Regulation and additional amendments to	Governance and Board Secretary and Associate Director for Corporate Affairs

			enable the policy and framework to remain factually accurate.	
4.3	January 2018	Information Governance Manager	Review by Governance and Board Secretary and Associate Director for Corporate Affairs	
5.0	February 2018	Information Governance Manager	Approved	Approved by IGC February 2018
5.1	April 2018	Governance and Board Secretary	Minor amendment to name of SIRO and name of DPO, as agreed at Executive Committee April 2018	Added to Skyline
5.2	November 2018	Information Governance Manager	Minor amendments to training section and SIRO responsibilities.	IGC
6.0	January 2019	Information Governance Manager	Approved	Approved policy added to Skyline and website
6.1	June 2019	Senior IG Officer	Draft – rolling review as per schedule	Governance and Board Secretary
7.0	July 2019	Senior IG Officer	Approved by IGC 18 July 2019	Added to Skyline
7.1	December 2019	Information Governance Manager	Draft – minor updates to reflect personnel and role changes.	IGC
8.0	January 2020	Information Governance Manager	Approved by IGC 16 January 2020	Added to Skyline

Contents

Section		Page
	Strategic Objectives	5
1	Introduction	6
2	Aims and Objectives	6
3	Scope	6
4	Accountability	7
5	Definition of Terms	9
6	Key Principles and Procedures	9
7	Training	13
8	Implementation and Dissemination	14
9	Monitoring Compliance and Effectiveness of the Policy and Framework	14
10	Associated documents	14
11	References	15
12	Equality Impact Assessment	16
Appendix A	Information Governance Management Framework	17
Appendix B	Information Governance Declaration Form	29
Appendix C	Caldicott Function Specification	31
Appendix D	Equality Impact Assessment	32

STRATEGIC OBJECTIVES

The CCG aims to:

- achieve a standard of excellence in information governance by ensuring information is dealt with legally, securely, efficiently and effectively in the course of its business, in accordance with the requirements of the Information Governance Policy and Framework and associated policies set out in Section 10 of this document

- meet a satisfactory rating against the NHS Digital Data Security and Protection Toolkit

- minimise the risks to the CCG in handling confidential information particularly in the area of cyber security and records management

- provide support to staff to be consistent in the way they handle personal information and to avoid duplication of effort

- improve assurance through the use of spot checks and confidentiality audits

These strategic objectives will be delivered through the approach set out within the Information Governance Management Framework and annual information governance work plan.

1. INTRODUCTION

1.1 NHS Wakefield Clinical Commissioning Group (CCG), hereafter referred to as the 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. Information Governance plays an integral role in commissioning quality services, supporting clinical governance, service planning and performance management that will improve local patients' experiences of care and their health outcomes.

1.2 Information Governance addresses the demands that law, ethics and policy place upon information processing – holding, obtaining, recording, using and sharing of information. It is crucial to ensure that all staff are aware of these demands and the implications for patient care.

1.3 The Information Governance Policy and Framework sets out the CCG's overall approach to the management of Information Governance and should be read in conjunction with the other Information Governance policies and procedures.

2. AIMS AND OBJECTIVES

2.1 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.

2.2 The CCG will establish, implement and maintain policies and procedures linked to this policy and framework to ensure compliance with the requirements of Data Protection legislation, Freedom of Information Act 2000, Common Law Duty of Confidentiality, Caldicott Principles, Records Management Code of Practice for Health and Social Care, Code of Practice on Confidential Information, Information Security industry best practice as well as other related legislation, guidance and its contractual responsibilities.

2.3 This policy supports the CCG in its role as a Commissioner of Health Services and will assist in the appropriate, secure and lawful sharing of information with its health and care partners and agencies.

3 SCOPE

3.1 This policy applies to NHS Wakefield CCG and all its employees and must be followed by all those who work for the organisation, including Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students and as well, any external organisations acting on behalf of the CCG including other CCGs in line with contract of employment or contract of service clauses.

3.2 The Information Governance Policy and Framework is applicable to all areas of the organisation and adherence to it should be included in all contracts for outsourced or shared services. There are no exclusions.

3.3 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 and business sensitive 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;
- Information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobiles, smartphones and cameras.

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

- Transmission of information – verbal, fax, e-mail, post, text and telephone;
- Sharing of information for clinical, operational or legal reasons;
- The storage and retention of information;
- The destruction of information.

3.4 Information Governance within member practices premises is the responsibility of the owner/partners. However, the CCG is committed to supporting independent member practices in their management of information risk and will provide advice and assistance and share best practice when appropriate.

3.5 The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and will continue to work with national bodies and partners to ensure the ongoing and appropriate, secure and lawful use and sharing of information to support health and care services.

3.6 Failure to adhere to this Policy may result in disciplinary action and/or referral to the appropriate professional regulatory body, health and care regulator as well as the police.

4. 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.

4.2 Integrated Governance Committee

The Integrated Governance Committee is responsible for the review and approval of this policy, related work plans and procedures and will receive regular updates on information governance compliance and any related issues or risks.

4.3 Accountable Officer

The Chief Officer is the Accountable Officer of the CCG and has overall accountability and responsibility for Information Governance within the CCG. The Chief Officer is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to information governance, are effectively managed and mitigated.

4.4 Senior Information Risk Owner

The Director of Corporate Affairsis the Senior Information Risk Owner (SIRO) and has organisational responsibility for Information Governance and data security risk, including the responsibility for ensuring the CCG has appropriate systems and policies in place to effectively manage information risk.

4.5 Caldicott Guardian

The Caldicott Guardian for the CCG is the Governing Body GP Lead for Quality. The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the CCG on the lawful and ethical processing of patient information. The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information.

4.6 Data Protection Officer

The Data Protection Officer for the CCG is the Governance and Board Secretary. The Data Protection Officer is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance. The role carries the broader responsibility of senior level lead for information governance for the CCG, overseeing the work of the Information Governance Team and ensuring effective management, compliance and assurance for all aspects of information governance. The role is also responsible for reviewing this policy and associated work plans and ensuring these are updated in line with any changes to legislation, national or local policy and guidance.

4.7 Information Asset Owners and Administrators

Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is identified and managed effectively in respect of the information assets that they are responsible for and that any new business processes and systems or changes to business processes and systems undergo a privacy impact assessment when appropriate.

Information Asset Administrators (IAAs) have delegated responsibility for the operational day to day management of Information Assets.

4.8 Heads of Service

Heads of Service are responsible for ensuring that they and their staff have met their statutory and mandatory training requirements in respect of information governance and are proactive in implementing this policy and its

associated guidance. They must ensure that any non-compliance with this policy is reported, investigated and acted upon.

4.9 System Administrators

Systems administrators have greater access rights in comparison to a normal system user. System Administrators hold a position of additional responsibility and trust, especially of systems holding personal and confidential information. System Administrators must sign an agreement which holds them accountable to the highest standards of use.

4.10 Information Governance Service

The Information Governance Service provides day-to-day information governance operational support to the SIRO, Data Protection Officer and Caldicott Guardian.

4.11 All Staff

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

Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer system is a disciplinary offence, which may result in disciplinary action, termination of contract of employment and criminal proceedings against the individual. All breaches will be reported to the SIRO and Data Protection Officer and (in the case of patient identifiable information) the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to Data Protection and Confidentiality.

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

6. KEY PRINCIPLES AND PROCEDURES

6.1 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 Caldicott Principles, legislation and guidance;
- Information about the organisation will be available to the public in line with the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Protection of Freedoms Act 2012 unless an exemption (or exception in the case of the Environmental Information Regulations) applies. The CCG will establish and maintain a Publication

Scheme in line with legislation and Guidance from the Information Commissioner's Office;

- Service users will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from service users 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;
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience;
- Legislation, national and local guidelines will be followed;
- The CCG will undertake annual assessments and audits (of its policies, procedures and arrangements for openness as part of Data Security and Protection Toolkit work programme);
- Patients will have ready access to information relating to their own health care under Data Protection legislation using the CCG's Access to Records Procedure;
- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

6.2 Legal Compliance

- The CCG regards all personal identifiable information relating to service users as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained. See the Confidentiality and Data Protection Policy;
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The CCG will establish and maintain policies to ensure compliance with Data Protection legislation, Human Rights Act 1998, Freedom of Information Act 2000 and Environmental Information Regulations 2004 and the Common Law Duty of Confidentiality and associated guidance.
- Data Security awareness training will be mandatory for all staff. This will include awareness and understanding of the Caldicott Principles and confidentiality, information security (including cyber security) and data protection. Data Security awareness will be included in induction training for all new staff and as part of the annual mandatory training programme. The necessity and frequency of any further bespoke training will be Personal Development Review (PDR) based;
- The CCG will undertake annual assessments and audits of its compliance with legal requirements as part of the annual assessment against the Data Security and Protection Toolkit and in line with changes and developments in legislation and guidance;
- The CCG will work with partner NHS health and care bodies and other agencies to put in place appropriate information sharing agreements to support the appropriate, secure and lawful sharing of personal identifiable information with other agencies, taking account of relevant legislation (e.g. Data Protection legislation, Health and Social Care (Safety and Quality) Act

2015, Crime and Disorder Act 1998, Children Act 2004 Code of Practice and Caldicott Principles);

- 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 ensuring that a statutory basis for disclosure of personal identifiable information exists.

6.3 Information Security

- The CCG will establish and maintain policies for the effective and secure management of its information assets and resources such as Network Security Policy and Information Security Policy;
- The CCG will undertake annual assessments and audits of its information security including cyber security arrangements as part of the annual assessment against the Data Security and Protection Toolkit and in line with changes and developments in legislation and guidance;
- The SIRO will take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control. The SIRO will assign responsibility to Information Asset Owners to manage information risk. An annual SIRO report will be issued to the Integrated Governance Committee as part of the Information Governance Report;
- Audits will be undertaken or commissioned to assess information and IT security arrangements;
- The CCG will promote effective confidentiality and information security (including cyber security) practice to its staff through policies, procedures and training;
- Information Governance and IT security related incidents, including cyber security incidents (including but not limited to, physical destruction or damage to the organisation's computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported and managed through the CCGs Incident Reporting Policy. An information governance incident of sufficient scale or severity which meets the threshold for reporting to the ICO as set out in the 'Breach Assessment Grid' within the NHS Digital Guide to the Notification of Data Security and Protection Incidents (July 2018) 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 NHS Digital Incident Reporting Tool;
    - Investigated and reviewed in accordance with the guidance in the NHS Digital incident guidance;
    - Reported publicly through the CCG's Annual Report.
- The CCG will aim to protect the organisations information assets from all known threats, whether internal or external, deliberate or accidental;
- The CCG will gain assurance from IT service providers as to the integrity of the CCG's IT systems and that controls are in place to reduce exposure to potential cyber-crime and through maintenance of robust information governance and network security practices;

- The CCG will implement pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information;
- The CCG will conform to developing guidance from NHS Digital and NHS England.

6.4 Clinical Information Assurance, Quality Assurance and Records Management

- The CCG will establish and maintain policies for information quality assurance and the effective management of records;
- Audits will be undertaken or commissioned of CCG's quality of data and records management arrangements;
- Managers will be expected to take ownership of, and seek to improve, the quality of data within their services;
- Wherever possible, information quality will be assured at the point of collection.
- The CCG will promote data quality through policies, procedures, the Information Governance Handbook and training;
- 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 meet the requirements of the law and address privacy concerns and information risk a Data Protection Impact Assessment (DPIA) must be undertaken when appropriate;
- The CCG will continue to implement its Records Management and Lifecycle Policy which covers all aspects of records management and is consistent with the Records Management Code of Practice for Health and Social Care.

6.5 Third Party Contracts and Clinical Services

- The CCG will ensure that contracts with third parties providing services to and on behalf of the CCG include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that Contractors are aware of their information governance obligations.
- In accordance with the NHS Standard Contract, 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 Data Protection legislation when providing services including, but not limited to, fair processing. Additionally, where relevant, to pay a data protection fee to the Information Commissioner (under the requirements of the Digital Economy Act 2017);

    - Complete the 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 that where any Serious 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.

7. TRAINING

7.1 Mandatory Training

Data Security awareness training including a test of competency will be mandated for all staff as part of induction and mandatory training. This will include awareness and understanding of National Data Security Standards, Caldicott Principles, confidentiality, information security and data protection. The CCG will identify the information governance training needs of key staff groups taking into account role, responsibility and accountability levels and will review this regularly through the PDR process.

All staff will receive Information Governance training in line with the CCG's mandatory training matrices. All new starters (new staff, temporary staff, agency staff and contractors) will undertake Data Security Awareness Level 1 training within one month of their start date unless they have completed appropriate Data Security training within the last year and can evidence this. In addition all new starters and temporary staff will be issued with an IG User Handbook (Appendix B).

7.2 Information Governance Training Principles

- Annual Data Security awareness training will be mandatory for all staff (including temporary staff, agency staff and contractors);
- Data Security awareness training will be undertaken using the Electronic Staff Records (ESR), the online e-Learning for Healthcare website, via completion of a training workbook or through attendance at a formal IG classroom based session;
- The CCG will identify the information governance training needs of key staff groups taking into account role, responsibility and accountability levels. This will be based on staff responsibilities and required training needs outcomes, other staff groups may be resourced to undertake additional training as required;
- Quarterly monitoring and reporting of uptake and completion of Data Security awareness training will be provided to the Integrated Governance Committee.

8. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Integrated Governance Committee this policy will be disseminated to staff via the CCG's intranet and communication through in-house staff briefings.

This Policy will be reviewed annually or in line with changes to relevant legislation or national guidance.

9. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

To be assured that this policy is being implemented, key elements will be monitored for compliance.

- **Compliance with all mandatory assertions within the Data Security and Protection Toolkit.** The Integrated Governance Committee will monitor overall progress through receipt of quarterly reports and take action to address any concerns and deficiencies will be noted and reviewed at subsequent meetings;
- **All staff receive annual training and competency test in Data Security awareness**. The Integrated Governance Committee will monitor progress via the workforce update report;
- **All Information Asset Owners (IAOs) trained in their role and undertaking annual risk reviews of information assets they are responsible for**. New information assets will be identified through this review process. Integrated Governance Committee will monitor progress through receipt of the annual SIRO report;
- **No Data Protection enforcement activity undertaken utilising the 'investigatory powers' or 'corrective powers' of the Information Commissioner.** Corrective powers include: reprimands, bans on processing, suspension of data transfers, ordering the correction of an infringement and administrative fines.
- **No Freedom of Information Act enforcement notices served on the organisation.** The Integrated Governance Committee will monitor progress via the quarterly Information Governance Report;
- **Staff know who and where to direct information governance concerns and queries to.** Results of annual information governance staff survey.

10 ASSOCIATED DOCUMENTATION (Policies, protocols and procedures)

The CCG will produce appropriate procedures and guidance relating to information governance as required by related policies.

This policy should be read in conjunction with:

- Confidentiality and Data Protection Policy
- Records Management and Information Lifecycle Policy
- Freedom of Information and EIR Policy
- Information Security Policy (incorporating Network Security)
- E-Communications and Social Media Policy and Procedure

- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy and Procedure
- Anti-Fraud Policy
- Anti-Bribery Policy

And their associated procedures (including but not limited to)

- Access to Records Procedure
- Interagency Information Sharing Protocol
- Data Protection Impact Assessment Procedure
- Safe Haven Guidelines and Procedure

This policy should be read in conjunction with the Information Governance Handbook which has been shared with all staff (See Appendix B). The handbook will be updated annually.

11 REFERENCES

- Official Journal of the European Union L 119/1 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and repealing Directive 95/46/EC (General Data Protection Regulation) Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- Great Britain. 2000. *Freedom of Information Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Department of Health and Social Care, 2000. Publications: Data Security and Protection Toolkit. Available at: https://nww.igt.hscic.gov.uk/
- NHS Digital, 2014, Publications Code of Practice on Confidential Information Available at: https://digital.nhs.uk/
- Department of Health and Social Care, 2016, Publications: Records Management Code of Practice for Health and Social Care. Available at: https://www.gov.uk/

12 EQUALITY IMPACT ASSESSMENT

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. A single Equality Impact Assessment is used for all policies and procedures.

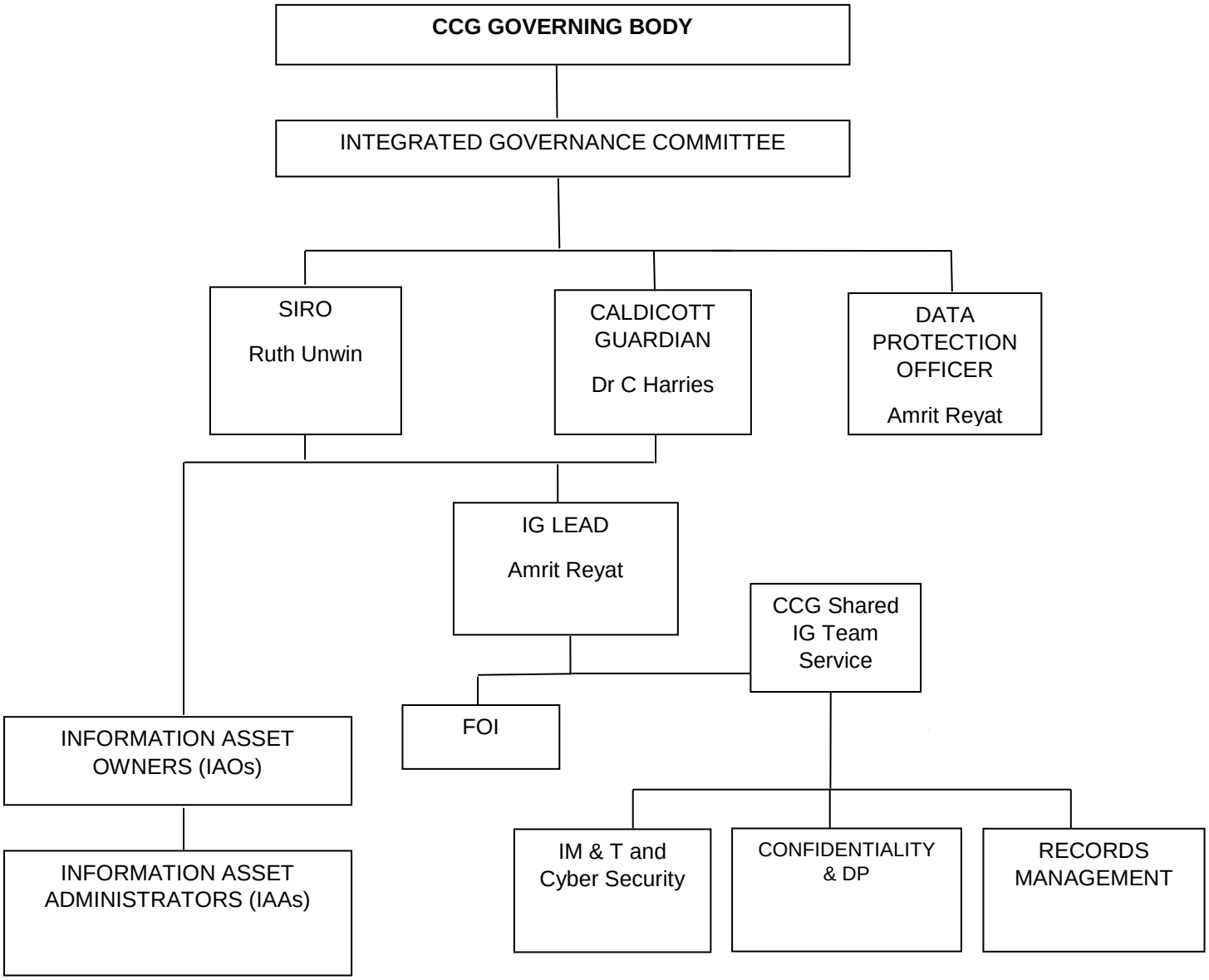
This document has been assessed to ensure consideration has been given to the actual or potential impacts on staff, certain communities or population groups.

See **Appendix D** – Equality Impact Assessment

Appendix A

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

1. Organisational Chart



The lines of responsibility and accountability are described in the narrative within Section 4 (Accountability) of this policy and within Section 2 (Outline of Roles and Responsibilities) of this Appendix.

2. Outline of Roles and Responsibilities

2.1 The Caldicott Guardian will:

- Ensure that the CCG satisfies the highest practical standards for handling identifiable/confidential information.

- Act as the ‘conscience’ of the CCG.
- Facilitate and enable information sharing and supported by expert advice from the Information Governance Team, advice on options for lawful and ethical processing of information.
- Represent and champion Information Governance requirements and issues at executive level.
- 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.

The Caldicott Guardian has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation’s overall governance framework.

2.2 Caldicott Function

Support to the Caldicott Function will be undertaken by the DPO with additional support from Information Governance Team.

The key responsibilities of the Caldicott Function are to:

- Support the Caldicott Guardian Function (Appendix C)
- Ensure the Information Governance work programme is successfully co-ordinated and implemented.
- Ensure compliance with the principles contained within the Confidentiality Code of Practice for Health and Social Care and that staff are made aware of individual responsibilities through policy, procedure and training.
- Provide support on the lawful and appropriate disclosure of personal information.
- Complete the Data Security and Protection Toolkit, contributing to the annual assessment.
- Provide routine reports to senior management on Confidentiality and Data Protection issues, as required.
- Review information sharing agreements for approval.

2.3 The Senior Information Risk Owner (SIRO) will:

- Be an Executive Director.
- Take overall ownership of the organisation’s approach to managing information risk.
- Act as champion for information risk within the CCG executive function and provide advice to the Chief Officer on the content of the CCG’s Statement of Internal Control in regard to information risk.
- Act as person with overall responsibility for data security, in line with the Data Security and Protection Toolkit.
- Understand how the strategic business goals of the CCG and how other client

organisations' business goals may be impacted by information risks, and how those risks may be managed.
- Implement and lead the Information Governance risk assessment and management processes within the organisation.
- Advise the Governing Body on the effectiveness of information risk management across the organisation.
- Receive annual training to ensure they remain effective in their role as SIRO.

2.4 The Data Protection Officer will:

- Monitor CCG compliance with the Data Protection legislation
- Provide advice and assistance with regards to the completion of Data Protection 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
- Provide routine documented reports to the Integrated Governance Committee and Governing Body on the organisation's state of compliance.
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, Data Protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

As part of their broader responsibilities around information governance the senior level lead for information governance will:

- Ensure that there is top level awareness and support for information governance resourcing and implementation of improvements
- Act as the organisational lead for Data Protection including subject access request, Freedom of Information, Information Security and Records Management.
- Work with the Information Governance Team to:
    - Maintain an oversight of information governance issues within the CCG.
    - Maintain comprehensive and appropriate documentation that demonstrates commitment to and ownership of information governance responsibilities.
    - Provide direction in formulating, establishing and promoting IG policies
    - Ensure appropriate IG training is made available to staff, completed as necessary and monitored and that IG training requirements are included in overall mandatory and statutory training matrices.

- Ensure that evidence is collated and uploaded to the Data Security and Protection Toolkit website and that the assessment is submitted by the 31st March annually.
- Ensure that IAOs, managers and team leaders are aware of the requirements of this policy.
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis.

2.5 Information Asset Owners (IAO) will:

- Know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset.
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy.
- Understand and address risks to the asset, and provide assurance to the SIRO.
- Ensure that privacy impact assessments are undertaken in relation to new business processes and systems that may impact on the privacy of individuals and in relation to changes introduced to processes and systems.
- Assist in the development of business continuity management arrangements for key information assets.

3. Resources

3.1 Information Governance Support

The Information Governance team provides expert advice and guidance to staff on all elements of Information Governance. The team provide the following support to NHS Wakefield CCG:

- advice and guidance on information governance
- advice and template resources relating to the Data Security and Protection Toolkit requirements
- ensure the consistency of information governance across the organisation.
- developing information governance policies and procedures.
- establishing protocols on how information is to be shared.
- developing information governance awareness and training programmes
- supporting organisational compliance with Data Protection, Freedom of Information and other information security related legislation.
- implementing Information Governance Alliance, NHS England, NHS Digital and Department of Health information governance policy and guidance.
- provide support to the Data Protection Officer, Caldicott Guardian, SIRO, IG Lead and IAOs.

The Information Governance Team hold professional certification in Data Protection and Freedom of Information. The team will support the CCG in fulfilling the following specific roles:

Information Security Lead - The Information Security Lead is tasked with providing advice on all aspects of information security management, utilising their own expertise and, where necessary, external advice.

The ICT Service Provider will have a nominated Information Security Officer / Manager with appropriate duties and resources to act as a source of expertise for advice on information and cyber security.

Corporate and Clinical Records Management Lead - The Records Management Lead is tasked with providing advice on all aspects of records management, information quality and lifecycle of information, utilising their own expertise and, where necessary, external advice.

4. Governance Framework

4.1 Staff Contracts

All CCG staff contracts contain Information Governance related clauses within them.

4.2 Non-NHS Third Party Contract Confidentiality Clause

Any non-NHS third party with whom the organisation contracts should include as a minimum a confidentiality clause within the contract of service. All third party contractors who have access to CCG information assets or process personal information on behalf of the CCG must provide assurance that they, where relevant, pay a data protection fee to the Information Commissioner (under the requirements of the Digital Economy Act 2017) in relation to the processing of personal data and that they encrypt all portable computing devices to minimum standard required by the NHS.

4.3 Information Assets and Asset Owners

Each information asset has been allocated an Information Asset Owner (IAO). The Information Asset Owner will review their information asset entries on the Information Asset Register at least annually and undertake regular risk assessments of these information assets and report findings to the SIRO.

4.4 Information Governance Management Reporting and Policy Reviews

The toolkit requires a number of standard items to be reported on a regular basis to the appropriate group with responsibility for specific Information Governance activities.

IG Activity	Includes but not limited to	Reported to	Completion by
Completion of Data Security and Protection Toolkit Assessment	Regular updates on progress. Final Toolkit assessment outcome	Integrated Governance Committee	Quarterly
	Review and sign off of final assessment for submission	IG Lead and SIRO	31 March 2020
	IG Update on progress, target scores and final scores	Integrated Governance Committee	Quarterly
IG Work Plan sign off	Operational actions identified following gap analysis against the new Data Security and Protection Toolkit	Integrated Governance Committee	July 2019
Monitoring of Data Security Training Compliance	Included in the workforce update report	Integrated Governance Committee	Quarterly
IG Update and IG Work Plan progress reports	Included in Information Governance Report	Integrated Governance Committee	Quarterly
IG and cyber security incidents	Included in Information Governance Report and in the Incident Report	Integrated Governance Committee	Quarterly
Confidentiality and Data Protection Assurance Updates	Included in Information Governance Report - Caldicott issues, confidentiality audits, data flow mapping, information sharing agreements	Integrated Governance Committee	Quarterly
Information Risk Assurance Updates	Included in Information Governance Report - summary of information asset reviews, risk assessments, access reviews and information system security controls.	Integrated Governance Committee	Six monthly

SIRO's Annual IG Report	Details of compliance, Data Security and Protection Toolkit Score, information risk management work and details of IG incidents	Integrated Governance Committee	April 2020
Requests for Information	Included in Information Governance Report - Numbers of FOI and Subject Access Requests. Compliance against timescales.	Integrated Governance Committee	Quarterly
Policy Reviews	Details of changes to policy or best practices	Integrated Governance Committee	Rolling schedule

4.5 Demonstrating compliance and accountability under Data Protection legislation

The CCG will ensure it is able to demonstrate compliance of Data Protection legislation through the implementation of policies, procedures and undertaking the following activities:

- Implementation of appropriate data security measures
- Establish data protection policies and procedures
- Undertake Staff training
- Record processing activities
- Appoint Data Protection Officer
- Complete data flow mapping listing all flows of personal data
- Recording their lawful justification and retention periods
- Incorporating data protection measures by default (Privacy by Design)
- Conducting regular data protection impact assessments

5. IG Training

5.1 Mandatory Information Governance Training

The NHS Operating Framework requires that all staff must undergo annual information governance training. The CCG will strive to meet this requirement. 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 on the ESR or e-Learning for Healthcare website when they first join the organisation unless they have completed appropriate Data Security training within the last year and can evidence this.

5.2 Role Specific Training

Role specific training will be identified through PDR processes. The CCG has identified additional training that those with specific responsibilities relating to Information Governance and information risk management will be required to undertake. Those staff members will be informed of the additional training that they are required to complete. Learning will be undertaken via the online e-Learning for Healthcare website or through suitable alternatives such as specific themed workshops, workbooks, face to face training and support materials.

5.3 Ad hoc Training

In addition to the above requirements any member of staff involved in an information governance related incident may be required to undertake additional training. The training to be undertaken will depend on the type of incident and the outcomes of any investigations into the incident.

5.4 IT Service Provider

The CCGs IT service provider is responsible for the provision of annual mandatory training, role specific and advanced data security training for its staff.

5.5 Training Needs Analysis

Training needs are monitored by line managers through the annual appraisal process. The training matrix below identifies mandatory and recommended IG training modules.

Staff Group	Level	Training Objective/Aim	Module /Course Name	Method of Delivery	Frequency of Training
New starters	Basic Level	To ensure new starters to the CCG are informed of their responsibilities to maintain good Information Governance.	Data Security Awareness Level 1	E-learning	Within 1 month of starting date
Governing Body	Basic Level	Governing Body members whose roles do not require them to access person identifiable data (PID), but do have access to business and safeguarding confidential and sensitive information.	Data Security Awareness Level 1	E-learning or classroom based session*	Annually

Staff Group	Level	Training Objective/Aim	Module /Course Name	Method of Delivery	Frequency of Training
		All Governing Body members that have previously completed the introductory module.			
All Staff	Basic Level	A foundation level module aimed at all staff to inform them about good Information Governance.	Data Security Awareness Level 1	E-learning or classroom based session*	Annually
Records Management staff	Basic Level	A foundation level module designed to provide practical information to enable understanding of the importance of good records management.	Access to Health Records or specialist training workshops (externally/internally sourced)	E-learning, workbook or classroom based session	3 yearly
Information Governance - Records Management leads – corporate and clinical	Essential Level	Accountability for leading on Records Management and acting as a source of knowledge/ advice to successfully co-ordinate and implement the information quality and records management agenda.	Practitioner level Access to Health Records or specialist training workshops (externally/internally sourced)	E-learning, workbook or classroom based session	3 yearly
Staff handling Subject Access Requests	Essential Level	Practitioner level to support staff dealing with Subject Access Requests or Access to Health Record responsibilities	Practitioner level Access to Health Records or specialist training workshops (externally / internally sourced)	E-learning, workbook or Classroom / individual session *	3 yearly
Information Asset Owners (IAOs)	Essential Level	An introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties.	NHS Information Risk Management for SIROs and IAOs	E-Learning for Healthcare website, IAO Handbook Classroom, workbook or individual session*	3 yearly

Staff Group	Level	Training Objective/Aim	Module /Course Name	Method of Delivery	Frequency of Training
SIRO	Expert Level	Accountability for organisational information risk. A foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.	NHS Information Risk Management for SIROs	E-Learning for Healthcare website, classroom, workbook or individual session*	3 yearly
Caldicott Guardian	Expert Level	A practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian	The Caldicott Guardian in the NHS and Social Care Patient Confidentiality	E-Learning for Healthcare website, classroom, workbook or individual session*	3 yearly
Information Governance Support	Expert Level	In depth understanding of Data Protection legislation and information security	Information Security Examination Board (ISEB) Data Protection and Information Security courses.	Specialist courses providers	Once only
Data Protection Officer (DPO)	Expert Level	A good level of understanding of data protection legislation	Online guidance material and/or specialist courses	e-learning, workbook or specialist training provider	3 yearly

5.6 The effectiveness of the training will be demonstrated in a number of ways:

Measure	Detail
Reactive Evaluation	Training feedback forms assessing the trainers performance as well as whether training objectives were met, are provided at all class room based learning events.
Evaluating Learning	Increase in knowledge after the training is measured by post training assessment test (either online assessment test or paper based assessment test). 80% is the pass mark for the assessments. Successful achievement of the assessment test is recorded against the learners training record.

Behaviour	The extent to which Information Governance training has been put into practice will be subjectively measured by: 1. The results of IG compliance spot checks. 2. Staff IG awareness survey (typically administered via questionnaire). 3. Numbers of Information Governance related incidents and risks reported.

6. Information Security Incidents

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the system or information being put at risk. Incidents may include cyber-attacks, theft, misuse or loss of equipment containing confidential information or other incidents that could lead to unauthorised access to data all of which will have an adverse impact to patients and to the organisation e.g.

- embarrassment to the patient/patients/organisation
- threat to personal safety or privacy
- legal obligation or penalty
- loss of confidence in the organisation
- financial loss
- disruption of activities

Whenever an incident, near miss or hazard occurs it must be reported using the incident reporting system. Information security incidents will be highlighted to the CCG IG Lead and Information Governance Team for investigation and advice. 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.

All ICT security and cyber incidents should be reported to the Health Informatics Service Desk upon detection to obtain support with preserving data, preventing an incident being prolonged, and enabling an audit trail and technical investigations to commence without delay. These will be highlighted to the IG Lead and Information Governance Team. The Service Desk will advise of any additional steps that are required to make the information secure, including initiating policy and procedure.

The CCG has an overarching Integrated Risk Management Framework which includes a section about taking into account the NHS Digital's 'Guide to the Notification of Data Security and Protection Incidents'. The Information Governance Team will use the criteria within the checklist document to work out the seriousness of a reported incident.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, the incident is reportable via the DSPT online incident reporting tool where full details will be automatically emailed to the ICO and the NHS Digital Data Security Centre. A summary of these incidents will be included in the Statement of Internal Control.

7. Communication

7.1 Communication with Staff

Information governance operational policies and procedures will be made available in electronic format and will be located on the intranet. Any updates/ new policies / procedures are approved by the Integrated Governance Committee and are communicated to staff via the intranet. Information Governance email alerts will be issued by the Information Governance Team as appropriate and authorised by the IG Lead.

Every new member of staff will be issued with the Information Governance User Handbook about handling personal and confidential patient information as part of the recruitment process. The Information Governance Team will continue to raise the profile and understanding of Information Governance through mandatory and ad hoc training, information governance alerts, staff newsletters, emails, intranet sites and staff briefings.

Appendix B

Information Governance Declaration Form

Please read carefully the Information Governance User Handbook, it is your responsibility to read and understand it and to raise any queries or concerns with your line manager or directly with the Information Governance Team.

This Handbook has been developed to signpost Users to Information Governance Policies and sets out the CCG's expectations of you in relation to handling information including the requirements of relevant law, national guidance and codes of practice around Data Protection, Confidentiality, Caldicott, Information Security, Record Keeping and Records Management, Information Quality, Freedom of Information and Access to Environmental Information.

Specifically they set out requirements around the:

- Appropriate collection, use, storage, transfer and disposal of personal and organisational information
- Appropriate use of CCG information, networks, systems and equipment (or those that are accessed by virtue of your employment/association with the CCG)
- Appropriate use of email
- Appropriate use of the internet
- How to report incidents relating to information security

It is IMPORTANT to remember that you are accountable for your computer login and that all activity is auditable. Confidentiality audits and compliance spot checks are undertaken regularly. Monitoring of email and internet activity is also carried out. It is your responsibility to ensure that only you know your password and that if you leave your PC logged in and unattended you must lock your PC (Press Ctrl+ Alt + Del) to stop any unauthorised use of your PC.

You should be aware that inappropriate behaviour including non-compliance with CCG policy and procedure may result in the withdrawal of IT facilities and, in accordance with CCG disciplinary procedures, could lead to disciplinary, civil or criminal proceedings being taken against you including the termination of your employment / association with the CCG.

Please complete, sign and date the following declaration:

I confirm that I have read and understood the Information Governance User Handbook and know where to access Information Governance policies and procedures. I understand that I can raise any queries or concerns with my line manager / sponsor and the Information Governance Team for further information about anything which I did not understand. I understand that it is my responsibility to raise queries or concerns with them.

I understand my obligation: to fully comply with Information Governance policies; to maintain the confidentiality and security of information and equipment to which I have access; and to return any equipment (such as USB sticks, laptops, tablets, mobile phones, ID cards, smart cards etc.) with which I have been issued, when I leave / change roles.

Please sign and return this form to your line manager, when signed this declaration will be held on your personal file.

Signed:	Date:
Name (Please Print):	
Job Title:	
Team:	
Contact Telephone Number:	

Appendix C

Caldicott Function Specification

The Caldicott function has been established to support the Caldicott Guardian. The Caldicott Guardian is required to be part of the Governing Body and have a clinical background. The CCG will also appoint a deputy Caldicott Guardian, also with clinical expertise, who will act on behalf of the main post holder in their absence.

The Caldicott Guardians will perform the functions as laid down in the Caldicott Guardian Manual, available on the gov.uk website, and will be responsible for protecting patient and service user confidentiality and enabling information sharing. The Caldicott Guardian will also have a strategic role in representing and championing Information Governance requirements and issues at Governing Body level.

The role of the Caldicott Guardian will be specified and promoted throughout the IG Management Framework documentation and will be made readily accessible to staff via the CCG's staff intranet. This role will be primarily supported by the Confidentiality Code of Practice for Health and Social Care.

The Caldicott Guardian will be supported by the CCG's Information Governance Lead and the Information Governance team on issues concerning data protection and will provide advice on the disclosure of personal information e.g. to the Police and other agencies, as appropriate.

Where Contractors of the CCG who are processing personal confidential data on behalf of the CCG feel that meeting information governance standards may cause operational difficulties or they feel that meeting standards would compromise patient care or safety, they can apply to the Caldicott Guardian for a decision on whether an acceptable risk status can be agreed.

Caldicott Issues Log Any incidents relating to patient confidentiality will be recorded and monitored through the existing CCG incident management system. A Caldicott Issues Log will be created to log any issues and risks escalated to the Caldicott function and include details of any approved information sharing agreements. The IG Lead will support the Caldicott Guardian to ensure that the CCGs benefit from lessons learned by sharing with the Integrated Governance Committee. The agreed acceptable risks will also be recorded in the Caldicott Log. Specific actions and improvements to address any gaps in compliance relating to data protection and confidentiality will be managed through the CCG's Information Governance Work Programme.

Appendix D

Equality Impact Assessment

Title of policy	Information Governance Policy and Framework	
Names and roles of people completing the assessment	Amrit Reyat – Governance and Board Secretary	
Date assessment started/completed	Started: 25/06/19	Completed 18/07/2019

1. Outline	
Give a brief summary of the policy	The Information Governance Policy and Framework sets out the CCG's overall approach to the management of Information Governance.
What outcomes do you want to achieve	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.

2.Analysis of impact			
This is the core of the assessment, using the information above detail the actual or likely impact on protected groups, with consideration of the general duty to; eliminate unlawful discrimination; advance equality of opportunity; foster good relations			
	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	**Are these negative or positive?**	**What action will be taken to address any negative impacts or enhance positive ones?**
Age	None identified	n/a	n/a
Carers	None identified	n/a	n/a
Disability	None identified	n/a	n/a

Sex	None identified	n/a	n/a
Race	None identified	n/a	n/a
Religion or belief	None identified	n/a	n/a
Sexual orientation	None identified	n/a	n/a
Gender reassignment	None identified	n/a	n/a
Pregnancy and maternity	None identified	n/a	n/a
Marriage and civil partnership	None identified	n/a	n/a
Other relevant group	None identified	n/a	n/a

If any negative/positive impacts were identified are they valid, legal and/or justifiable? Please detail.	None identified.

4. Monitoring, Review and Publication			
How will you review/monitor the impact and effectiveness of your actions	None identified - not applicable		
Lead Officer	**n/a**	**Review date:**	**n/a**

5.Sign off			
Lead Officer	Amrit Reyat, Governance & Board Secretary		
Director		**Date approved:**	18/07/2019