NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY AND MANAGEMENT FRAMEWORK 2019 - 2021

Ratification Process

Lead Author:	CCG Information Governance Manager CCG Corporate Support Manager (IG)
Reviewed by:	CCG IG, BI & IM&T Steering Group
Approved by:	CCG IG, BI & IM&T Steering Group – 18th July 2019
Endorsed by:	Integrated Performance and Assurance Committee - 27th August 2019
Ratified by:	CCG Governing Body – 3rd September 2019
Version:	1.0
Review date:	July 2021 (or earlier if significant change to local or national requirements)
Valid on:	3rd September 2019

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the IG, BI and IM&T Steering Group and endorsed by the Integrated Performance and Assurance Committee (IPAC)
Dissemination	This Policy will be promoted to all staff within the CCG and held on the CCG's website.
Implementation	The Director of Finance (SIRO) is responsible for monitoring the application of the policy by ensuring that: • The Policy is brought to the attention of all employees and building users; • Managers are aware of their responsibilities for ensuring that staff under their control implement the policy; • Staff are informed and consulted as appropriate; • Appropriate training and guidance is provided to staff; • Corporate business processes support the implementation of the Policy.
Training	Training will be undertaken as part of the CCG's induction process.
Audit	Implementation of the Policy will be monitored in line with Data Security and Protection Toolkit requirements.
Review	This policy and associated strategy will be reviewed in May 2021 or earlier if required, taking into account any national changes to legislation or statutory requirements that may be required, and/or guidance from the Department of Health or other regulatory body.
Links with other Documents	This Policy should be read in conjunction with key CCG policies listed in Appendix C.
Equality and Diversity	The Human Resources Advisor with responsibility for E&D has carried out an Equality & Diversity Impact Assessment and concluded that the Policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date Ratified
1.0	Whole document	IG Policy and IG Management Framework combined into a single Policy.	3rd September 2019

CONTENTS

Page

1. Introduction

The Information Governance Framework (the 'Framework') is a national framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management and regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.

The standards are set out in the Data Security and Protection Toolkit (DSPT) as a road map enabling Cambridgeshire and Peterborough CCG (the 'CCG) to plan and implement standards of practice and to measure and report compliance on an annual basis. The CCG's performance against these standards is mandated by and reported to the Department of Health and forms a part of the assurance processes associated with the Care Quality Commission; NHS England and NHS Improvement (NHSE & NHSI) and the NHS Resolution risk management standards.

This Policy sets out the overarching Framework of law and best practice for the strategic Information Governance agenda and looks at the operational and management structures, roles, responsibilities, systems, policies and audit controls that the CCG intends to establish to ensure such issues are appropriately addressed throughout the organisation. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the CCG. Senior leadership through the appointment of a Senior Information Risk Owner (SIRO) demonstrates the importance of ensuring information security remains high on the CCG Governing Body agenda.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management. It is therefore of paramount importance to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

This Policy gives assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care for our population. The Policy and its supporting standards and instructions are fully endorsed by the Governing Body who will ensure that sufficient resources are provided to support its requirements.

2. Scope

This Policy applies to:

- All staff working for and on behalf of the CCG;
- All types of information held or processed by the CCG (paper and electronic);
- Organisations or staff holding or processing data on behalf of the CCG;
- All Information Technology application systems within the CCG.

This Policy covers all aspects of information within the organisation, including but not limited to:

- Patient/client/service user information;
- Personnel information;
- Organisational information.

This Policy covers all aspects of handling information, including but not limited to:

- Structured record systems – paper and electronic
- Transmission of information –email, post, telephone and in exceptional circumstances, fax.

This Policy covers all information systems purchased, developed and managed by, or on behalf of the organisation, and any individual directly employed or otherwise by the organisation.

3. General Principles

'Information Governance' is an umbrella term for a collection of distinct but overlapping disciplines. Information Governance is about the way in which the CCG handles its information, particularly personal data. The CCG relies on good quality information being available at the point of need in order to provide a high-quality service. Staff rely on the quality of data they use to make decisions about patient care and treatment, and the way in which we use resources and run CCG business. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe.

The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The CCG also recognises the need to share information with other health organisations and other agencies in a controlled and legal manner consistent with the interests of the patient and, in some circumstances, the public interest.

The CCG believes that accurate, timely and relevant information is essential to support the delivery of the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the Information Governance Policy:

- Openness and transparency;
- Legal compliance;
- Information security;
- Quality assurance.

Reference to 'information governance' in this document shall also mean reference to the following areas:

- Access to information (Freedom of Information Act 2000 and Subject Access Requests);
- Confidentiality and data protection legislation such as the General Data Protection Regulation and Data Protection Act 2018;
- Information security assurance; Information quality assurance; and Records Management.

4. Legal Compliance

- The CCG regards all identifiable personal information relating to patients as confidential;
- 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 undertake or commission annual assessments and audits of its compliance with legal requirements through the Data Security and Protection Toolkit;
- The CCG will establish and maintain policies to ensure compliance with the Data Protection Act; the Human Rights Act and the Common Law Duty of Confidentiality;
- The CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act and Protection of Children Act)
- The CCG has a comprehensive range of information governance policies **(Appendix C**) supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.

The following Legislation, Standards and Guidelines are applicable to this Policy but not limited to:

- Data Protection Act 2018
- The General Data Protection Regulation May 2018
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 2018)
- Freedom of Information Act 2000
- International Information Security standard: ISO/IEC 27002: 2005
- Caldicott Guidance
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Access to Medical Records Act
- Copyright, Designs and Patents Act 1988 (as amended by the copyright computer programmed regulations 1992)
- Mental Capacity Act 2005
- Health and Social Care Act 2012
- Public Records Act 1958
- Records Management Code of Practice for Health and Social Care 2016
- Electronic Communications Act 2000
- Common Law Duty of Confidentiality
- Communications Act
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Information Security Management: NHS Code of Practice 2007
- Crime and Disorder Act 1998
- Regulations of Investigatory Powers Act 2000 (RIPA)

5. Information Governance Management

The CCG's information governance performance and management are monitored through quarterly reporting to the Information Governance, Business Intelligence and Information Management and Technology (IG, BI and IM&T) Steering Group (the 'Steering Group') with exceptions and assurance reported up to the Integrated Performance and Assurance Committee (IPAC). Individual items of action may be included within the Corporate Directorate Risk Register for regular monitoring. See **Appendix A** - High Level CCG Governance Structure and **Appendix B** – IG, BI and IM&T Steering Group Terms of Reference. *(Note: the CCG is currently operating a Pilot Committee Structure, the IG, BI and IM&T Steering Group previously reported to the Clinical Executive Committee*).

The Steering Group has responsibility for:

- overseeing the implementation of this Policy, the annual Data Security and Protection Toolkit assessment and the annual Information Governance improvement plan;
- Oversight of CCG Cyber and Security development programme and responding to national directives;
- establishing, maintaining, reviewing and approving all Information Governance related policies and procedures to ensure compliance with the requirement of NHS Digital's Data Security and Protection Toolkit. (See **Appendix C** for Key CCG Policies);
- co-ordinating and monitoring the Information Governance Strategy across the organisation;
- Joint and collaborative working with NHS SBS, Egton, STP Digital Enabling Group, Serco Risk Team and the East of England Information Governance Forum membership.

6. Senior Roles and Resources

Senior Roles	
Accountable Officer	Chief Officer
Senior Information Risk Owner	Chief Finance Officer
Information Governance Lead / Data Protection Officer	Corporate Services Manager
Caldicott Guardian	Chief Nurse
Information Technology Security	Senior ICT Service Development Manager
Freedom of Information Lead	CCG Secretary / Associate Director of Corporate Affairs
Data Quality Lead	Associate Director of Business Intelligence
Risk Lead	CCG Secretary / Associate Director of Corporate Affairs

Resources

- Corporate Services Manager (IG Lead)
- Corporate Services Support Manager (IG)
- Senior ICT Service Development Manager
- CCG Secretary (Freedom of Information Lead; Risk and Business Continuity Lead)
- Data Quality Lead (Associate Director of Business Intelligence)
- Serco Risk Services (SLA with the CCG identifies areas where specialist advice and support are provided. Signed Data Processing Agreement in place)
- Information Governance and Legal Manager support provided by Serco
- Information Technology Infrastructure supported by Egton
- Information Technology Security Manager (Egton)
- Registration Authority (Head of RA, NEL CSU)
- NHS Mail (supported by NEL CSU)
- Information Management and Technology budget includes funding for base IT security e.g. device encryption. Additional IT and Cyber Security developments and requests for funding are reported to the IG, BI and IM&T Steering Group

7. Data Security and Protection Toolkit

The annual information governance assessment is measured via an assessment process of compliance against the standards set out in the NHS Data Security and Protection Toolkit (DSPT) and assured by Internal Audit.

The CCG is required to publish its assessment to NHS Digital by the 31st March each year with the objective of meeting a compliant ‘Standards Met’ toolkit. Assessment results are shared with the Care Quality Commission; NHS England; NHS Improvement and the National Information Governance Board and also available to the general public on the DSPT website.

The outcome of the CCG's annual Data Security and Protection Toolkit Assessment is reported to the IG, BI and IM&T Steering Group and to the Integrated Performance and Assurance Committee (IPAC). See **Appendix A** for High Level CCG Governance Structure. *(Note: the CCG is currently operating a Pilot Committee Structure, the IG, BI and IM&T Steering Group previously reported to the Clinical Executive Committee*).

National Data Security Standards

The DSPT has been developed in accordance with the National Data Security Standards following a review of data security, consent and opt outs by the National Data Guardian (NDG). The NDG recommended that the following 10 Data Security Standards are applied in the health and social care system in England:

PEOPLE: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	
Data Security Standard 1 **Personal Confidential Data** (Assertions 1-8 apply)	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
Data Security Standard 2 **Staff Responsibilities** (Assertions 9-11 apply)	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3 **Training** (Assertions 12-16 apply)	All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit (or provide similar via inhouse training programmes).

PROCESS: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses**.**	
Data Security Standard 4 **Managing Data Access** (Assertions 17-19 apply)	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5 **Process Reviews** (Assertions 20-22 apply)	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6 **Responding to Incidents** (Assertions 23-26 apply)	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7 **Continuity Planning** (Assertions 27-28 apply)	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
TECHNOLOGY: Ensure technology is secure and up-to-date.	
Data Security Standard 8 **Unsupported Systems** (Assertions 29-31 apply)	No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9 **IT Protection** (Assertions 32-35 apply)	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10 **Accountable Suppliers** (Assertions 36-38 apply)	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Data Security and Protection Toolkit Assertions

To enable the CCG to publish a compliant 'Standards Met' Toolkit, it must respond to and evidence the following 38 mandatory Assertions:

Data Security and Protection Toolkit Assertions	
1	There is senior ownership of data security and protection within the organisation.
2	There are clear data security and protection policies in place, and these are understood by staff and available to the public.
3	Individuals' rights are respected and supported (GDPR Article 12-22).

Data Security and Protection Toolkit Assertions (cont)	
4	Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 (Part 4).
5	Personal information is used and shared lawfully.
6	The use of personal information is subject to data protection by design and by default.
7	Effective data quality controls are in place.
8	Personal information processed by the organisation is adequate (and not excessive) for the purposes.
9	There is a clear understanding of what Personal Confidential Information is held.
10	Personal Confidential Information is processed / shared legally and securely.
11	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.
12	There has been an assessment of data security and protection training needs across the organisation.
13	Staff receive suitable data security and protection training.
14	Staff pass the data security and protection mandatory test.
15	Staff with specialist roles receive data security and protection training suitable to their role.
16	Leaders and board members receive suitable data protection and security training.
17	The organisation maintains a current record of staff and their roles.
18	Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.
19	All staff understand that their activities on IT systems will be monitored and recorded for security purposes.
20	Process reviews are held at least once per year.
21	Participation in reviews is comprehensive, and clinicians are actively involved.
22	Action is taken to address problem processes as a result of feedback at meetings or in year.
23	A confidential system for reporting security breaches and near misses is in place and actively used.
24	Users know how to spot an incident and where to report it, and incidents are effectively reported.
25	All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.
26	Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.
27	There is a continuity plan in place for data security incidents, and staff understand how to put this into action.
28	There is an effective annual test of the continuity plan for data security incidents.
29	All software has been surveyed to understand if it is supported and up to date.

Data Security and Protection Toolkit Assertions (cont)	
30	Unsupported software is categorised and documented, and data security risks are identified and managed.
31	Supported systems are kept up-to-date with the latest security patches.
32	All networking components have had their default passwords changed.
33	Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities.
34	All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them.
35	A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.
36	The organisation can name its suppliers, the products and services they deliver and the contract durations.
37	Basic due diligence has been undertaken against each supplier according to ICO (Information Commissioner's Office) and NHS Digital guidance.
38	All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.

8. Information Governance Training

Fundamental to the success of delivering the Information Governance Policy and Management Framework is developing an Information Governance culture within the CCG. To promote this culture, awareness and training must be provided to all CCG staff (including staff on temporary contracts; secondments; agency workers and students) who utilise information in their day-to-day work.

All CCG staff complete NHS Digital's Data Security Awareness Level 1 training annually on the e-Learning for Healthcare portal. The training includes Caldicott and confidentiality, data protection, information security and freedom of information. Data Security Awareness training is incorporated into the CCG's schedule of mandatory training and new starters are required to undertake the training on their first day in post as set out in the CCG's Orientation and Induction Programme. Data Security training compliance is monitored by the CCG's Learning and Development Team with support from the Information Governance Team where required.

Training Needs Analysis

Staff holding specialist roles e.g. Senior Information Risk Owner (SIRO); Caldicott Guardian; Data Protection Officer; roles involve handling Personal Confidential Information; Information Asset Owners; Information Asset Administrators etc receive additional training commensurate with their role.

The frequency of any further information governance training will be determined as part of the CCG's organisation development plan and appraisal process.

9. The Fundamental Standards

The Care Quality Commission (CQC) inspects and assesses provider organisations against the fundamental standards using five key questions:

- are they safe;
- are they effective;
- are they caring;
- are they responsive to people's needs;
- are they well led.

The CQC cross-checks CCG commissioned services against their Data Security and Protection Toolkit submissions as part of assurance that the CCG is meeting the fundamental standards.

The CCG must have effective governance and systems to check on the quality and safety of care. These must facilitate service improvement and reduce any risks to patient's health, safety and welfare. For example, the standards require the CCG to ensure that medical records are accurate, fit for purpose, held securely and remain confidential.

10. Confidentiality of Personal Data

The Data Protection Act 2018 introduced additional levels of security around the processing of personal data. The CCG, as the legal person and Data Controller for the purposes of the Data Protection legislation must ensure the **confidentiality** (information is accessible only to those who have a proven need to see it); **Integrity** (information held is accurate and up-to-date) and **availability** (information is there when it is needed to support care) of the personal data that we use.

The CCG will ensure that all personal data it holds is controlled and managed in accordance with the terms of current data protection legislation principles, the Department of Health Confidentiality: NHS Code of Practice, European Convention of Human Rights (Article 8) (Human Rights Act 1998), Health and Social Care Act 2015 and common law as set out in the CCG's Data Protection Policy; Records Management and Lifecycle Policy; Access to Records Policy. (See **Appendix C** for Key CCG Policies).

11. Confidentiality Code of Conduct

All staff, whether permanent, temporary; contracted or voluntary who have been provided with privileged access to personal, confidential and or sensitive information are responsible for ensuring that it is always handled in confidence. Staff must be aware of their individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. Failure to maintain confidentiality may lead to disciplinary action, including dismissal.

12. Openness and Transparency

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information is defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act. Non-confidential information on the CCG and services are available to the public through a variety of means, in line with the CCG's code of openness and in compliance with the Freedom of Information Act, Freedom of Information Policy, Code of Conduct for Confidentiality, Data Protection Act and Access to Records Policy.

Patients have access to information relating to their own health care, options for treatment and their rights as patients. There are clear procedures and arrangements in place for handling queries from patients and the public.

The CCG has clear procedures and arrangements in place for liaison with the press and broadcasting media. **See Appendix C** for associated policies.

Integrity of information is developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

Availability of information for operational purposes is maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory framework will be achieved, monitored and maintained.

The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The CCG establishes and maintains policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act.

Information Governance training including awareness and understanding of legal and statutory requirements including Caldicott principles and confidentiality, information security and data protection, is mandatory for all staff on an annual basis. Information governance is included in induction training for all new staff. The necessity and frequency of any further training is assessed at appraisal and determined as part of the CCG's organisational development plan.

13. Privacy and Fair Processing Notice

As data controllers, the CCG is required to provide certain information to people whose information (personal data) is held and used. The CCG does this by providing information to its staff via the Extranet and to the public via the CCG's Privacy and Fair Processing Notice on the CCG website. The privacy notice identifies who the CCG is, what they do and provides contact details for the CCG's Data Protection Officer. The CCG must also explain the purposes for which personal data are collected; used; disclosed; how long it is kept and the legal basis for processing.

The CCG is committed in ensuring that individuals are adequately informed about confidentiality and their rights as data subjects, in particular how they may contact the CCG about or to access their personal data.

14. Information Risk

See **Appendix D** for Key Responsibilities for Information Risk Roles.

The CCG establishes clear lines of accountability for information risk management that lead directly to the Governing Body through the SIRO, DPO and the appointment of Information Asset Owners' (IAO) and Information Asset Administrators who are collectively responsible for the maintenance of a CCG wide Information Asset Register.

The IAOs and SIRO are accountable to the Accountable Officer, the Chief Officer for the management and mitigation of information risks and provide assurance to that effect for the Annual Report which includes the Annual Governance Statement and Statement of Internal Control.

The IAO ensures that information risk assessments are performed at least once each quarter on all information assets where they have been assigned 'ownership'. They ensure that any significant risks are included in a quarterly assessment to the CCG's SIRO.

Each Directorate is responsible for developing and maintaining a Directorate Risk Register which links into the CCG's Assurance Framework (CAF) and Risk Register. In line with the CCG's Risk Management Policy, the CAF and Directorate risk registers are used to identify, manage and prioritise CCG risks.

Directorates must nominate a Risk Co-ordinator; the nominee is required to have an awareness of the CCG's Datix Incident Reporting System and the ability to familiarise themselves with the management of risks;

At least once a year, each of the CCG's IAOs carry out a risk assessment to examine forthcoming potential changes in services, technology and threats and provide assurances to the CCG's SIRO on the security and use of assets they 'own'. All high risks should be escalated to the Governing Body via the CCG Assurance Framework and Risk Register.

15. Information Security

The CCG protects personal data held in its information systems through compliance with the Department of Health Information Security Code of Practice an associated standard of ISO/IEC 27002:2005.

The CCG ensures that personal data is protected by encryption in accordance with Department of Health directives. Please refer to the CCG's Information Security for Staff Policy. (See **Appendix C** for Key CCG Policies).

- The CCG establishes and maintains policies for the effective and secure management of its information assets and resources;

- The CCG undertakes or commissions annual assessments and audits of its information and IT security arrangements through the Data Security and Protection Toolkit framework;
- The CCG promotes effective confidentiality and security practice to its staff through policies, procedures and training;
- The CCG establishes and maintains incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of confidentiality and security;
- All planned major information systems within the Organisation are assessed via the Data Protection Impact Assessment process before these systems become live to ensure appropriate levels of privacy and security are in place prior to launch.

16. The Health and Social Care Network (HSCN) Connection Agreement

All organisations wishing to access and use NHS systems and services, including the HSCN network, must meet the terms and conditions in the HSCN Connection Agreement.

The Connection Agreement replaces the N3 Information Governance Statement of Compliance (IGSoC). In doing this, the arrangements for being able to use HSCN are separated from those relating to accessing data or systems available on HSCN.

The HSCN Connection Agreement sets out the things HSCN customers must do before and whilst using HSCN:

- HSCN customers acknowledge responsibility for securing information. Practically, this means that patient data should always be encrypted when being sent across any network, including the HSCN;
- The right of audit by NHS Digital or nominated third parties;
- Change Control Notification procedures and approval processes;
- Organisations to achieve or be working towards ISO27001;
- Organisations to report security events and incidents.

17. Incident Management

The CCG's SIRO and Caldicott Guardian via the relevant IAO must be informed immediately of all information security incidents involving the unauthorised disclosure of patient information for consideration of any necessary actions.

The Datix System is used for reporting, investigation and management of Information Governance and Information Security incidents and near misses. All information incidents reported on Datix will be reviewed by the IG Lead in accordance with NHS Digital's Incident Reporting Guidance to identify SI levels and reporting procedures. Relevant leads are identified for management and review of IG related incidents. Shared learning from incidents is disseminated via all staff email or staff bulletin as appropriate.

A key function of the Steering Group is to monitor and review untoward occurrences and incidents relating to Information Governance and to ensure that effective remedial and preventative action is taken. Reports of such incidents will be distributed to the Steering

Group for consideration. Information incident reporting will be in line with the overall incident reporting processes as outlined in the CCG's Serious Incident Guidelines.

18. Data Protection Impact Assessments (DPIAs)

The impact of any proposed changes to the CCG's processes and / or information assets need to be assessed in accordance with the CCG's Data Protection Impact Assessment Policy and Procedure, to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset so that they can decide if a DPIA is required for a project or planned service change.

19. Information Asset Register

All assets must be clearly identified on the CCG's Information Asset Register.

It is the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in their Directorate's Information Asset Register which forms part of a CCG wide Register owned by the CCG's SIRO.

The Information Asset Register should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The register should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified as should details of risk assessor, risk assessment frequency, risk assessment rating and date of last risk assessment.

There are many types of assets, including:

- **information:** databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- **software assets**: application software, system software, development tools, and utilities;
- **physical assets**: computer equipment, communications equipment, removable media, and other equipment;
- **services:** computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- **people** and their qualifications, skills, and experience;
- **intangibles** such as reputation and image of the organisation.

All information and assets associated with information processing facilities should be owned by a designated part of the organisation, for example a CCG Directorate. **Priority**

must be given to information assets that comprise or contain personal information about patients or staff.

The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies.

Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis (i.e. an Information Asset Administrator (IAA)), but the responsibility remains with the owner.

In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case, the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

20. Freedom of Information

The CCG uses all appropriate and necessary means to ensure that it complies with the Freedom of Information Act 2000 and associated Codes of Practice issued by the Lord Chancellor's Department pursuant to sections 45(5) and 46(6) of the Act. This is set out in the CCG's Freedom of Information Policy. (**Appendix C** - Key CCG Policies).

21. Records Management

The CCG is committed to a systematic and planned approach to the Management of records within the organisation, from their creation to their ultimate disposal. The CCG ensures that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of the information efficiently when it is no longer required. The CCG will ensure that Health Records are managed in accordance with the Department of Health's Records Management: NHS Code of Practice for Health and Social Care 2016. This is set out in the CCG's Records Management and Lifecycle Policy. (See **Appendix C** for Key CCG Policies).

22. Information Quality Assurance

The quality of information acquired and used within the CCG is a key component to its effective use and management. As such, managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

The CCG:

- promotes data quality through the use of policies and procedures including the Records Management and Lifecycle Policy and Data Quality Policy and associated statutory professional requirements;
- undertakes or commissions annual assessments and audits of its arrangements in line with the Data Security and Protection Toolkit requirements;

- ensures that, wherever possible, information quality is assured at the point of collection;
- ensures that data standards are set through clear and consistent definition of data items in accordance with national standards.

23. Review of Contracts and Third-Party Contracts

The SIRO and IAOs must take all reasonable steps to ensure that contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

It is not unusual to have third parties gaining access to the CCG's information assets, e.g. computers, telephones, paper records etc. The third parties include temporary agency staff, consultants, IT support staff etc. It is possible that as a result of access to information assets, third party staff may have access to patient or staff personal data. This situation therefore clearly has information governance risk implications such as data being used inappropriately.

Suitable clauses are included when negotiating and completing contracts with third parties who have access to or process personal information on behalf of the CCG. All contractors or support organisations with access to the CCG's information assets are clearly identified and appropriate information governance clauses included in their contracts. The terms and conditions of a contract ensure that failure to deliver any aspect of information governance assurances will be at the third party's risk.

Attention must also be paid to the possible use of sub-contractors by the third party to provide services in order to undertake the contract.

A register of all contracts including third party contracts is maintained by the CCG.

24. Contractual Risk Assessments

Directorates and IAOs should ensure that a risk assessment has been carried out prior to any agreement being made with a third party to evaluate any potential threats to information; networks; systems and locations from third party operatives.

The ways in which third parties gain access, will help determine how extensive the risk assessment needs to be. For example, a risk assessment for cleaning contractors will be different to that carried out for a contractor connecting to the network. Temporary access will also see different considerations to long-term access.

25. Consent to share information

The GDPR requires that organisations (data controllers) that process personal data demonstrate compliance with its provisions. Part of this involves establishing and publishing a basis for lawful processing, and where relevant, a condition for processing special category data.

Consent is one of several options to meet each of these requirements under the GDPR. There are a variety of consent practices for the use and disclosure of information in health and social care, from 'implied consent', often assumed as the basis for processing for direct care purposes to explicit consent where it is obtained for research purposes. These remain valid for common law requirements and are integral to health and social care practices. However, some consent practices do not necessarily meet the requirements of the GDPR and even where they do, consent may not be the preferred legal basis for the processing of personal data for GDPR purposes.

There are exceptions where it is believed that the reasons for disclosure are so important (sometimes termed a public interest justification or defence) that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed).

26. Information Sharing Agreements

Sharing information about an individual between partner agencies is vital to the provision of co-ordinated and seamless services. The need for shared information standards and robust information security to support the implementation of joint working arrangements is recognised.

Information sharing protocols can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing the person whose information it is about the possibility of sharing and the choices they have to limit sharing. If the individual dissents to sharing, then confidential information may only be shared in exceptional circumstances.

Routine information sharing continues to require information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. Information sharing protocols are not required where the sharing is for an ad hoc request for information.

27. Transfers of Personal Information outside the UK

The Data Protection Act governs transfers of personal information and requires that personal information is not transferred to countries outside of the European Economic Area (EEA) unless that country has an adequate level of protection for the information and for the rights of individuals. The EEA is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway.

All transfers of personal data outside the EEA must be for a lawful and justified purpose and the CCG's Caldicott Guardian must be informed of such transfers. A log of such transfers must be maintained.

Personal Information should only be transferred outside the EEA if the individual's consent, which should be explicit, has been obtained or following a risk assessment the Caldicott Guardian is satisfied that there is an adequate level of protection in place. In

certain circumstances a contract containing standard EU approved clauses as providing adequate protection to transfer individuals' personal information may be necessary.

28. Monitoring/Audit

- The CCG will monitor this policy and related strategies, policies and guidance through the Steering Group;
- As assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT) will be undertaken each year;
- The Steering Group will ensure implementation of the Data Security and Protection Toolkit (DSPT) Improvement Plan;
- An IG Annual report which will include a strategic plan for each work strand will be presented to the CCG's Integrated Performance and Assurance Committee;
- Internal Audit annual review is expected;
- The CCG will ensure that the support infrastructure for the SIRO and Caldicott Guardian is in place and kept under regular review.

Annex A - Equality Impact Assessment Form

Name of Proposal (policy/strategy/function/ service being assessed)	CCG IG Policy and Management Framework v1.0
Those involved in assessment:	Policy developed in consultation with the IG, BI & IM&T Steering Group and for endorsement by the Integrated Performance and Assurance Committee
Is this a new proposal?	CCG IG Management Framework document has been incorporated into the CCG IG Policy that was already in place.
Date of Initial Screening:	11 April 2017 (IG Policy), updated 23 May 2019

What are the aims, objectives?	This Policy will provide assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care for our population.
Who will benefit?	All staff working for and on behalf of the CCG
Who are the main stakeholders?	Staff; Managers; IG, BI, IM&T Steering Group
What are the desired outcomes?	Staff awarenenss of the Policy through being advised of its availability on the CCG's website via iConnect.
What factors could detract from the desired outcomes?	• Lack of awareness of the existence of the Policy; • Failure to follow the Policy/procedure.
What factors could contribute to the desired outcomes?	Knowledge of the policy and implementation
Who is responsible?	Staff, managers, IG, BI, IM&T Steering Group
Have you consulted on the proposal? If so with whom? If not, why not?	Policy developed in consultation with the IG, BI & IM&T Steering Group for approval and endorsement by the Integrated Performance and Assurance Committee.

Which protected characteristics could be affected and be disadvantaged by this proposal *(Please tick)*		**Yes**	**No**
Age	Consider: Elderly, or young people		x
Disability	Consider: Physical, visual, aural impairment; Mental or learning difficulties		x
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned		x
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		x
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related matter		x
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		x
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		x
Sex /Gender	Consider: Male and Female		x
Sexual Orientation	Consider: Known or perceived orientation		x

What information and evidence do you have about the groups that you have selected above?

The above protected characteristics will have no adverse impact as the Policy has been developed in accordance with new Data Protection legislation (ie General Data Protection Regulation May 2018).

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People

Examples of impact are given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how services may be accessed by lesbian, gay, bi-sexual and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

Please list the positive and negative impacts you have identified in the summary table on the following page.

Summary	
Positive impacts (note the groups affected) N/A	Negative impacts (note the groups affected) N/A

Summarise the negative impacts for each group:

N/A

What consultation has taken place or is planned with each of the identified groups?

Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group prior to endorsement by the Integrated Performance and Assurance Committee.

What was the outcome of the consultation undertaken?

Approval, and Endorsement sought.

What changes or actions do you propose to make or take as a result of research and/or consultation?

Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided. The Information Governance Team on behalf of the Associate Director of Corporate Affairs will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

Will the planned changes to the proposal:

	Please State Yes or No
Lower the negative impact?	N/A
Ensure that the negative impact is legal under anti-discriminatory law?	N/A
Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	N/A

Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits.

Information risk - The CCG must respect patient confidentiality in accordance with the NHS Constitution, ICO Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of PCD.

What monitoring/evaluation/review systems have been put in place?

Monitoring will be undertaken by the Information Governance team. The frequency of review will be every other year or as required.

When will it be reviewed?

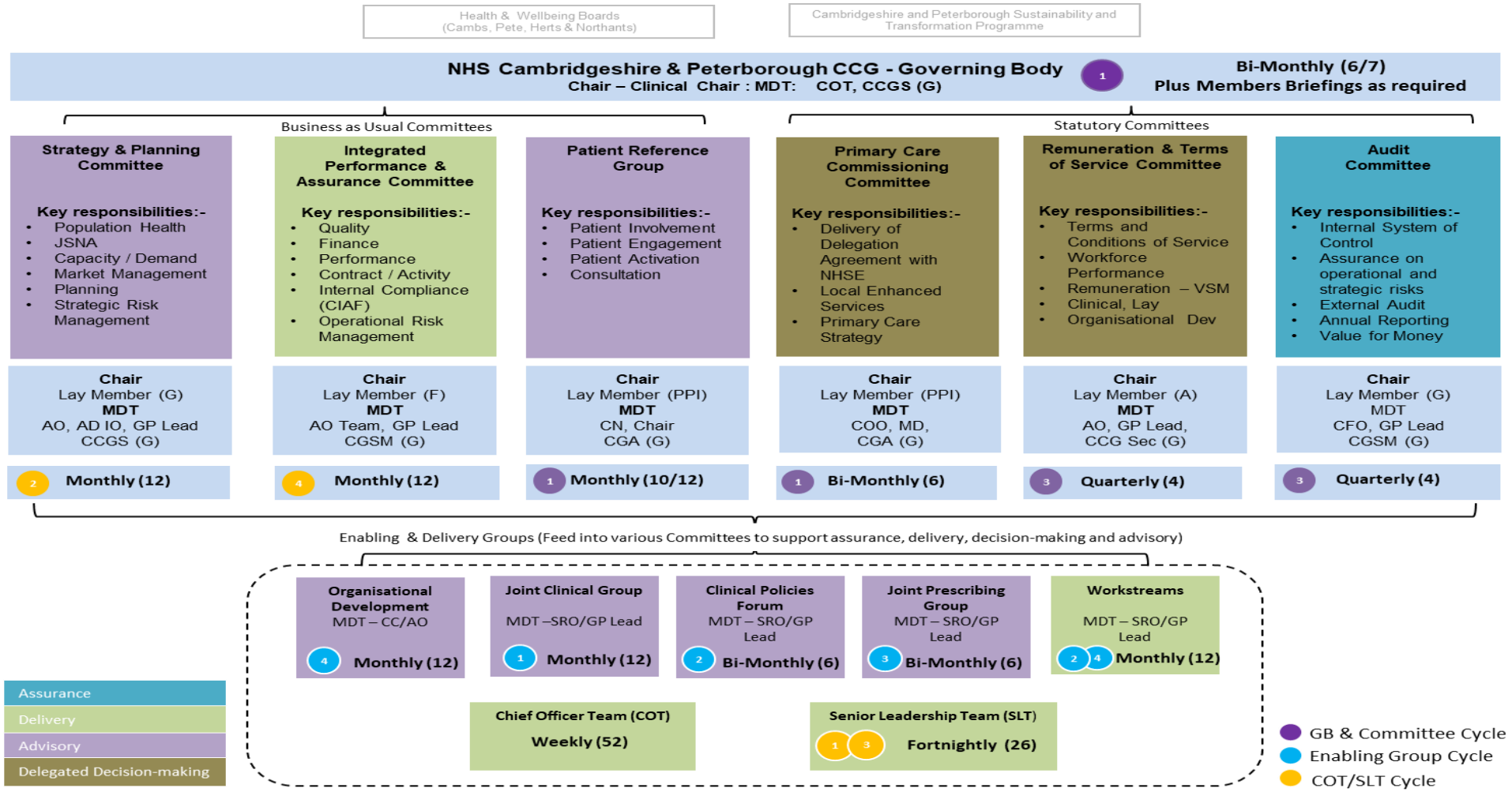
May 2021

Date completed:	23 May 2019
Signature:	Corporate Services Support Manager (IG)
Approved by:	OD & HR Advisor, Equality and Diversity
Date approved:	27 June 2019

Appendix A – CCG Pilot Committee Structure

CCG Governance Framework to support Pilot Committee Structure is available **here**

Source: Constitution– Version 11 - Ratified by NHSE 29.03.19



Appendix B - IG, BI and IM&T Steering Group Terms of Reference

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Information Governance (IG), Business Intelligence (BI) and Information Management & Technology (IM&T) Steering Group Terms of Reference

1. PURPOSE

- The key strategic aim is to ensure that IG, BI and IM&T is at the heart of the Clinical Commissioning Group (CCG) and to promote and ensure that all business and commissioned services and systems are compliant with national standards, legislation and statutory duties;
- To act as the project board for selected CCG IG, BI and IM&T projects and to agree IM&T investments in line with national, area and local priorities;
- To set the IG, BI and IM&T Strategies and related policies and procedures, providing assurance to the Governing Body;
- Group members are to ensure that wider CCG strategic goals are reflected in the work of the Group and Organisation;
- To provide leadership around the opportunities for using technology and information to shape and improve the health and wellbeing of the local heath economy.

2. MEMBERSHIP

The core membership of the Steering Group is set out below:

Chief Finance Officer (Chair of the Group and SIRO)
Associate Director of Corporate Affairs and CCG Secretary (Deputy Chair; Corporate Governance; FOI Lead and Deputy SIRO)
Chief Nurse (Caldicott Guardian)
Deputy Chief Nurse (Deputy Caldicott Guardian)
Corporate Services Manager (Data Protection Officer, Privacy Officer and Information Governance Lead)
Corporate Services Support Manager (Information Governance SME)
Associate Director of Business Intelligence (Data Quality Lead)
Senior Information Manager
Senior ICT Service Development Manager
Strategic Clinical Services IM&T Consultant
Primary Care IT Manager
Contracts and Procurement Specialist
Head of Project Management Office

The Steering Group can invite people whose attendance is relevant to matters to be discussed. All other attendance will be at specific invitation of the Group, including attendance as an observer.

The principle of arranging a 'deputy' to attend the Steering Group meetings on behalf of members who are unable to attend will apply. Attendance will be monitored and reported annually.

3. QUORUM

A quorum shall be the Chair (or nominated deputy) and the SIRO (or their deputy) and the Caldicott Guardian (or their deputy). If these members are not available, then the meeting can take place, but decisions must be deferred. For matters that cannot wait until the next scheduled meeting, virtual decision making is permitted.

4. OBJECTIVES

4.1 CCG Business

- To ensure consistent and high standards of record keeping and information handling, in accordance with statutory and legal requirements;
- To interpret, monitor and review progress for the Data Security and Protection Toolkit (DSPT) self-assessment on behalf of the CCG, ensuring any concerns are highlighted and addressed;
- To review, monitor and action relevant internal audits;
- To review and approve Information Sharing Agreements and Data Protection Impact Assessments (DPIAs);
- To manage the reporting and investigation of breaches of confidentiality and security; cyber security and any other IG and IT related incidents. Where necessary, undertake or recommend remedial action and cascade learning from these events where appropriate to mitigate recurrence;
- To review and triangulate the risks identified that relate to information governance; IM&T; business intelligence and cyber security. Escalate where necessary to the CCG Assurance Framework (CAF) and Risk Register;
- To monitor the IG training programme uptake, ensuring that mandatory IG training is completed, and an agreed plan is in place to address escalation of non-compliance as required;
- To provide support, advice and guidance to the organisation's Accountable Officer, Caldicott Guardian and Senior Information Risk Owner (SIRO);
- To maintain an assurance management framework for Information Governance across the CCG;
- To receive minutes or reports from any relevant groups led by CCG members, and any items of interest from local or national forums;
- To ensure consistent and high standards of Business Intelligence are in place across the CCG to support work programmes;
- To monitor and review progress and change with DSCRO and DARs related issues;

- To support the CCG's objectives in the delivery of high-quality patient care ensuring appropriate records management; data quality; data confidentiality, integrity, and availability; information sharing, and security measures are in place;
- To develop and advise CCG teams of best practice in relation to information governance;
- To promote and raise awareness of appropriate multi-agency information sharing in support of integrated care, to both patients and staff;
- To maintain strong working relationships with existing partner organisations and develop same with new organisations to promote multi-agency integrated care;
- To provide oversight to various Groups whose business relates to IG, BI and IM&T;
- To ensure that the organisation's approach to information handling is communicated to all staff and where appropriate made available to the public.
- To work with NHS Digital and NHS England & NHS Improvement in the development of systems and process to support the provision of data to Clinical Commissioning Groups and ensure the views of those organisations are represented.
- To find and evaluate new information technologies to support the delivery of Business Intelligence to the CCG.

5. POLICY REVIEW

The Steering Group has delegated responsibility for the approval of IG, BI and IM&T policies and procedures. Approval of new policies and procedures will, where possible, take place at meetings; alternatively, virtual approval will be sought with 'sign off' at the next meeting. For minor revisions to an existing policy/procedure, the front page of the document only will be circulated for approval showing the version control with the amendments clearly documented. Endorsement by the Integrated Performance and Assurance Committee (IPAC) will be sought through an exception report after each meeting for onward reporting to the Governing Body requesting ratification.

6. MEETING FREQUENCY, STRUCTURE AND ADMINISTRATION

Meetings of the Steering Group will be held quarterly. The Chair of the meeting may request additional meetings as necessary. The Steering Group shall be supported administratively by the Corporate Services Team whose duties in this respect will include:

- Agreement of the agenda and circulation of papers;
- Taking the Minutes;
- Keeping a record of matters arising and action log to be carried forward;
- Prompting members to complete actions.

7. REPORTING ARRANGEMENTS

The IG, BI and IM&T Steering Group will advise and assure the Governing Body of key issues through regular exception reporting to the Integrated Performance and Assurance Committee. Annual reports will be prepared for the Governing Body. Highlight reports for specific issues will be prepared as required.

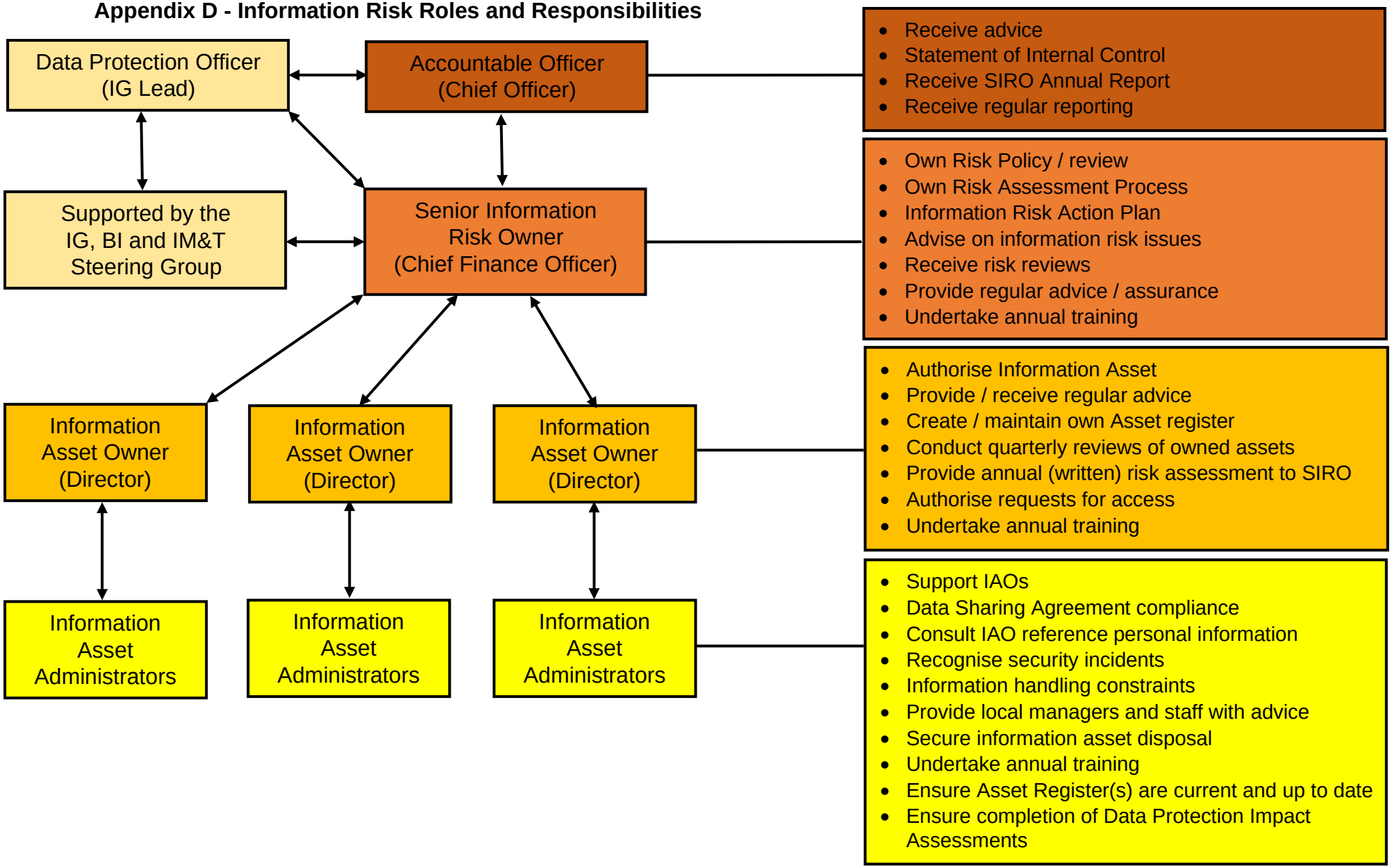
Author: Amanda Holloway, IG Lead and Data Protection Officer

Approved by:	**Endorsed by:**
IG, BI and IM&T Steering Group	Integrated Performance and Assurance Committee
Date: 3rd May 2019	Date: 28th May 2019
Next Review Date: **April** 2020 - The Terms of Reference will be reviewed on an annual basis or before if required.	

Appendix C - Key CCG Policies

Policy	Date Ratified	Review Date
Access to Records Policy	May 2019	April 2021
Cambridgeshire Information Sharing Framework	July 2019	July 2020
Code of Conduct for Staff in Respect of Confidentiality	August 2019	July 2021
Controlled Environment for Finance (CEfF) Policy	August 2019	July 2021
Data Protection Impact Assessment Policy and Process Guidance	May 2019	May 2021
Data Protection Policy	July 2018	April 2020
Data Quality Policy	May 2019	May 2021
Freedom of Information Act Policy & Publication Scheme Policy	February 2018	February 2020
Information Governance Forensic Readiness Policy	May 2019	April 2021
Information Governance Policy and Management Framework	August 2019	July 2021
Information Governance Strategy	August 2019	July 2021
Information Security for Staff Policy	October 2018	August 2020
Records Management and Lifecycle Policy	October 2018	September 2020
Registration Authority Policy and Procedure (NEL CSU)	October 2016	October 2018
Removable Media Policy	August 2017	August 2019
Risk Management Policy	May 2019	May 2021
Safe Haven Policy	August 2017	August 2019
All Information Governance Policies are available to staff and the public on the CCG's website **here**. Staff are notified of all new policies or revisions through publication of articles in the weekly staff bulletin (iConnect).		

Appendix D - Information Risk Roles and Responsibilities



Appendix C (Cont) – Information Risk Roles and Responsibilities

The Chief Officer

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

The Senior Information Risk Owner (SIRO)

The Chief Finance Officer at the CCG is the SIRO with overall responsibility for managing information risk across the organisation and is the owner of the CCG's Information Asset Register. The SIRO is a member of the Governing Body and provides written advice to the Accountable Officer on the content of the Annual Governance Statement and the Statement of Internal Control in regard to information risk.

The SIRO is responsible to the Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this Framework.

The SIRO owns the CCG's overall information risk assessment process, tests its outcome, and ensures it is used. The SIRO is responsible for how the organisation implements NHS Information Governance risk management in its own services and activities and those of its delivery partners, and how compliance is monitored. The SIRO ensures that quarterly information asset risk reviews are completed. Based on the information risk assessment the SIRO evaluates the information risks to the organisation and its business partners through its delivery chain, and ensures that they are addressed, and that they inform investment decisions including the risk considerations of outsourcing.

The SIRO is supported by Information Asset Owners, the CCG's Caldicott Guardian and members of the IG, BI and IM&T Steering Group, although ownership of Information Risk and the information risk assessment process remains with the SIRO.

Key Responsibilities of the Senior Information Risk Owner (SIRO)

- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework;
- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control;
- To review and agree an action plan in respect of identified information risks;
- To ensure that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- To provide a focal point for the resolution and/or discussion of information risk issues;
- To ensure the Board is adequately briefed on information risk issues;
- To advise the Chief Officer and the Board on information risk management strategies and provide periodic reports and briefings on progress.

Caldicott Guardian

The Chief Nurse is the CCG's Caldicott Guardian and the 'conscience' of the organisation, providing a focal point for patient confidentiality and information sharing issues and advising on the options for lawful and ethical processing of information as required.

Key responsibilities of the Caldicott Guardian

- Strategy and Governance: The Caldicott Guardian champions confidentiality issues at Governing Body/executive management team level and sits on an organisation's Information Governance Committee/Group and acts as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.
- Confidentiality and Data Protection expertise: The Caldicott Guardian develops a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott and information governance functions, but also on external sources of advice and guidance where available.
- Internal information processing: The Caldicott Guardian ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key aspects that need to be addressed by the organisation's Caldicott function were detailed in the Information Governance Toolkit up to March 2018 and these remain embedded as good practice.
- Information sharing: The Caldicott Guardian oversees all arrangements, protocols and procedures where confidential personal information is shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.
- Caldicott Training: is required to be undertaken every other year.

Data Protection Officer (DPO)

The Data Protection Officer provides the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the Principles and Data Subject Rights laid down in the General Data Protection Regulation (GDPR).

Key responsibilities of the Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for monitoring compliance with data protection law and ensuring data practices internally comply with applicable requirements. The DPO is also responsible for staff training, data protection impact assessments and internal audits, and serves as the primary contact for supervisory authorities and individuals whose data is processed by the organisation. The DPO reports to the Caldicott Guardian on relevant matters and escalate any serious concerns or issues to the Board of Directors.

The DPO is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR. The organisation must appoint a DPO whose job description is compliant with GDPR requirements and in particular must ensure:

- that the DPO role directly reports to the highest management level of the organisation – this does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team;
- that the DPO role is provided with adequate resources: financial and human resources, and is supported in maintaining his or her expertise;
- that the DPO has proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the GDPR, and sufficient understanding of the organisation's business and processing;
- that information governance and related policies address organisational accountability;
- DPO reporting arrangements;
- timely involvement of the DPO in all data protection issues;
- compliance assurance: privacy by design and default advising on where data protection impact assessment is required;
- the DPO's role in incident management;
- that the DPO does not receive any instruction regarding the exercise of his or her tasks, and is protected from disciplinary action, dismissal or other penalties;
- that where the DPO performs another role or roles, that there is no conflict of interest;
- that the contact details of the DPO are published in the CCG's transparency information for subjects and are communicated to the ICO.

Information Asset Owner (IAO)

Information Asset Owners (IAOs) 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'. IAOs also lead and help foster, within their respective Directorates, a culture that values, protects and uses information. IAOs must be a member of staff senior enough to make decisions concerning the asset at the highest level. All the CCG's IAOs are members of the Board involved in running the Organisation. Their role is also to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They ensure that all threats, vulnerabilities and impacts are properly assessed and included in the CCG's Information Asset Register.

The owner can assign day to day responsibility for each information asset to an administrator or manager known as an Information Asset Administrator, which must be formalised in job descriptions.

The SIRO is responsible for the appointment and management (in terms of information assets) of the IAOs.

Key Responsibilities of the IAO

To understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of these assets (understands the CCG's plans to achieve and monitor the right NHS IG culture, across the CCG and with its business partners and to take visible steps to support and participate in that plan (including completing own training).

Working closely with the Data Protection Officer and Information Governance Manager, IAO's will take appropriate actions to:

- Know what information the Asset holds and understands the nature and justification of information flows to and from the asset (approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops is minimised and are effectively protected to NHS IG standards.
- Know who has access and why, and ensure their use is monitored and compliant with policy (checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Conduct Data Protection Impact Assessments for all new projects in line with the CCG's Data Protection Impact Assessment Policy and Procedure.
- Participate in an Annual Information Risk Assessment.
- Understand and address risks to the asset and provide assurance to the SIRO (makes the case where necessary for new investment or action to secure 'owned' assets; provides an annual written risk assessment to the SIRO for all assets 'owned' by them).
- Ensure that information risk assessments are reviewed at least once every quarter on all information assets where they have been assigned 'ownership' and where:
  - New systems, applications, facilities etc. is introduced that may impact the assurance of CCG Information or Information Systems;
  - Before enhancements, upgrades, and conversions associated with critical systems or applications;
  - Ensure that all high risks follow the CCG's process for inclusion on the CCG's Assurance Framework and Risk Register.
- IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks;
- Compile their Information Asset Register.
- Ensure the asset is fully used for the benefit of the organisation and its patients, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required; receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with NHS IG standards of good practice and the policy of the organisation.
- Approve and oversee the disposal mechanisms for information of the asset when no longer needed).

Information Asset Administrator (IAA)

Information Asset Owners (in consultation with the SIRO) are responsible for appointing Information Asset Administrators (IAAs). It is at the IAOs discretion how many IAAs are appointed to support them in their role. Information Asset Administrators are operational staff with day to day responsibility for managing risks to their information assets. They will

support IAOs by ensuring that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, ensure that data protection impact assessments are completed and ensure that information asset registers are accurate and up to date.

Key Responsibilities of the IAA

Information Asset Administrators will provide support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents. They will consult their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.

Ensuring compliance with data sharing agreements within the local area and that information handling procedures are fit for purpose and are properly applied.

Under the direction of their IAO, they will ensure that personal information is not unlawfully exploited, and they will, upon recognising new information handling requirements (e.g. a new type of information arises) that the relevant IAO is consulted over appropriate procedures. They will consult with the IAOs regarding any potential or actual security incidents.

Reporting to the relevant IAO on current state of local information handling and ensure that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO. They will act as first port of call for local managers and staff seeking advice on the handling of information.

Under the direction of their IAO, they will ensure that information is securely destroyed when there is no further requirement for it.