NHS
Calderdale
Clinical Commissioning Group

Information Governance Policies Book

Review and Amendment Log / Control Sheet

Responsible Officer:	Corporate Systems Manager/IG Lead
Governing Body / Clinical Lead:	Chief Finance Officer/Deputy Chief Officer
Author:	Information Governance Team
Date Approved:	1. 14 October 2021 2. 9 December 2020
Committee:	1. Audit Committee 2. Finance and Performance Committee
Version:	3.0
Review Date:	24 February 2023

Version History

This policies book has been developed from a suite of IG policies adopted by NHS Calderdale CCG. For previous versions and their version history, please contact the Corporate Systems Manager**.**

Version no.	Date	Author	Status	Commentary	Circulation
0.1	20/08/20	IG Team	Draft	Initial compilation of IG Policies book and review of policy content.	Virtual consultation with SMT
0.2	24/08/20	IG Team	Draft	Amendments following comments from SMT members.	Audit Committee.
0.2	24/09/20	IG Team	Draft	Audit Committee Approved the policy	Quality, Finance and Performance

Version no.	Date	Author	Status	Commentary	Circulation
				book with the exception of the Records Management Sections which requires separate approval from Q, F and P committee.	Committee for virtual approval of Records Management Section
1.0	09/12/20	IG Team	Final	Records Management Section approved by Quality, Finance and Performance Committee. Full book now approved.	All staff
1.1	11/01/21	IG Team	Draft	DSPT 20/21 related enhancements to Chapter 4 Information Security Policy and Chapter 7 Glossary of Terms.	Virtual consultation with SMT
2.0	25/02/21	IG Team	Final	Enhancements to Chapters 4 and Chapter 6 approved by Audit Committee.	All staff
2.1	28/09/21	IG Team	Draft	Update of the password complexity rules in Section 4.3	Audit Committee

Version no.	Date	Author	Status	Commentary	Circulation
3.0	14/10/2021	IG Team	Final	Enhancement to password complexity rules in section 4.3 Approved by Audit Committee.	Audit Committee

Contents

Chapter 1: Introduction, Scope and Accountability 8

1.1 Overall Introduction 9

1.2 Overall Scope 9

1.3 Accountability 11

1.4 Definition of Terms 16

Chapter 2 - Information Governance Policy and Framework 17

2.1 Strategic Objectives 18

2.2 Key Principles 18

2.3 Information Security 21

2.4 Clinical Information Assurance, Quality Assurance and Records Management 22

2.5 Third Party Contracts and Clinical Services 23

2.6 Information Governance Management Framework – Organisational Chart 25

2.7 Outline of Key Roles and Responsibilities 25

2.8 Resources 29

2.9 Governance Framework 30

2.10 IG Training 34

2.11 Information Security Incidents 41

2.12 Communication with Staff 42

Chapter 3: Confidentiality and Data Protection Policy 43

3.1 Introduction 44

3.2 Aims and Objectives 44

3.3 Scope 45

3.4 Confidentiality Codes of Practice, Guidance and Legislation 46

3.5 Principles and Procedures 52

3.6 Individuals Rights 54

3.7 Consent and Information Sharing 59
3.8 Data Protection by Design and Default 63
3.9 Confidentiality and Data Protection by Design Audit Procedures 64
3.10 Working with Confidential Information 64
3.11 Transferring Information 67
3.12 Anonymisation and Managing Data Protection Risk 69
3.13 Personal Data Breaches 69
3.14 Data Protection Fee 71
3.15 Using NHS Numbers 71
Chapter 4: Information Security Policy (incorporating Network Security) RESTRICTED ..72
Chapter 5: Records Management and Information Lifecycle Policy 73
5.1 Introduction 74
5.2 Scope 74
5.3 Aim 75
5.4 Legal and Professional Obligations 76
5.5 Records Management Procedures 77
5.6 Tracking of Records 79
5.7 Manual Record Storage 79
5.8 Digital and other media records 80
5.9 Records in Transit 81
5.10 Taking Records Off Site 82
5.11 Incident Reporting 83
5.12 Retention of Records, Archiving and Disposal 83
5.13 Scanning 86
5.14 Data and Information Quality 86
5.15 Using NHS Numbers 87

5.16 Using Electronic Signatures 88
5.17 Emails as Records..... 89
5.18 Digital, Audio, Visual, Photographic, Text and other Electronic Records..... 90
5.19 Access to Records..... 90
5.20 Decommissioning of Buildings/ Vacating Premises..... 90
5.21 Records Management Systems Audit 90
5.22 Information Asset Registers 91
5.23 Clear Desk Policy 92
Chapter 6: Training, Implementation and Monitoring.....93
6.1 Training and Guidance 94
6.2 Implementation and Dissemination..... 95
6.3 Monitoring Compliance and Effectiveness of the Policy 95
6.4 Legal References and Guidance 96
6.5 Associated Documentation (Policies, protocols and procedures) 97
6.6 Glossary of Terms 99
6.7 Equality Impact Assessment..... 104
Chapter 7: Appendices.....105
Appendix A: Caldicott Function Specification..... 106
Appendix B: Information Governance Declaration Form 2020- 23..... 108
Appendix C: Equality Impact Assessment..... 111

Chapter 1: Introduction, Scope and Accountability

1.1 Overall Introduction

NHS Calderdale Clinical Commissioning Group, 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.

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.

The aim of this policy book is to ensure that all staff understand their obligations with regard to information governance such that information is dealt with legally, securely, efficiently and effectively.

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

The policies within this book support the CCG in its role as Commissioner of Health Services and will assist in the appropriate, secure and lawful sharing of information with health and care partners and agencies.

1.2 Overall Scope

The policies within this book cover all information held by the organisation, including (but not limited to):

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

- Organisational information
- All aspects of handling information, including (but not limited to):
- Structured record systems - paper and electronic
- Transmission of information – paper and electronic
- All information systems purchased, developed and managed by/or on behalf of, the organisation
- Photographic images, digital, text or video records
- 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):

- 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.

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

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 appropriate, secure and lawful use and sharing of information to support the health and care service.

The policies within this book must be followed by all staff who work for or on behalf of the CCG, including those on temporary or honorary contracts, secondments, volunteers, Governing Body members, pool staff, contractors and students, as well as any external

organisations acting on behalf of the CCG including other CCGs in line with contract of employment or contract of/for service clauses.

If there is evidence that any user is not adhering to this policy, this will be investigated under the Disciplinary Policy and Procedure. Breach of this policy could amount to misconduct or gross misconduct depending on the circumstances.

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

1.3 Accountability

The purpose of this section is to set out the responsibilities of key committees and roles in relation to the effective implementation of the policies set out within this book. This section also sets out the responsibilities placed on all staff.

Governing Body

The Governing Body of the CCG is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy book, for the appointment of an approved SIRO and to receive by exception, significant risks and gaps in compliance on issues relating to information governance.

Audit Committee

The Audit Committee is responsible for the review and approval of this policy book, related work plans and procedures and will receive regular updates on compliance and any related issues and risks. The Audit Committee's Terms of Reference define the Committee's roles and responsibilities which are delegated to them by the Governing Body.

Accountable Officer

The Chief Officer (Robin Tuddenham) 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 security, confidentiality and data

protection, records management and electronic communication and social media are effectively managed and mitigated.

Senior Information Risk Owner

The Chief Finance Officer and Deputy Chief Officer (Neil Smurthwaite) is the CCG's Senior Information Risk Owner (SIRO) and has organisational responsibility for all aspects of Information Governance and data security risks, including the responsibility for ensuring the CCG has appropriate systems and policies in place to effectively manage information risk.

The SIRO is responsible for drawing to the attention of the Governing Body any identified risks to compliance with this policy book; ensuring that, where appropriate, staff receive Data Security (and cyber security) awareness training; setting the overall information security policy for the organisation, in collaboration with THIS; monitoring and seeking assurance that the technical, organisational and procedural information security controls set out in this policy book are being met.

Caldicott Guardian

The Caldicott Guardian for the CCG is Steven Cleasby, Chair, NHS Calderdale CCG.

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information. They are responsible for ensuring patient identifiable information is shared and disclosed in an appropriate and secure manner. They also have a strategic and operational 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. The Caldicott Guardian role is advisory.

A detailed description of the Caldicott Function is given in Section 2.7.

Data Protection Officer

The Data Protection Officer (DPO) for the CCG is the Chief Finance Officer and Deputy Chief Officer. The DPO is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance.

The DPO will be the first point of contact for the Information Commissioner's Office (ICO) on all data protection matters and for individuals whose data is processed by the CCG (employees, service users and the general public).

The DPO will advise the CCG on the reporting of Serious Incidents Requiring Investigation, and will liaise with the ICO in relation to incidents reported to the ICO.

Information Governance Lead

The senior level information governance lead for the CCG is the Corporate Systems Manager (Rob Gibson). The IG Lead is responsible for ensuring effective management, compliance and assurance of all aspects of information governance. They are 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.

The IG Lead, with the support of the Information Governance Team, is responsible for investigating and reviewing incidents in respect of possible breaches of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 and agreeing recommended actions.

Senior Management Team

The Senior Management Team will received information governance progress reports, contribute to policies reviews and help manage the resolution of information governance operational issues.

Information Asset Owners

Information Asset Owners (IAO) 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.

IAOs will ensure that documented user registration and de-registration procedures for access are in place in relation to key information assets identified within the information asset register. Additionally, they will ensure that operational, managerial and technical

security access controls have been defined, documented and approved for key information assets identified in the information asset register.

Information Asset Administrators (IAAs) have delegated responsibility for the operational use of the CCG's information assets.

System Administrators

System 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.

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 Data Security Awareness and are proactive in implementing this policies book and its associated procedures.

The responsibility for local records management (including retention and disposal of records) is devolved to the Heads of Service. Heads of Service within the CCG have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Records Management and Information Lifecycle Policy (Chapter 5).

Heads of Service / Line managers are additionally responsible for ensuring that personal use of the internet and email systems by their staff is proportionate, not excessive and does not interfere with their duties.

Requests for internet usage logs must be authorised by an appropriate Head of Service, and such requests should be by exception rather than the norm. The advice of a Human Resources representative must be sought and any requests made for internet usage logs must be with the prior agreement of Human Resources.

Heads of Service are responsible for ensuring that they and their staff are familiar with this policy book and its associated procedures. They must ensure that any breaches of policy are reported, investigated and acted upon.

Line Managers

Line Managers are responsible for ensuring that information governance policy and procedures are implemented in their area of responsibility; championing information governance principles and promoting a culture of personal responsibility for compliance with policy; seeking advice from IAOs and the Information Governance Team on information security matters; ensuring the security of the physical environment where information is processed and stored; ensuring that they and their staff undertake annual mandatory Data Security Awareness training.

Head of Information Management and Technology (IM and T)

The Head of I M and T is responsible for ensuring the technical, procedural and organisational responsibilities of THIS, as set out in the Information Security Policy (incorporating Network Security) at Chapter 4, are met. This will be achieved through management of the contractual agreement (including associated Service Level Agreements) between the CCG and THIS. The CCG shares the Head of IM and T and wider IT expertise as part of the Shared Service for IT, which is hosted by NHS Calderdale CCG.

Information Governance Team

The CCG receives Information Governance support including advice on data protection and confidentiality from the Information Governance Team. The Information Governance Team provides day-to-day information governance operational support to the SIRO, DPO and Caldicott Guardian.

All Staff

Information Governance compliance is an obligation for all staff. Staff should note that there is a Non-Disclosure of Confidential 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 of information governance requirements.

Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems 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, DPO and (in the case of patient identifiable information) the Caldicott Guardian.

All staff are personally responsible for compliance with the law in relation to data protection and confidentiality.

The Health Informatics Service (as determined through agreement with the CCG)

The Health Informatics Service (THIS) is responsible for:

- Implementing an effective framework for the management of network security in line with the CCG's requirements;
- Assisting in the formulation of Information Security Policy (incorporating Network Security) and related policies and procedures;
- Advising on the content and implementation of the relevant action plans;
- Co-ordinating network security activities particularly those related to shared information systems or IT infrastructures;
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk;
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with business needs, policy and guidance;
- Ensuring that access to the organisations' network is limited to those who have the necessary authority and clearance;
- Advising on the accreditation of IT systems, applications and networks.

1.4 Definition of Terms

The words used in this policy are used in their ordinary sense and technical terms have been avoided. Please refer to the glossary of terms within Chapter 6 of this book of policies.

Chapter 2 - Information Governance Policy and Framework

2.1 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 6.5 of Chapter 6 of this book
- 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 using spot checks and Confidentiality and Data Protection by Design Audits.

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

2.2 Key Principles

Openness

- 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 organisations will be available to the public through the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Protection of Freedoms Act 2012 unless an exemption 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, staff, other agencies and the public.

- 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 the Data Security and Protection Toolkit work programme.
- Service Users 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.

Legal Compliance

- The CCG regards all identifiable personal information relating to service users as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained. See Chapter 3 for 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 and procedures 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, 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.

- Information risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable information governance controls are in place.

- 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, Confidentiality Codes of Practice and Caldicott Principles, Health Service (Control of Patient Information) Regulations 2002).

- 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.

2.3 Information Security

- The CCG will establish and maintain operational policies for the effective and secure management of its information assets and resources, such as the Information Security Policy (incorporating Network Security).

- The CCG will undertake annual assessments and audits of 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.

- 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 their staff through policies, procedures and training.

- The CCG will ensure that the security of the information it holds complies with legislation, national guidelines and codes of practice.

- 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 CCG's Incident Management and 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 and Governance Statement.

- 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 (for example through independent audit or evidence of completed external assessments/industry standard certifications) 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 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 locally implement guidance published by the Information Governance Alliance, NHS Digital, NHS England, NHS X and the Information Commissioner's Office.

2.4 Clinical Information Assurance, Quality Assurance and Records Management

- The CCG will establish and maintain operational policies for information quality assurance and the effective management of records.

- Audits will be undertaken or commissioned of the CCG's data quality 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 awareness training.

- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisations to meet the requirements of the law and address privacy concerns and information risk a Data Protection Impact Assessments (DPIA) must be undertaken when appropriate.

- The CCG will continue to implement the Records Management and Information Lifecycle Policy which covers all aspects of records management and is consistent with the NHS Records Management Code of Practice for Health and Social Care.

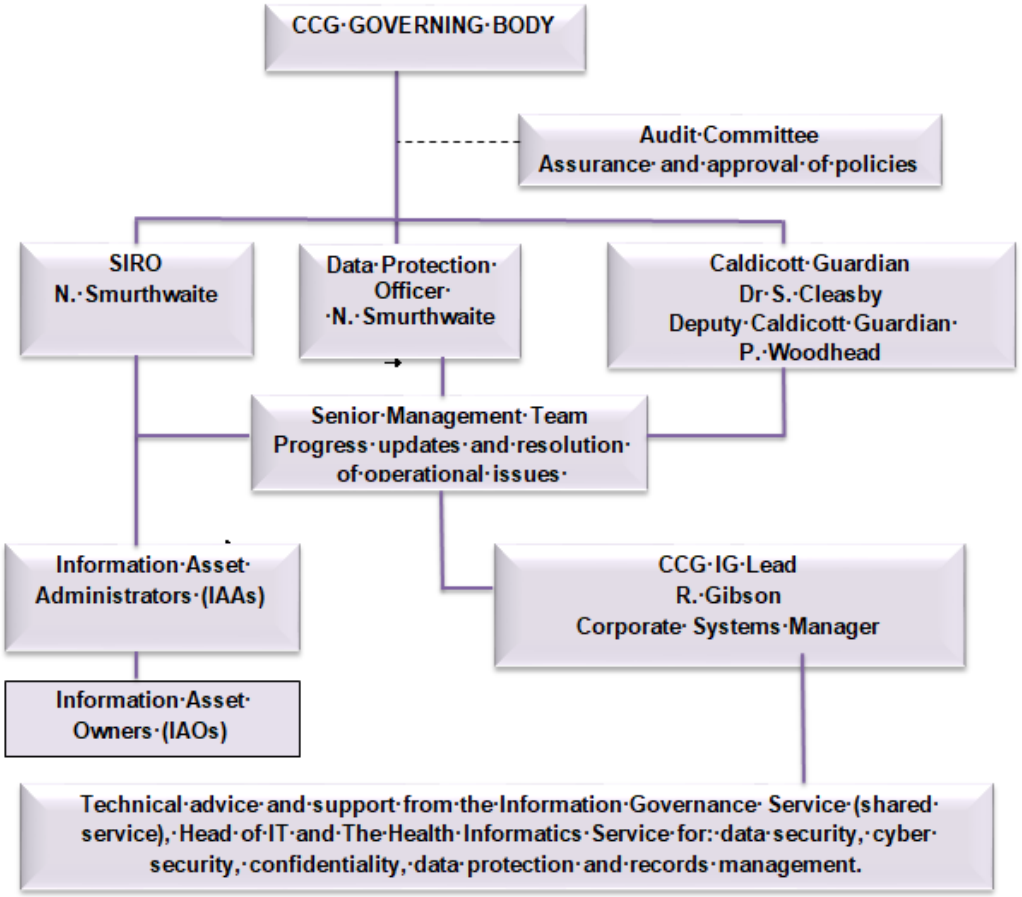
2.5 Third Party Contracts and Clinical Services

- The CCG will take all reasonable steps to 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.

2.6 Information Governance Management Framework – Organisational Chart



The lines of responsibility and accountability are described in the narrative within Section 1.3 (Accountability) of Chapter 1 of this policy book and within 2.7 (Outline of Key Roles and Responsibilities) below.

2.7 Outline of Key Roles and Responsibilities

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, advise 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 of 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.

Caldicott Function

Support to the Caldicott function will be undertaken by the DPO together with the Information Governance Team.

The key responsibilities of the Caldicott function are to:

- Support the Caldicott Guardian (See Appendix A in Chapter 7 of this book).
- 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.

The Senior Information Risk Owner (SIRO) will:

- Be an Executive Director.
- Take overall ownership of each organisation's approach to managing information risk.
- Act as champion for information risk within the CCG executive function and provide advice to the Accountable Officer on the content of the CCG's Statement of Internal Control in regard to information risk.
- Act as the 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 other client organisations' business goals may be impacted by information risks, and how those risks may be managed.
- Implement and lead the information security risk assessment and management processes within the organisation.
- Advise the Governing Body on the effectiveness of information risk management across the organisation.
- Receive training to ensure they remain effective in their role as SIRO.

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 Commissioner's 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 Audit 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.

The Information Governance Lead will:

- Ensure that there is top level awareness and support for information governance resourcing and implementation of improvements.
- Act as the organisational lead for Freedom of Information, Information Security and Records Management and day to day lead for Data Protection including subject access requests (working closely with the Data Protection Officer).
- 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 IG training requirements are included in overall mandatory and statutory matrices and monitor and report on mandatory and statutory information governance training compliance
    - Ensure that evidence is collated and uploaded to the Data Security and Protection Toolkit website and that the assessment is submitted by the 31 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.

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 data protection impact assessment is undertaken in relation to new business processes and systems that may impact on the privacy of individuals and in relation to changes introduced to business processes and systems.

- Assist in the development of business continuity management arrangements for key information assets.

2.8 Resources

Information Governance Support

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

- Advice and guidance on information governance.

- Advice and template resources relating to the Data Security and Protection Toolkit requirement.

- Ensure the consistency of information governance across the organisation.

- Develop information governance policies and procedures.

- Establish protocols on how information is to be shared.

- Develop information governance awareness and training programmes.

- Support organisational compliance with Data Protection, Freedom of Information and other information security related legislation.
- Implement Information Governance Alliance, NHS England, and NHS Digital, NHS X and Department of Health information governance policy, guidance and codes of practice.
- Provide support to the Data Protection Officer, Caldicott Guardian, SIRO, IG Lead and IAOs.

The Information Governance Team holds professional certification in Data Protection and Freedom of Information. The team will support the CCGs 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.

2.9 Governance Framework

Staff Contracts

All CCG staff contracts contain Information Governance related clauses within them. All staff is contractually obligated to take personal responsibility for data security and data protection.

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 for the service. All third party contractors who have access to CCG information assets or process personal information on behalf of the CCG to 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.

Information Assets and Asset Owners

Each information asset has been allocated an Information Asset Owner (IAO) and an Information Asset Administrator (IAA) and is managed in line with supporting operational policies and procedures. 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.

Information Governance (IG) 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	Audit Committee	3 times a year.
Completion of Data Security and Protection Toolkit	Review and sign off of final assessment for submission	IG Lead and SIRO	End of March each year

IG Activity	Includes but not limited to:	Reported to:	Completion by;
Assessment			
Completion of Data Security and Protection Toolkit Assessment	IG Update on progress against the DSPT	Audit Committee	3 times a year.
IG work plans sign off	Operational actions identified following gap analysis against latest version of the Data Security and Protection Toolkit (incorporates the annual information security and risk management annual activities)	CCG IG Lead	July each year
Monitoring of Data Security Training Compliance	Included in Governance Assurance Dashboard Reports	Audit Committee	3 times a year.
IG Update and IG work plans progress reports	Included in Governance Assurance Dashboard Reports	SIRO with a summary report to Senior Management Team	3 times a year.
IG and cyber security incidents	Included in Governance Assurance Dashboard Reports	Audit Committee	3 times a year.
Confidentiality and Data	Included in IG Update Reports Compliance,	SIRO with a summary	3 times a year.

IG Activity	Includes but not limited to:	Reported to:	Completion by;
Protection Assurance Updates	Caldicott issues, confidentiality and data protection by design audits, data flow mapping, information sharing agreements	report to Senior Management Team	
Information Risk Assurance Updates	Included in IG Update Reports IG Incidents, summary of information asset reviews, risk assessments, access reviews and information system security controls.	SIRO with a summary report to Senior Management Team	3 times a year.
SIRO's Annual IG Report	Details of compliance, Data Security and Protection toolkit Scores, information risk management work and details of IG incidents	Audit Committee and Chief Operating Officer	June each year
Requests for Information	Included in Governance Assurance Reports - Numbers of FOI and Subject Access Requests. Compliance against timescales.	Audit Committee	3 times a year.
Policy Reviews	Details of changes to policy or best practices	Circulated to Senior Management Team before submitting to Audit	Rolling schedule

IG Activity	Includes but not limited to:	Reported to:	Completion by;
		Committee and/or Quality, Performance and Finance Committee	

Demonstrating compliance and accountability under Data Protection legislation

The CCGs will ensure they are 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

2.10 IG Training

Mandatory IG 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 Data Security and Awareness training module via the electronic staff record, e-Learning for Healthcare website or where necessary, a classroom session may be used an alternative training method, when they first

join the organisation unless they have completed appropriate Data Security training within the last year and can evidence this.

Staff awareness of IG will also be assessed by questions in the Annual IG Staff survey in order to provide assurance that the training is effective.

Role Specific Training

Role specific training will be identified through the PDR processes. The CCG has identified additional training that those with specific responsibility 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. There will be specific training material available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the training relevant to their roles. An Information Governance Handbook and an Information Asset Owner's Handbook are available for all staff to ensure that they are fully aware of their responsibilities. Learning will be undertaken via the online e-Learning for Healthcare website or through suitable alternatives such as specific themed workshops, workbooks, and face-to-face training and support materials.

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 one or more modules of the online e-learning for Healthcare website, the modules to be undertaken will depend on the type of incident and the outcomes of any investigations into the incident.

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.

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 CCGs are informed of their responsibilities to maintain good Information Governance.	Data Security Awareness Level 1	E-learning	Within 3 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. All Governing Body members that have previously completed the	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
		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.	Practitioner level Access to Health Records or specialist training workshops (externally/ internally sourced)	E-learning or workbook, 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	Practitioner level Access to Health Records or specialist training workshops (externally/internally sourced)	E-learning, workbook or classroom based session	3 yearly

Staff Group	Level	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
		information quality and records management agenda.			
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 or 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 or workbook, individual session*	3 yearly
SIRO	Expert Level	Accountability for organisational	NHS Information Risk Management for	e-learning for Healthcare	3 yearly

Staff Group	Level	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
		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.	SIROs	website or classroom/ workbook/ individual session*	
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 (e-learning) or classroom/ individual session	3 yearly
Information Governance Support	Expert Level	In depth understanding of the Data	Information Security Examination	Specialist course providers	Once only

Staff Group	Level	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
		Protection legislation and information security	Board (ISEB) Data Protection and Information Security courses.		
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

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 regular staff IG compliance checks. 2. Staff IG awareness survey (typically administered via questionnaire). 3. Numbers of Information Governance related incidents and risks reported.

2.11 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 Commissioner's 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 CCGs have an overarching Incident Reporting Framework which includes a section about taking into account NHS Digital's 'Guide to the Notification of Data Security and Protection Incidents'. The IG Team will use the criteria within the guidance 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.

2.12 Communication with Staff

The 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 Audit 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 information as part of the recruitment process. All staff are required to sign the Information Governance declaration to confirm that they have read and understood their responsibilities. A copy of this form will be kept on their staff record.

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.

Chapter 3: Confidentiality and Data Protection Policy

3.1 Introduction

The CCG is committed to the principles of both accountability and transparency which are enshrined within the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018, in relation to its data processing activities.

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. The CCG also recognise 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.

All staff working, employed by, or providing services to the CCG are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 and, for health and other professionals, through their own professions' Codes of Conduct.

The CCG places great emphasis on the need for the strictest confidentiality and information security in respect of personal data and special category data (sensitive personal data). This applies to manual and computer records and conversations about service users' treatments. Everyone working for the CCG is under a legal duty to keep service users' information, held in whatever form, confidential and secure. Service users who feel that confidence has been breached may issue a complaint under the CCG complaints procedure or they could take legal action.

3.2 Aims and Objectives

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 requirements of the General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018 and other related legislation and guidance and to support the assertions of the NHS Digital Data Security and Protection Toolkit.

This policy supports the CCG in its role as commissioner of health services and will assist in the secure and confidential sharing of personal information (personal data and special category data) with its partner agencies.

3.3 Scope

This policy covers:

all aspects of information within the organisations, 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 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, 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

Confidentiality and Data Protection within member practices' premises is the responsibility of the owner/partners. However, the CCG is committed to supporting member practices 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 will continue to work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

3.4 Confidentiality Codes of Practice, Guidance and Legislation

The purpose of this section is to set out the key legislation, codes of practice and guidance which everyone working for the CCG is responsible for observing, to ensure that information (in particular personal information) is managed in line with confidentiality, privacy and security requirements.

General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 - Data Protection Principles

All information and data which can identify a living individual, held in any format (visual/ verbal / paper / electronic / digital media etc.) is safeguarded by data protection legislation. The legislation includes six principles which set out the main responsibilities for the CCG in relation to data protection law.

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except as originally understood or with subsequent consent.

In some instances, judgements have been given which recognise a public interest in disclosure but these are on a case by case basis. United Kingdom courts rely extensively on this duty of confidentiality coupled with the Human Rights Act 1998 in making decisions on breaches of confidence.

The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

Caldicott Principles

The Caldicott Principles should be proactively applied to the handling of all patient identifiable information by the CCG:

Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

Do not use personal confidential data unless it is absolutely necessary

Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Understand and comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

The duty to share information can be as important as the duty to protect patient confidentiality

Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

NHS Digital Guidance

The Health and Social Care Information Centre (now NHS Digital) is responsible for facilitating the management and sharing of data across the re-configured NHS to support both operational and other functions such as planning, research and assessments. NHS Digital produced a Code of Practice: ‘A Guide to Confidentiality in Health and Social Care’ in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

The NHS Care Record Guarantee and Social Care Record Guarantee for England

The NHS Care Record Guarantee and Social Care Record Guarantee for England set out the rules that govern how individual care information is used in the NHS and Social Care. They also set out what control the individual can have over this.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

Health and Social Care (Safety and Quality) Act 2015

The 2012 Act introduced changes regarding access to patient confidential data and placed particular restrictions on access to patient data by commissioning organisations and their support organisations. The 2015 Act introduced provision about the safety of health and social care services in England, about the integration of information relating to users of health and social care services in England and about the sharing of information relating to an individual for the purposes of providing that individual with health or social care services in

England. In particular it introduced a duty to share the NHS number for direct care purposes.

NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable. Regulations under the Act support the sharing and use of information for defined commissioning activities and support NHS structure subject to safeguards.

Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access to data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which govern the sharing of very specific types of data in such areas as;

- Safeguarding Children
- Sexually Transmitted Diseases
- Terminations, Assisted Conception
- Registration of Births and Deaths

- Criminal Investigations
- Terrorism
- Communicable Diseases

This is not an exhaustive list and further guidance can be obtained from the organisation's Caldicott Guardian, SIRO, DPO, or the Information Governance Team.

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

All staff are bound by the codes of conduct produced by their professional regulatory body (where relevant), by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice for Health and Social Care sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

3.5 Principles and Procedures

The purpose of this section is to set out the principles, operational procedures and process which support compliance with data protection and confidentiality law. In summary these include:

- General Principles
- Individual's Rights
- Consent and Information Sharing
- Data Protection Impact Assessments
- Confidentiality and Data Protection by Design Audit Procedures

- Protecting Information
- Personal Data Breaches
- Data Protection Fee
- Use of NHS Number

General Principles

- The CCG is committed to the principles of accountability and transparency in their processing of personal data and special category data under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018.
- The CCG will maintain records on its data processing activities and will conduct regular reviews of the personal data processed and update records of data processing activities accordingly.
- The CCG will regard all identifiable personal information (personal data and special category data) relating to service users, staff and others coming into contact with the CCGs as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The CCG regards all identifiable personal information (personal data and special category data) relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCG will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018, Human Rights Act, the common law duty of confidentiality, the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate,

effective and affordable confidentiality and data protection controls are in place.

- The CCG will adhere to any relevant Codes of conduct and certifications that cover the CCG's data processing activities in order to demonstrate compliance with the requirements of the General Data Protection Regulation (EU) 2016/679 (Articles 40 and 42) and Data Protection Act 2018.

3.6 Individuals Rights

The CCG acknowledges the rights that individuals have in respect to their personal information (personal data and special category data) processed by the CCG and will take steps to ensure these are managed in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018.

The Right to be informed

The CCG will ensure privacy notices are intelligible and easily accessible and meet the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018. The CCG will make Privacy Notices available at the time of collection of the personal data and where personal data is obtained through other sources; the CCG will provide individuals with privacy information within a reasonable period of time and no later than one calendar month.

Where relevant the CCG will ensure privacy notices are written in a language children will understand.

The CCG will maintain a comprehensive privacy notice on its public website.

Please contact the CCG IG Team for advice on the process to follow for providing information about processing and individuals' rights at the correct time.

The Right of Access

Individuals have a right of access to information held about them by the CCG in line with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018.

The procedure for the management of the right of access is set out in the Subject Access Request and Access to Health Record Procedure within Chapter 7 of the Information Governance Procedures Book. This procedure also provides guidance in relation to requests for the records of deceased individuals under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

All staff should familiarise themselves with the Subject Access Request and Access to Health Record Procedure which should be followed for all requests for personal data.

Access to corporate information and records will be in accordance with the CCG's Freedom of Information Act and Environmental Information Regulations Policy.

The Right to Rectification

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 provides individuals with the right to have their personal data rectified if it is inaccurate or incomplete.

A request under the right to rectification may sometimes follow a subject access request.

The outline process for managing requests for personal data to be rectified is set out in Chapter 6 of the Information Governance Procedures Book.

The Right to Erasure

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 provides individuals with the right to erasure which is also known as the 'right to be forgotten'. The right to erasure is not an absolute 'right to be

forgotten'. In law individuals only have a right to have personal data erased and to prevent processing in specific circumstances. Individuals have the right if:

- the personal data is no longer necessary for the purpose which the CCG originally collected or processed it for;
- the CCG is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- the CCG is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the CCG is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the CCG have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- the CCG have to do it to comply with a legal obligation; or
- The CCG have processed the personal data to offer information society services to a child.

The CCG may refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise or defence of legal claims.

There are two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services).

The outline process for managing requests for personal data to be erased is set out in Chapter 6 of the Information Governance Procedures Book.

The Right to Restrict Processing

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 provides individuals with a right to 'block' or suppress processing of their personal data. In law there are some specific circumstances where the CCG is required to restrict the processing of personal data, some of which relate to other 'rights' exercised by the individual. The right applies in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;

- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;

- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or

- The individual has objected to you processing their data under Article 2 and you are considering whether your legitimate grounds override those of the individual.

The outline process for managing requests for personal data to be erased is set out in Chapter 6 of the Information Governance Procedures Book.

The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

The CCG will provide the personal data in a structured, commonly used and machine readable format and provide the information free of charge.

The outline process for managing requests for data portability is set out in Chapter 6 of the Information Governance Procedures Book.

The Right to Object

Individuals have the right to object to the processing of their personal data when it is processed on the grounds of 'legitimate interests' or the 'performance of a task' in the public interest/exercise of official authority (including profiling), when it is processed for direct marketing or processed for the purposes of scientific/historical research and statistics. There are particular conditions attached to each of the above.

In relation to the above grounds for processing and purposes of use, the CCG will inform individuals of their right to object 'at the point of first communication' and in privacy notices.

The outline process for managing requests under the right to object is set out in Chapter 6 of the Information Governance Procedures Book.

The NHS has introduced a new data opt-out provision. This allows people to opt out of their confidential patient information being used for research and planning. If a patient wants to change their choice, they should use the new national data opt-out service to do this. You can find out more about the service at the NHS.uk website on the your NHS data matters web page.

The procedure for compliance with the National Data Out-Out is set out in Chapter 6 of the Information Governance Procedures Book.

Rights in Relation to Automated Decision Making and Profiling

In the event that the CCG carries out any processing deemed to involve automated decision making about an individual (making a decision solely by automated means without any human involvement) or undertakes any profiling activity (automated processing of personal data to evaluate certain things about an individual), it will take steps to ensure the individual's right is managed in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018.

3.7 Consent and Information Sharing

Consent to Process Personal Data

The CCG will establish record and inform individuals about the lawful basis that it is relying on to process personal data. Where appropriate the CCG will also test whether consent should be obtained to meet confidentiality requirements under common law.

In certain circumstances individuals will be unable to provide their own consent as they do not have the capacity to do so. In such situations a person acting as

an advocate may be involved in decisions relating to the use and processing of personal information. This includes:

- Persons appointed by the Court of Protection
- Persons holding a registered Lasting Power of Attorney for health and welfare and those with a Deputyship Order in place
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005.

For further advice on the need to obtain consent, seek advice from the IG Team.

Sharing Confidential Personal Information without Consent

Whilst the default position is that we must not share confidential personal information without consent, there may be occasions when we are required to do so, even though this is against the known wishes of the individual.

Exceptional Circumstances

There are only three exceptional circumstances that disclosure without consent in an individual with capacity may be justified. These are where:

1. Statute law requires e.g. disclosures to the coroner, disclosures to the DVLA where an individual is medically unfit to drive, investigations into fraud in the NHS;
2. There is a court order (ordering the disclosure);
3. Disclosure may be necessary in the public interest where a failure to disclose information may expose others to risk of death or serious harm.

The duty to share information can be as important as the duty to protect patient confidentiality.

Actions to take:

- Discuss the request with the Caldicott Guardian and/or the DPO.

- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- If the request is from the police or another enforcement agency ask for the appropriate request form in line with the Access to Records Procedure. This should clearly evidence the legal power or duty under which the police are making the request.
- Follow any locally agreed Information Sharing Protocols and national guidance.
- Information may also be shared with Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Using and Disclosing Confidential Patient Information for Direct Healthcare

Consent to share personal information for direct care is usually on the basis of implied consent, which may also cover administrative purposes where the individual has been informed or it is otherwise within their reasonable expectations. When information sharing is needed for direct healthcare patients should still be informed about;

- The use and disclosure of their healthcare information and records
- The choices that they have and the implications of choosing to limit how information may be used or shared;
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations;

- The potential use of their records for the clinical governance and audit of the care they have received.

Under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 for processing of personal data in the delivery of direct care and for administrative purposes, the following conditions of lawful processing that are available to all publically funded health and social care organisations in the delivery of their functions will apply:

- GDPR Article 6 (1) (e) 'for the performance of a task carried out in the public interest or in the exercise of official authority', and
- GDPR Article 9 (2) (h) 'medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems'.

Personal Data Relating to Children

Where processing is likely to involve children's personal data, the CCG will ensure relevant privacy notices are written so that they are able to understand what will happen to their personal data and the rights they have.

The CCG will undertake Data Protection Impact Assessments where data processing is likely to involve the processing of children's data and is likely to result in a high risk to the rights and freedoms of children.

Using and Disclosing Confidential Staff Information

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct communications related to their role, salary payment and pension arrangements. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of Freedom of Information Request where the Public Interest in Disclosure is deemed to override confidentiality considerations.

Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and it should only be disclosed, when appropriate, through the proper processes.

Information Sharing Agreements

The organisation will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Data Sharing Code of Practice and the additional safeguards introduced by the Health and Social Care Act 2012.

The CCG is a signatory to the Information Sharing Protocols which should be followed at all times.

Where appropriate the CCG will ensure they are proactive in putting specific information sharing agreements in place to support information governance and transparency requirements.

3.8 Data Protection by Design and Default

It is a requirement of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act that organisations put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual's rights. This is known as 'data protection by design and by default'.

All new projects, processes and systems (including software and hardware) must meet data protection by design and meet confidentiality requirements. To enable the CCG to identify and minimise any data protection risks, a Data Protection Impact Assessment (DPIA) must be undertaken when processing of personal data is likely to result in a 'high risk to individuals'. A DPIA will:

- Identify privacy risks to individuals and fix problems at an early stage
- Demonstrate compliance with the CCG's data protection obligations

- Meet an individual's expectations of privacy
- Help avoid reputational damage which might otherwise occur

All staff should ensure they are familiar with the contents of this procedure.

Please also refer to the Safe Haven and Pseudonymisation Guidelines and Procedure for further information which can be found in the Information Governance Procedures Book.

3.9 Confidentiality and Data Protection by Design Audit Procedures

In order to provide assurance that access to confidential person identifiable information is gained only by those individuals that have a legitimate right of access to the information, the CCG ensures that access to person identifiable information is monitored on at least an annual basis.

Confidentiality and Data Protection by Design Audits focus not just on controls within electronic information management systems, but also on physical access to paper based information. Audits may identify whether confidentiality has been breached, or put at risk through deliberate misuse of a system, or as a result of weak, non-existent or poorly applied controls.

Regular audits will be carried out in line with the Confidentiality and Data Protection by Design Audit Procedures which can be found in the Information Governance Procedures Book.

3.10 Working with Confidential Information

Staff must follow good practice principles and comply with appropriate legislation when working with confidential information:

- Discussions on confidential matters should take place where they cannot be overheard. Take care in public places and at social events.
- Confidential information should never be left open and unattended on a desk.
- Confidential information not in use should be locked away securely.

- Storage systems should be secure and be kept locked at all times.
- All information assets held should be recorded on the Information Asset Register.
- Access to confidential information should be limited to the minimum necessary.
- Consent to share confidential information should be recorded and the sharing limited to that which was agreed.
- Use sealed envelopes marked confidential when sharing confidential information with internal colleagues.
- Confidential paper records must not be taken outside of the workplace except in line with an agreed protocol or procedure.
- Comply with the organisation's procedures for disposal of confidential electronic or paper information.
- Comply with the organisation's policies and procedures on all aspects of information security and seek advice if you are unsure.
- Work related information or images should not be uploaded to social media sites.
- Confidential information must not be given out over the phone except in line with an agreed protocol or procedure.

Additional guidance when working with electronic equipment:

- Ensure you have read and understood the organisation's information security policies and procedures.
- Computer screens should be locked whenever you are away from your device.
- Log off when you have finished using a computer.

- Always remove a Smartcard when you are away from your desk even for a few minutes.
- Restrict access to confidential information which is stored on the server.
- All portable media equipment must be encrypted including memory sticks.
- Downloading confidential information to a non NHS portable device is forbidden.
- Retain confidential information in line with business requirements and record retention schedules.
- Seek advice on fully deleting computer data if you are unsure.
- Follow password guidance and change passwords regularly.
- NEVER share a password or Smartcard with anyone or accept an instruction to do so.
- Electronic equipment must only be disposed of via The Health Informatics Service.
- Portable devices must not be left unattended and on display e.g. in the foot well of a car or passenger seat.
- Keep back-up tapes, memory sticks etc. separate to your mobile device.
- Password protect mobile devices with a strong password.
- Mobile storage devices must only be used in line with agreed local procedures.
- Information should only be kept on encrypted mobile devices for short term operational reasons and this should be backed up to a server regularly.

All staff are personally responsible for ensuring the safe processing of information.

3.11 Transferring Information

All paper transfers of confidential information must be secure:

- If your department needs to routinely transfer confidential information internally or externally ensure that there is an agreed protocol for such transfers.
- Only use sealed envelopes for confidential information.
- Fully address envelopes and mark them private and confidential regardless of how they are to be transferred.
- Large or particularly sensitive files should be double enveloped and sent recorded delivery, hand delivered or a courier should be used.
- Follow up transfers of sensitive confidential information to check receipt.
- Keep confidential information being transported by car out of sight? Ensure it is not left unattended or in the car overnight.
- Special consideration is needed for transfer of information outside the European Economic Area. Please contact the Information Governance Team for further advice.

All electronic transfers of confidential information must be secure:

- Follow all Information Security policies and procedures including the guidance within the IG User Handbook.
- Seek advice from the Information Governance Team or the DPO, if you have any concerns as to the disclosure and/or security of transfer arrangements.
- Only use approved NHS e mail accounts. Confidential patient and staff information may only be transferred using NHS Mail or an approved method of encryption.

- Ensure you do not send confidential information to a personal e mail address. If a member of the public makes a request to correspond by email e.g. complaints or individual funding request correspondence, using their non-secure email address, it is the responsibility of the member of staff to ensure the member of public is provided with a clear explanation of the risks of using unsecure email addresses and consent must be obtained.

- Do not forward emails containing offensive information. Contact the Service Desk (THIS) for advice.

- Where there is a business requirement to download or transfer confidential data, seek advice from the Information Governance Team in the first instance who will advise if the approval of the DPO is required.

- Confidential information should only be transmitted by fax where there is no secure alternative method of transfer available. A cover sheet should be used at all times giving names and contact details of both sender and recipient.

- Check fax numbers regularly, programme them in where possible; send a test fax before sending confidential information and ring to check receipt of all faxes sent.

- Ensure the fax will be received in a safe haven or that a named individual is there to collect it immediately.

- Ensure confidential correspondence is not left unattended on the fax machine if there is a delay in transmission.

Please refer to the Safe Haven and Pseudonymisation Guidelines and Procedure for further information which can be found in the Information Governance Procedures Book.

3.12 Anonymisation and Managing Data Protection Risk

Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data. Anonymisation is of particular relevance, given the increased amount of information being made publicly available through the Government's Open Data agenda. The Protection of Freedoms Act 2012 enhances access to information by requiring a public authority to consider data held in a dataset that is not already published. Where the Freedom of Information Act 2000 requires the publication of a dataset the CCG is required to release it in a form that is reusable.

The CCG will ensure that data released under the Freedom of Information Act 2000 and Government's Open Data Agenda are fully anonymised. All staff will adhere to the Information Commissioner's 'Anonymisation Code of Practice' which describes the steps an organisation must take to ensure that Anonymisation is conducted effectively, while retaining useful data.

3.13 Personal Data Breaches

All staff need to be aware of their responsibilities for keeping personal information secure and ensuring the confidentiality of such information held by the CCG. The duty of confidentiality is written into employment contracts.

A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty may be a disciplinary offence which could result in dismissal and/ or prosecution. No employee shall knowingly misuse any information or allow others to do so. It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

All actual, potential or suspected personal data breaches including breaches of confidentiality must be reported via the CCG's Incident Reporting Policy. All incidents involving patient data should additionally be reported to the Caldicott

Guardian. The DPO should consider whether serious breaches of confidentiality or those involving large numbers of individuals need to be reported to the Information Commissioner via the national process for reporting, managing and investigating information governance serious incidents. It is a legal requirement to report certain types of incident to the Information Commissioner's Office. Where this is required, it must be undertaken within 72 hours of becoming aware of the incident, where feasible.

What should be reported through the incident reporting process?

Misuses of personal data and information security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same incident does not occur again. The following list gives some examples of personal data and information security related incidents which should be reported:

- Sharing of passwords.

- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that the disclosure is not in accordance with the Data Protection Act and the Confidentiality: NHS Code of Practice.
- Transferring or transmitting data in a way that breaches confidentiality.
- Leaving confidential information lying around in public area e.g. photocopier.
- Theft or loss of patient-identifiable or staff identifiable information.
- Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient record and or content of, in ordinary waste paper bin.

3.14 Data Protection Fee

Under the Data Protection (Charges and Information) Regulations 2018 and as organisations that determines the purposes for processing personal data, the CCGs will pay an annual fee to the Information Commissioner's Office. The DPO will ensure the annual fee is paid by the date due.

3.15 Using NHS Numbers

The NHS Number is the national, unique identifier that makes it possible to share patient and service user information across the NHS and social care safely, efficiently and accurately. The Health and Social Care (Safety and Quality) Act 2015 which places a legal obligation on organisations that commission or provide health care or adult social care to include a consistent identifier when processing patient and service user information for purposes that might facilitate the provision of health services and adult social care to individuals.

The CCG will ensure the NHS Number is used as consistent identifier for direct care purposes and that staff follow the NHS Number Principles of Find It, Use It and Share It.

Staff involved with recording service user data need to ensure that it is performed in a timely manner and that the details being recorded are checked with the source at every opportunity. In situations where data is shared between systems it is imperative that the source data be validated initially.

Staff must ensure all patient and service user identifiers including the NHS number are appropriately used and kept secure and confidential. Information sharing agreements or contracts should ensure that the confidentiality and security standards are clear and complied with. The Common Law Duty of Confidentiality and Data Protection legislation constraints continue to apply. If there is a legal basis for sharing information (e.g. consent) and the purpose is likely to facilitate care, then the information must be shared and where it would not require unreasonable effort the NHS Number must be included.

Chapter 4: Information Security Policy (incorporating Network Security) RESTRICTED

Chapter 5: Records Management and Information Lifecycle Policy

5.1 Introduction

The CCG recognises the importance of reliable information in terms of 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 creates, processes, stores, shares and disposes of information.

The Records Management and Information Lifecycle Policy sets out the CCG's overall approach to the management of records and should be read in conjunction with the other information governance policies and procedures detailed in Section 6.5 of Chapter 6 of this book.

The CCG's records are the corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the CCG, its clients and the rights of NHS staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

It is the responsibility of all staff and governing body members including those working on behalf of the CCG, those on temporary or honorary contracts, agency staff and students to comply with this policy.

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.

5.2 Scope

This policy relates to all records held in any format by either CCG.

Examples of records which have been created or collated as a result of the work of the CCG include:-

- Patient information and health records (electronic or paper based)

- Administrative records (including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling)
- Photographs, Microform (i.e. fiche/film) Audio and videotapes, cassettes, CD-ROM, digital images and other images
- Computer databases, output, and disks etc., and all other electronic records
- Material intended for short term or transitory use, including notes and 'spare copies' of documents
- Meeting papers, agendas, records of formal and informal meetings including notes taken by individuals in note books and bullet points are all subject to the above
- Emails and text messages

If any aspect of records management is contracted to another organisation the CCG will seek assurances that the appropriate systems and processes are in place.

Partner organisations providing support services to the CCG such as providers of commissioned services and third parties that have access to CCG owned records will be expected to manage CCG owned records in accordance with this policy.

5.3 Aim

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

This will ensure that:

- **records are available when needed** - from which the CCG is able to form a reconstruction of activities or events that have taken place;

- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;

- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;

- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;

- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;

- **Records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;

- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value;

- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management; and

- **The CCG complies with the law and professional guidance.**

5.4 Legal and Professional Obligations

All NHS records are public records under the Public Records Act 1958. This provides statutory obligations upon the CCG. The organisation will take actions as necessary to comply with the legal and professional obligations set out in the

Records Management Code of Practice for Health and Social Care, in particular:

- The General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018
- Access to Health Records Act 1990
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Human Rights Act 1998
- Protection of Freedoms Act 2012
- Caldicott Principles
- NHS Digital Guide to Confidentiality in Health and Social Care 2013
- The Common Law Duty of Confidentiality
- Health and Social Care (Quality and Safety) Act 2015
- The Nursing and Midwifery Council Code of Professional Conduct.

and any other new or existing legislation affecting records management.

5.5 Records Management Procedures

Records are held to ensure that information is available within the CCG:

- To support the care process and continuity of care
- To support day to day business of a CCG
- To support evidence based practice
- To support sound administrative and managerial decision making

- To meet legal requirements, including requests from patients under the General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018 and Access to Health Records Act 1990
- To assist clinical and other audits
- To support improvements in clinical effectiveness through commissioning/research and also to support archival functions by taking account of the historical importance of material and the needs of future research
- Whenever and wherever there is a justified need for information, and in whatever media it is required

In order to ensure records can be identified and retrieved when needed all staff should follow the guidance provided:

- Corporate Records Management Guidance (see Chapter 5 of Information Governance Procedures Book)
- Guidance on Creating a Corporate Filing Structure (see Chapter 5 of Information Governance Procedures Book)
- Patient Record Keeping Best Practice (see Chapter 5 of Information Governance Procedures Book)
- Good Practice Data and Information Quality Standards (see Chapter 5 of Information Governance Procedures Book)

Records must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails should track all use and changes. Records must be held in a robust format, which remains readable for as long as records are required.

All individuals undertaking roles and responsibilities on behalf of the CCG are responsible for the safe custody of records in their use. Personal confidential information must be handled in accordance with Data Protection legislation, the Records Management Code of Practice for Health and Social Care and any other guidance.

To ensure quality and continuity of operational services all records should be accurate and up to date. Records and record keeping should be kept according to professional guidelines. Local procedures should be developed to ensure data quality for both manual and electronic records. These procedures should be passed on to all staff and Governing Body members who are responsible for recording the information. It is also essential that these procedures are reviewed and updated regularly.

Staff with clinical record handling responsibilities should follow the appropriate legal and professional guidance at all times.

Staff using SMS messaging, WhatsApp or Microsoft Teams should be made aware that all information captured by any of these tools may be disclosable under Freedom of Information Act 2000 and data protection legislation.

5.6 Tracking of Records

Accurate recording and knowledge of the whereabouts of all records is crucial if the information they contain is to be located quickly and efficiently.

Tracking mechanisms should record the following (minimum) information:

- The item reference number or other identifier
- A description of the item (e.g. the file title)
- The person, unit or department, or place to whom it is being sent
- The date of the transfer to them

Further guidance on tracking clinical records is provided in Chapter 5 of Information Governance Procedures Book.

5.7 Manual Record Storage

Storing Current Paper Records

When a record is in constant or regular use, or is likely to be needed quickly, it makes sense to keep it within the area responsible for the related work. Storage equipment for current records will usually be adjacent to users i.e. their

desk drawers or nearby cabinets, to enable information to be appropriately filed so that it can be retrieved when it is next required. Records must always be kept securely and when a room containing records is left unattended, it should be locked. A sensible balance should be achieved between the needs for security and accessibility.

There is a wide range of suitable office filing equipment available. The following factors should be taken into account:

- Compliance with Health and Safety regulations (must be the top priority)
- Security (especially for confidential material)
- The user's needs
- Type(s) of records to be stored
- Their size and quantities
- Usage and frequency of retrievals
- Suitability, space efficiency and price

5.8 Digital and other media records

Follow guidance within Chapter 5 of the Information Governance Procedures Book and instructions from Information Technology support teams:

- Corporate Records Management Guidance
- Guidance on Creating a Corporate Filing Structure
- Patient Record Keeping Best Practice
- Keeping Patient, Client or Personnel Information Physically and Electronically Secure.

5.9 Records in Transit

Labelling and Packing

If records are being delivered to another location they should be enclosed in envelopes or opaque wallets and sealed for transfer. Any records that may be damaged in transit should be enclosed in suitable padding or containers.

For larger quantities, records should be boxed in suitable boxes or containers for their protection.

Each box or envelope should be addressed clearly and marked confidential with the sender's name and address on the reverse of the envelope and signed for on receipt. In the case of communications relating to healthcare and other sensitive issues it may be more appropriate not to include information on the outside of the envelope other than a Box No if available.

There are various options if records are to be mailed, such as recorded delivery, registered mail etc. Please see further details within the Safe Haven Guidelines and Procedures in Chapter 3 of the Information Governance Procedures Book.

When choosing options staff should consider the following: -

- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
- Does the mail provider offer "track and trace" options and is a signature required on delivery?

In addition, the number of records per envelope should be considered. It is recommended that no more than 20 records should be placed in one envelope. Ensure the correspondence is suitably secure. Seek guidance from the IG Team in relation to secure transfer of responses. Transit envelopes must **not** be used for sending records.

Items sent in any internal mail system should be fully addressed, sealed and marked private and confidential if appropriate.

For further advice please contact the Information Governance Team.

Handling and Transporting Records

- No-one should eat, drink or smoke near records
- Clinical records being carried on-site e.g. from the archive storage to the department, should be enclosed in an envelope
- Records should be handled carefully when being loaded, transported or unloaded. Records should **never** be thrown
- Records should be packed carefully into the boot of vehicles to ensure that they will not be damaged by the movement of the vehicle
- Vehicles must be fully covered so that records are protected from exposure to weather, excessive light and other risks such as theft
- No other materials that could cause risks to records (such as chemicals) should be transported with records
- Vehicles containing records should be locked and the records should be locked in the boot so that they are kept out of sight, particularly when the vehicle is stationary.

5.10 Taking Records Off Site

Records should only ever be taken off site with the approval of the line manager. Security of these records should be paramount, especially in the case of confidential records. The local records manager and/or the Information Governance Team can provide advice on the precautions to take. Individuals are responsible for the safe custody of records in their use both on and off CCG or client premises. Personal confidential information must be handled in accordance with Data Protection legislation.

Records should not be left unattended and visible. If, in exceptional circumstances, a confidential record is to be taken home (with prior line manager approval), it must be stored securely. It is essential that any such records are tracked out of the organisation so that staff are aware of the location of the record.

Within the CCG, faxed information should be transferred internally through the use of 'Safe Haven' fax machines ensuring the maintenance of confidentiality. For further guidance refer to the Safe Haven Guidelines and Procedure within Chapter 3 of the IG Procedure Book.

5.11 Incident Reporting

If a record is missing, lost or inappropriately disclosed it should be reported to the relevant line manager as soon as possible and the incident should be recorded on the CCG's online incident reporting system (DATIX).

Incidents involving the loss of any records containing personal data should be reported promptly and the IG Lead, DPO and SIRO should be informed. In the case of patient data related incidents, the Caldicott Guardian should also be informed. Certain losses may need reporting externally to the Information Commissioner. The DPO will be responsible for ensuring that the Senior Management Team and Audit Committee are aware of any breaches of this policy and for overseeing any investigations or action plans.

5.12 Retention of Records, Archiving and Disposal

Retention

- It is a fundamental requirement that all CCG and client records are retained for a minimum period of time for legal, operational, research and safety reasons.
- The length of the retention period depends upon the type of record and its importance to the business of the CCG. The destruction of records is an irreversible act, whilst the cost of keeping them can be high and continuing.

- The CCG has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care. See the CCG Records Retention Period Register on the Intranet.
- If a particular record is not listed within the register, advice must be sought from the Information Governance Team who will establish the retention period in consultation with the relevant IAO and the IG Lead.
- The CCG will ensure compliance with any local or national judicial instruction to retain (past the designated retention time) certain categories of record which may fall under the scope of an inquiry or inquest. Adhere to the Guidance Relating to Document Retention and Court Proceedings which can be found within Chapter 5 of the Information Governance Procedures Book.

Archiving

- Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. The storage of closed records should follow National Archives guidance relating to environment, security and physical organisation of the files and closed records should therefore be stored with the CCGs document storage contractor.
- Data Protection legislation (Article 5 (e) of the GDPR) does not permit the keeping of personal information for longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (e.g. archiving purposes in the public interest, scientific or historical research purposes).
- Any documents identified as requiring permanent preservation must be transferred to the appropriate repository e.g. National Archives Approved Places of Deposit. Disposal decisions made following an appraisal must be recorded.

Disposal

- It is particularly important under both Data Protection and Freedom of Information legislation that the disposal of records – which is defined as the

point in their lifecycle when they are either transferred to an archive or destroyed is undertaken in accordance with this policy.

- The destruction of records is an irreversible act. Many NHS records contain sensitive and/or confidential information and their destruction must be undertaken in secure locations and proof of secure destruction may be required. Destruction of all records, regardless of the media, should be authorised and should be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure. A record of destruction must be kept. See the guidance on Scanning Records and Destruction of Paper Records and the template in the Certificate of Records / Information for Permanent Destruction guidance. These documents can be found in Chapter 5 of the Information Governance Procedures Book.

- When destroying master copies of records the following must be undertaken:

- The intended destruction must be authorised. See the approval form within the Certificate of Records / Information for Permanent Destruction guidance.

- A list of records being destroyed must be kept. This should show their reference, description and date of destruction (disposal schedules would constitute the basis of such a record).

- Certification should be received and kept as proof of destruction by the Information Governance Team.

- If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.

- At no time should records be left unsecured whilst awaiting destruction.

Further guidance on archiving and disposal of records can be found in the Corporate Records Management Guidance which can be found within Chapter 5 of the Information Governance Procedures Book.

5.13 Scanning

For reasons of business efficiency or in order to address problems with storage space, the CCG may consider the option of scanning paper records into electronic records.

Where this is proposed, the scanning equipment must be of a quality to meet the British Standards and in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008) and the scanning guideline should be followed (see Chapter 5 of Information Governance Procedures Book).

5.14 Data and Information Quality

Data quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever this is required. Data quality is vital to effective decision making at all levels of the organisation.

It is also important to ensure that the data quality of personal data is of a high standard in order to comply with the Data Protection Principles within the GDPR in particular Article 5 (d) 'accurate and, where necessary, kept up-to-date' and to satisfy the data quality requirements within the NHS Care Record Guarantee.

Within any record keeping system, there is a primary instance which can be considered the version that needs to be kept and this will normally be held by the person or the team with the function to provide the service or activity about which the records relates.

It is not necessary to keep duplicate instances of the same record unless it is used in another process and is then a part of a new record. An example of this is incident forms. Once the information is transcribed into the incident management system, there is no longer a need to hold the (now) duplicate instance of the original form used to record the incident.

Where multiple copies of the same record exist the master copy should be identified, along with the owner, where it is stored and any changes or additions should be made to the master copy.

The standards for good data quality are reflected in the criteria below. Data needs to be:

- Complete (in terms of having been captured in full)
- Accurate (the proximity of the data to the exact or true values)
- Relevant (the degree to which the data meets current and potential user's needs)
- Accessible (data must be retrievable in order to be used and in order to assess its quality)
- Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised national and local standards)
- Defined (understood by all staff who need to know and reflected in procedural documents)
- Appropriately sought (in terms of being collected or checked with the service user during a period of care)
- Appropriately recorded and free from duplication

For guidance on data quality management please see Chapter 5 of Information Governance Procedures Book.

5.15 Using NHS Numbers

The NHS number is a unique way of identifying patients in NHS systems. With this in mind it is imperative that this is recorded correctly and in all systems where patient information is present.

The Personal Demographics Service (PDS) and Exeter will be used to obtain verified NHS numbers i.e. NHS number status and as PDS has significant historic data it will enable record matching process and support the resolution of data anomalies.

5.16 Using Electronic Signatures

In order to ensure the security and legal validity of an e-signature the use of a scanned representation of a handwritten signature must be recorded by the relevant team.

Images of signatures should be used only where a clear audit trail of authorisation including written permission has been granted by the signatory. Though it is only a small deterrent to copying images of signatures, they should be sent outside the organisation in PDF files rather than emails, Word documents or spreadsheets. The PDF files should be created with the highest levels of protection.

Documents containing the image of another person's signature must not be sent without a clear audit trail of authorisation including written permission of the person concerned, unless prior delegation and clearance procedures have been agreed. In such cases:

- such agreement, including the list of recipients, must be obtained in advance for each document.
- the content of the document must not be changed after authorisation to issue it has been obtained
- once such a document has been sent, it must not be sent again (or to additional recipients) without further explicit authorisation.

A ‘clear audit trail of authorisation’ can be achieved by an email communication from the mailbox of the signatory (or person to whom the signature relates) evidencing their permission for its use. The audit trail recording that the document/form has been signed and establishing the signatory’s identity must be accessible for the length of the retention period required for the document/form, as set out in the CCG’s Record Retention Period Register.

All staff who allow a proxy to access their email account or scanned signature must ensure that the proxy is informed of the limits of their authority in the sending of emails or signing documents on behalf of the member of staff.

Electronic signatures should not be used in transactions where there is a legal requirement for a written signature, for example in the signing of a deed or other document where the signature is required to be witnessed.

5.17 Emails as Records

All emails sent or received by anyone with a CCG email account can be classed as a CCG record.

If an email does relate to the conduct of the CCG's business such as information likely to be required for the determination of actions or decision making then it is considered a record.

All emails could be produced in a Court of Law, under the eDiscovery regulations.

To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities and decision making. It is important that email messages and their attachments which are considered as 'records' are moved from individual mailboxes and managed in the same way as other records.

Emails have differing retention periods dependent on their subject and content. Emails are subject to the same records management principles as the equivalent record in any other format. Please refer to the CCG Records Retention Period Register for details of the minimum retention period for specific record types.

Email should only be used to send confidential information where it is sent between approved secure email addresses (e.g. NHS Mail, COIN sender and receiver with password protected attachment) or where it is adequately protected through the use of an encryption solution e.g. using THIS Encrypt solution, WinZip version 9.0 or above or Sophos encrypt. Seek advice from the Information Governance Team if you require advice on emailing information securely.

The Email system should not be used for long term storage. Emails considered as records should be stored in the relevant filing system and then be deleted from the inbox/sent items box. See Chapter 5 of Information Governance Procedures Book for instruction on how to save email to a network drive location.

Emails sent from or to personal email accounts which relate to work matters may be considered public records for the purpose of legislation such as the Freedom of Information Act 2000.

5.18 Digital, Audio, Visual, Photographic, Text and other Electronic Records

All records are subject to this policy regardless of the format in which they are held.

5.19 Access to Records

Under Article 15 of the GDPR data subjects have the right to access personal information held about them by the CCG, subject to certain exemptions. Please refer to the Subject Access Request and Access to Health Records Procedure (Chapter 7 of Information Governance Procedures Book).

Under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 individuals have the right to access corporate information, subject to certain exemptions. Please refer to the Freedom of Information and Environmental Information Regulations Policy.

5.20 Decommissioning of Buildings/ Vacating Premises

It is the responsibility of the CCG's management team to undertake a visual check of CCG premises that are being closed to ensure that all assets of the CCG (including information assets) have been removed.

5.21 Records Management Systems Audit

The CCG will ensure that arrangements are in place to audit the Records Management and Information Lifecycle Policy, processes, implementation and compliance with legal, regulatory and statutory guidance. The Audit Committee

may request an independent audit to be conducted to provide further assurance of compliance, overall adequacy and effectiveness of the CCG's systems.

The results of audits will be reported to the CCG's Audit Committee.

Audits of individual corporate record systems will be conducted in line with the 'Corporate Records Management Guidance' in Chapter 5 of Information Governance Procedures Book.

Clinical Record Audits will be conducted as appropriate in line with good practice and professional guidelines.

5.22 Information Asset Registers

All information assets (record collections) held by the CCG must be included in an Asset Register which should include as a minimum:

- Name of Information Asset
- System Type
- Description of the purpose of the asset
- Purpose of processing
- Data Held
- Any Joint Data Controllership
- Physical location of the asset
- Class – e.g. personal or business
- Components and format e.g. database, paper files
- Name of Information Asset Owner
- Any special categories of personal data and description of that data
- Lawful basis of processing of personal data
- Critical assets
- Risk Assessment
- Business continuity plans
- Access controls
- Retention time of the information asset
- Description of manner of secure destruction of the information asset
- Additional information e.g. data flows

5.23 Clear Desk Policy

Under no circumstances should personal confidential information be left out in the open e.g. on an unattended desk or on a computer screen or any place visible to the public. Where rooms containing records are left unattended, they must be locked. Personal confidential information should be stored securely in either a locked cabinet or within a secure environment on a computerised system.

When storing electronic records, care must be taken to ensure that no personal identifiable information e.g. health records, human resources records etc., are stored in public/shared folders or on the local drive of the PC. All records of this nature must be stored within a folder that can only be accessed via a password or within a specific secure area. Restricted access can be set up by contacting The Health Informatics Service Desk.

All staff should be aware that non-personal corporate information may be confidential and similar care should be taken of these records.

Please refer to **section 4.20 Clear Desk and Clear Screen Procedure.**

Chapter 6: Training, Implementation and Monitoring

6.1 Training and Guidance

All staff are effectively informed about their information governance responsibilities, along with the policies included within this book, through annual Data Security Awareness training, staff briefings and other bespoke awareness sessions, the IG User Handbook, bulletins or a combination of these.

All line managers must actively ensure that their staff undertake and complete the annual mandatory Data Security Awareness training and ensure that all new employees are provided with the IG User Handbook and an explanation as to the service's records management arrangements including the controls applied to paper and electronic files containing person identifiable and business sensitive information.

It is the line managers' responsibility to ensure that all staff are made aware of their record keeping responsibilities through generic and specific staff training and guidance so that they understand:

- what they are recording and how it should be recorded;
- why they are recording it;
- how to validate information with the patient or carers or against other records – to ensure that staff are recording the correct data;
- how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;
- the use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and
- how to update information and add in information from other sources.

Additionally, the CCG will ensure that users of information systems, applications and the network are provided with the necessary information security guidance and awareness to discharge their information security responsibilities.

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 processes.

6.2 Implementation and Dissemination

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

This policy book will be reviewed every two years or in line with changes to relevant legislation or national guidance.

6.3 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 the mandatory assertions of the Data Security and Protection Toolkit.** The Audit Committee will monitor overall progress through receipt of the quarterly Governance Assurance Dashboard Report 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 Audit Committee will monitor progress via the Governance Assurance Dashboard Report.
- **All Information Asset Owners (IAOs) trained in their role and undertaking annual (as a minimum) risk reviews of information assets they are responsible for. New information assets will be identified through this review process.** The Audit Committee and the SIRO will monitor progress via the annual SIRO report.
- **Statistically validated reduction in Information Governance related incidents.** Monitoring of incidents by the Audit Committee.
- **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.

- **Staff know who and where to direct data protection and confidentiality concerns and queries to.** Results of annual information governance staff survey.

In addition, compliance will be monitored through the commissioning of external and internal audits. Specific technical security audits may be commissioned when necessary.

6.4 Legal References and Guidance

- Access to Health Records Act 1990 Health and Social Care Act 2012
- Audit and Internal Control Act 1987
- Bribery Act 2010
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Enterprise and Regulatory Reform Act 2013
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018
- Health and Social Care Act 2012
- Health and Social Care (Quality and Safety) Act 2015
- Health and Social Care Information Centre Guidance (NHS Digital)
- Health Service (Control of Patient Information) Regulations 2002
- Human Rights Act 1998
- Information Commissioner's Guidance Documents
- ISO/IEC 27001:2005 Specification for an Information Security Management system

- ISO/IEC27002:2005 Code of Practice for Information Security Management
- National Data Guardian's Ten Data Security Standards
- NHS Act 2006
- NHS Information Security Management Code of Practice 2007
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Professional Codes of Conduct and Guidance
- Protection of Freedoms Act 2012
- Public Records Act 1958
- Public Interest Disclosure Act 1998
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- www.getsafeonline.org

This is not an exhaustive list and further guidance can be obtained from the Information Governance Team.

6.5 Associated Documentation (Policies, protocols and procedures)

The CCG will produce appropriate procedures and guidance relating to information governance as required by related policies. This includes an Information Governance Handbook which is updated annually and has been shared with all staff. New staff sign for receipt and confirm that they have read the handbook.

This policy book should be read in conjunction with the associated procedures set out within the IG Procedures Book (including but not limited to):

- Confidentiality and Data Protection by Design Audit Procedures
- Data Protection Impact Assessment Procedure

- Safe Haven Guidelines and Procedure
- Subject Access Request and Access to Health Records Procedure

Additionally it should be read in conjunction with:

- Standards of Business Conduct
- Anti-Fraud, Bribery and Corruption Policy
- Business Continuity Plan
- Disciplinary Policy
- Equality and Diversity Policy
- Freedom of Information and Environmental Information Regulations Policy
- NHS mail Acceptable Use Policy.
- Incident Reporting Policy
- Interagency Information Sharing Protocol
- Integrated Risk Management Framework
- Risk Management Policy
- System Level Security Procedures
- Whistleblowing Policy

The above procedures can be found on the Intranet.

6.6 Glossary of Terms

Bulk transfer of person identifiable or sensitive data	Used to describe information relating to 51 or more individuals.
Consent	The consent of the 'data subject' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
Corporate Information	All categories of corporate information should be regarded as confidential in the first instance although they may be releasable through the Freedom of Information Act regime, including via the Publication Scheme. This includes (but is not limited to): • Governing Body and committee meeting papers and minutes • Tendering and contracting information • Financial information • Project and planning information
Data Breach	Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Controller	Data Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor	Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Data Protection Officer (DPO)	The DPO is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance which includes conducting assurance audits.
Data Subject	An identified or identifiable 'living individual' whose personal data is processed by a controller or processor. Otherwise known within data protection legislation as a 'natural person'.
Encryption	The process of transforming information (referred to as plain text) using an algorithm (called 'cipher') to make it unreadable to anyone except those possessing special knowledge, usually referred to as a 'key'.
Health Record	Information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.
Information Asset Owners (IAO)	Are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several information assets.
Information Asset Register	Is a list of information assets owned by the CCG
Information Assets	Are operating systems, infrastructure, business applications, off the shelf products, services, user-developed applications, records, and information.
Mobile Computing	Covers the use of portable computing devices, such as laptops, mobile phones, tablet computers, memory sticks or equivalent mobile computing equipment.

Network File Server	Is computer hardware with large storage capacity which is held in a highly secure area.
Personal Data	Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, including (but not limited to); • Name • Date of Birth • Post Code • Address • National Insurance Number • Photographs, digital images etc. • NHS or Hospital/Practice Number • Location data Personal data that has been pseudonymised e.g. key coded, can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.
Processing	Processing means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each identifiable patient data item. It enables NHS organisations to undertake secondary usage of patient data in a legal, safe and secure manner.

Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (the ISO standard, ISO 15489-1:2016 Information and documentation - records management).
Records Management	The process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.
Responsible User	Individual members of staff who personally adhere to the CCGs IT Security Policy (incorporating Network Security) and make use of the computer facilities provided to them by the CCG in an appropriate and responsible fashion.
Safe Haven	A term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the CCG whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles.
Senior Information Risk Owner (SIRO)	The SIRO is a senior officer of the CCG. The SIRO acts as an advocate for information risk across the CCG and leads and implements the information risk assessment programme.

Special Category Data	Special Category Data (or sensitive personal data) are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Subject Access Right	Entitles the data subject to have access to and information about the personal data that a controller has concerning them. Also known as the Right of Access.

6.7 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.

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

Please see Appendix C of Chapter 7 for Equality Impact Assessment.

Chapter 7: Appendices

Appendix A: 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 Guardian 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 intranet. This role will be primarily supported by the Confidentiality Code of Practice for Health and Social Care.

The Caldicott Guardians 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 CCG benefits from lessons learned by sharing with the Quality and Safety Committee. The agreed acceptable risks will also be recorded in the Caldicott Log. Specific actions and improvements to address any gaps compliance relating to data protection and confidentiality will be managed through the CCG's Information Governance Work Programme.

Appendix B: Information Governance Declaration Form 2020- 23

This declaration must be signed by all NHS Calderdale Clinical Commissioning Group (CCG) employees, including temporary, seconded staff or those contracted from other organisations.

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 and confidentiality breaches

It is important to remember that you are accountable for your computer login and that all activity is auditable. Confidentiality and Data Protection by Design 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.

You have a responsibility to report any information governance and IT related incidents, including cyber security incidents through the CCG's Incident Management and Reporting system – DATIX (cyber security incident must also be reported to the IT Service desk). If you are involved in an information governance related incident it may be necessary to undertake a training needs assessment as part of the lessons learned process, to consider if there is any further training required.

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 card access etc.) with which I have been issued, when I leave / change roles.

Please sign and return this form only to Human Resources, when signed this declaration will be held on your personal file.

Signed:

Name (Please Print):

Date:

Job Title:

Team:

Contact Telephone number:

Appendix C: Equality Impact Assessment

Title of policy: Information Governance Policy Book

Names and roles of people completing the assessment:

Caroline Squires, Information Governance Manager

Date assessment started/completed: February 2021

1. Outline

Give a brief summary of the policy

The aim of this policy book is to ensure that all staff understand their obligations with regard to information governance such that 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 requirements of the General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018 and associated legislation and guidance.

What outcomes do you want to achieve

That the CCG has compliance with the requirements of General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018 and other related legislation and guidance.

That all staff understand confidentiality and data protection obligations with regard to personal confidential information which they come into contact with in the course of their work.

That no Data Protection enforcement activity is undertaken utilising the ‘investigatory powers’ or ‘corrective powers’ of the Information Commissioner.

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;

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative, positive or neutral?	What action will be taken to address any negative impacts or enhance positive ones?
Age	No	Neutral	N/A
Disability	The data protection framework protects personal data 'concerning health' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). Additional safeguards are provided throughout the data protection framework.	Neutral	N/A
Disability	The standards of consent are higher under the data protection framework than under the 1998 Act. This may have an impact on those incapable of giving consent which is 'freely given, specific, informed and unambiguous', such as those who have a learning disability.	Positive	Under the GDPR, consent to process personal data can be given legally by another with a lasting power of attorney or through the Court of Protection.
Gender reassignment	The data protection framework protects	Neutral	N/A

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative, positive or neutral?	What action will be taken to address any negative impacts or enhance positive ones?
	personal data 'concerning health' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). Additional safeguards are provided throughout the data protection framework		
Marriage and civil partnership	No	Neutral	N/A
Pregnancy and maternity	The data protection framework protects personal data 'concerning health' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). Additional safeguards are provided throughout the data protection framework.	Neutral	N/A

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative, positive or neutral?	What action will be taken to address any negative impacts or enhance positive ones?
Race	The data protection framework protects personal data 'revealing racial or ethnic origin' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4).	Neutral	N/A
Religion or belief	The data protection framework protects personal data regarding 'religious or philosophical beliefs' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4).	Neutral	N/A
Sex	No	Neutral	N/A
Sexual orientation	The data protection framework protects personal data 'concerning sex life and sexual	Neutral	N/A

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative, positive or neutral?	What action will be taken to address any negative impacts or enhance positive ones?
	orientation' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). The existing condition for processing personal data 'for the purpose of identifying or keeping under review the existence or absence of equality of opportunity' is newly expanded to include personal data concerning an individual's sexual orientation.		
Carers	No	Neutral	N/A
Other relevant group	No	Neutral	N/A
Human Rights	Yes	Potentially negative in relation to accessing of emails	Monitoring of email and internet usage must ensure that the employee's right to privacy is respected. However, in exceptional

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative, positive or neutral?	What action will be taken to address any negative impacts or enhance positive ones?
		and internet usage.	circumstances and following proper protocol, individual's privacy cannot be guaranteed at work.
Health Inequalities	No	Neutral	N/A

3. Impact on equality groups

If any negative/positive impacts were identified are they valid, legal and/or justifiable? Please detail.

No anticipated detrimental impact on any equality group. The data protection framework maintains the strong protections that currently exist to protect individuals and the processing of personal data that would reveal protected characteristics. The policy is applicable to all staff and adheres to legal requirements and best practice. There are no statements, conditions or requirements that disadvantage any particular group of people with a protected characteristic.

4. Monitoring, Review and Publication

How will the impact and effectiveness of the actions be monitored/reviewed and by whom?

Monitoring of any issues of unlawful treatment of protected groups of staff (or others) (such as harassment or discrimination) relating to the implementation of this IG Policy Book

When will this EQIA be reviewed and by whom?

Review will be at policy refresh

Lead Officer: Corporate Systems Manager

Review date: Policy refresh

5. Sign off

Lead Officer: Equality and Diversity Manager

Director: Corporate Systems Manager

Date approved: [enter date on approval of policy]