NHS
Lincolnshire
Integrated Care Board

Information Governance Management Framework
(Including Policy and Strategy)

ICB document reference:	**ICB IG 001**
Name of originator/author:	NHS AGEM CSU
Date of approval:	March 2024
Name of responsible Committee:	Executive Committee/Audit & Risk Committee
Responsible Director/ICB Officer:	Julie Ellis-Fenwick, Head of Corporate Governance
Category:	Information Governance
EIA undertaken:	
Date issued:	March 2024
Review date:	March 2027
Target audience:	All staff
Distributed via:	Email, Website, Intranet and Board Portal

Document Control Sheet

Document Title	Information Governance Management Framework (Including Policy and Strategy)
Version	0.7
Status	DRAFT
Authors	NHS AGEM CSU
Date	07/02/2024

Document history			
Version	**Date**	**Author**	**Comments**
0.1	27/10/20	NHS AGEM CSU/Optum Health Systems Support IG Services	Updated document based on predecessor Lincolnshire CCG documentation & taking account of the Data Protection Act 2018.
0.2	01/12/20	NHS AGEM CSU/Optum Health Systems Support IG Services	Updated to reflect role of SIRO & Lincolnshire Commissioning Support Forum in policy approval process
0.3	21/12/20	NHS AGEM CSU/Optum Health Systems Support IG Services	Updated to reflect governance/approval arrangements
0.4	26/01/21	NHS AGEM CSU/Optum Health Systems Support IG Services	IGAF Appendix 1 added and minor word changes
0.5	05/02/21	NHS AGEM CSU	Minor changes and addition of Appendix 1
0.6	24/06/2022	NHS AGEM CSU	Policy review and rebrand for the transition of the CCG to an ICB
0.7	07/02/2024	NHS AGEM CSU	Minor wording changes, reference updates, Addition of the Deputy SIRO role and ICB IG lead updated.

CONTENTS

Definitions that apply to this Policy

Legal	Established by law
Ethical	Conforming to accepted standards of conduct, in this case respecting the privacy and dignity of the patient and obtaining their consent
Asset Owners	Those responsible for the information assets used within the service
Asset Administrators	Those given delegated authority to safeguard the use and security of the information assets
Statement of Internal Control	The mechanism for providing assurance in relation to appropriately managing and controlling resources
Forensic readiness	Ability to collect credible digital evidence and estimating the cost of an incident response
Data Protection Impact Assessment	Assessing the extent to which activities intrude on privacy
Due Regard	Having **due regard** for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life • Or in other activities where their participation is disproportionately low.

1.0 Summary of Policy

Information plays a key part in the clinical and corporate governance of NHS Lincolnshire ICB (referred to from here as “the organisation”) and the quality of the commissioning of patient services, planning, performance management, assurance, and financial management relies upon accurate and available information.

The Information Governance Assurance Framework (IGAF) is the national framework of standards that brings together all statutory, mandatory, and best practice requirements concerning information management. The standards are set out in the Data Security and Protection Toolkit (DSPT) as a roadmap enabling organisations to plan and implement standards of best practice and to measure and report compliance on an annual basis.

Performance against these standards is mandated by and reported to NHS England and the Care Quality Commission (CQC) and forms part of the assurance processes associated with risk management requirements.

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to within DSPT as the organisation’s Information Governance Assurance Framework (IGAF). The IGAF brings together all the requirements, standards and best practice that apply to the processing of personal information to ensure:

- Compliance with the law
- Implementation of Department of Health guidelines
- Planned year on year improvement
- DSPT requirements

This framework sets out the approach the organisation is taking to provide and comply with Information Governance (IG) standards.

This document provides a comprehensive view of the overarching framework for the strategic Information Governance agenda within the organisation.

2.0 Introduction

Information is a vital asset and resource, both in terms of commissioning and the efficient management of services and its support. It plays a key part in healthcare governance, service planning and performance management and improvement. It is of paramount importance to ensure that information is managed legally, ethically, and efficiently; that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management. This policy is

supported by and dependent on ensuring appropriate information is given to members of the public, service users and staff at service interface points to ensure that the ICB's processes are open and transparent.

Information Governance is a framework that brings together all the requirements, standards and best practice, that apply to the handling of personal information.

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embed information risk management into the overall risk management culture of the organisation. Senior Leadership through the appointment of a Senior Information Risk Officer (SIRO) demonstrates the importance of ensuring information security remains high on the ICB's agenda.

3.0 Purpose

To describe a system that ensures the organisation meets its responsibility for the legal and ethical management of information assets and resources and ultimate compliance with the DSPT, NHS and other professional Codes of Conduct relating to confidentiality and consent; and guidance from the Information Commissioner's Office (ICO).

The DSPT is used as a performance measure and the introduction of partnership working and national systems increase the importance of maintaining a suitable management framework to progress the IG agenda. The DSPT is used by the Care Quality Commission (CQC) to determine the quality of the ICB's services.

Information Governance covers **all** staff employed by the organisation including, private contractors, volunteers and temporary staff. The scope is:

- All information recorded, disclosed and used by the organisation
- All information systems managed by the organisation
- Any individual using information '*owned*' by the organisation
- Any individual requiring access to information '*owned*' by the organisation

4.0 Duties within the Organisation

Senior roles within the organisation supporting the Information Governance agenda are held by the organisation's Senior Information Risk Owner (SIRO) (Section 4.4), and the Caldicott Guardian (Section 4.3). They are supported by an IG Team in NHS Arden and Greater East Midlands Commissioning Support Unit (NHS AGEM) who provide additional expertise and support under NHS Service Level agreement arrangements.

4.1 ICB Responsibilities

The organisation will ensure that all staff members are clear about their legal and ethical responsibilities when using personal and patient identifiable information and will ensure the provision of appropriate education and training.

The ICB will make arrangements to meet the mandatory performance assessed requirements of NHS England's DSPT, to a satisfactory compliance level

To manage its obligations the ICB will issue and support standards, policies and procedures ensuring information is Held, Obtained, Recorded, Used and Shared correctly (HORUS principles).

4.2 Responsibilities of Users

Recorders and users of information must:

- Be aware of their responsibilities
- Comply with policies and procedures issued by the ICB
- Work within the principles outlined in the DSPT, relevant NHS and statutory bodies Codes of Practice and conduct

4.3 Caldicott Guardian

The Caldicott Guardian has a key role in ensuring that the ICB achieves the highest standards in handling patient information. This includes representing and championing patient confidentiality requirements and issues wherever appropriate within the ICB's overall governance framework. The Director of Nursing and Quality is the ICB Caldicott Guardian.

4.4 Senior Information Risk Owner (SIRO)

The SIRO is responsible for ensuring that there is a risk policy and strategy that incorporates the management of information risk; there is a risk assessment process for information risk; that relevant risks are included in the annual Statement of Internal Control; that threats to information security are managed; to ensure that employees are aware of their responsibilities and to keep the Senior Leadership Team informed about relevant information risks. The Director of Finance and Contracting is the ICB SIRO.

4.5 Information Asset Owners (IAO's)

Organisational IAO's are designated by the SIRO and will be supported where appropriate by Information Asset Administrators (IAA's), who are responsible for managing specific business services.

4.6 Information Asset Administrators (IAA's)

IAA's roles are to understand what information is held in their business areas, manage the additions and removal of assets, understand how information is moved

and shared and manage who has access to it and why. As a result they are able to understand and address risks to information assets they "own" and to provide assurance to the IAOs and SIRO on the security and use of the assets. The ICBs Information Asset Register details the IAO's and IAA's for each of the ICB assets where it is felt appropriate to identify them at business service level. IAO's have day to day responsibility to ensure that policies and procedures are followed by staff in their services and they have a responsibility to recognise actual or potential security incidents and manage these under the organisations Incident Policy arrangements.

4.7 ICB Information Governance Lead and Deputy Senior Information Risk Owner

The ICB IG lead is the Deputy SIRO, the Head of Corporate Governance and ICB board secretary. The Information Governance Lead is responsible for co-ordinating the above functions and to ensure the development of robust information governance in the ICB.This is done in conjunction with and through the support of the Information Governance team in NHS AGEM CSU. NHS AGEM CSU also provide the Data Protection Officer (DPO) function for the ICB.

4.8 Data Protection Officer

The DPO is responsible for ensuring that the ICB remains compliant at all times with data protection legislation and will lead on the provision of subject matter expertise in this field, including the following:

- Data protection legislation,
- Privacy & Electronic Communications Regulations,

4.9 The Governing Body Chair

To ensure that Information Governance and Data Security are championed at the highest level of the organisation, the Governing Body Chair ensures that the ICB is accountable for maintaining an effective programme of practices and assurance.

5.0 ICB Information Governance Aims and Objectives

The fundamental aims of Information Governance are:

- To support the commissioning and therefore provision of high-quality care by promoting the ethical, legal, effective and appropriate use of information
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.

- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.
- To hold information securely and confidentially
- To obtain information ethically, legally and efficiently, i.e. in line with the Data Protection Act 2018 and relevant codes of practice including those issued by the Department of Health and Professional regulatory bodies.
- To record information accurately and reliably and with the consent of the individual concerned (staff and/or patient) as appropriate.
- To use information effectively, legally and ethically.
- To disclose information ethically and lawfully
- To commission safe care and maximise respect for public and service user privacy and dignity.

6.0 Legal and Regulatory Framework

There are a number of legal and ethical obligations placed upon the ICB for:

- The use and security of personal identifiable information.
- Appropriate disclosure of information when required.
- Regulatory frameworks for the management of information via NHS England's DSPT.
- NHS and professional Codes of Conduct for consent to the recording and use of information.
- Operating procedures and codes of practice adopted by the NHS

7.0 Key Elements of the Information Governance Assurance Framework

The principles of this IGAF are based on the following elements:

7.1 National Requirements

The NHS Operating Framework in England sets out the key priority areas for systematically improving quality across the NHS.

The IG element details that the legal framework governing the use of personal confidential data in health care is complex. It includes the NHS Act 2006, the Health and Social Care Act 2012, the Health and Social Care (Quality and Safety) Act 2015, the Data Protection Act 2018, and the Human Rights Act. The law allows personal data to be shared between those offering direct care to

patients, and it protects patients' confidentiality when data about them are used for non-direct care and other purposes.

It includes the requirement for all NHS organisations to achieve satisfactory compliance against all relevant mandatory requirements in the DSPT, as set out by NHS England.

It notes that "secondary uses" of data are essential if organisations are to run a safe, efficient, and equitable health service.

The ICB is responsible for ensuring that all organisations, with which data is shared, including independent contractors and the third sector, have the required information governance controls and assurances in place. Information security and confidentiality are key priorities in ensuring continued commissioning of quality healthcare and patient centred health services.

7.2 Data Security and Protection Toolkit

The annual information governance assessment is measured via a self-assessment process of compliance against the standards set out in the DSPT and verified by NHS England's Audit Review. The standards are grouped into 10 self-assessment areas:

NHS organisations are required to submit online IG performance reports to NHS England which can be tracked by monitoring bodies (for example CQC, NHS England). Currently ICB's are required to make an annual self-assessment report. This performance assessment is shared with the Care Quality Commission, and the Department of Health. The results are publicly available on NHS England's website. The ICB is required to provide information on DSPT compliance in each Annual Report.

7.3 ICB's Information Governance Management arrangements

The ICB's Director of Finance and Contracting is the SIRO and Information Governance lead and has day to day responsibility for the Information Governance agenda and is supported by the information Governance team in NHS AGEM CSU.

Information Governance responsibility in the organisation lies with the Senior Leadership Team. The Senior Leadership Team discharges its information governance functions through the Audit and Risk Committee as an assurance group to the Governing Body. The Director of Finance and Contracting as the SIRO and IG lead provides assurance on Information Governance to the Audit and Risk Committee.

The Director of Finance and Contracting has overall responsibility for overseeing the development and implementation of this framework. This is subject to regular review as part of the annual DSPT planning cycle.

8.0 Information Governance – Key Areas

8.1 Asset Register

The ICB Asset Register is reviewed annually to appropriately scope and prioritise risk areas.

Information assets are classified for sensitivity and criticality to the ICB.

ICB information assets will have an identified owner and where appropriate will have Information Asset Administrators who will be senior individuals involved in managing the relevant business areas. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. Identified key risks (those rated medium or high), once assessed by the SIRO, will be considered for inclusion on the ICB Risk Register.

8.2 Audit and Compliance checks

The use of audit and compliance check aim to:

- Help raise the awareness of Data Protection compliance and the legal framework upon which Information Governance is based
- Show the organisation's commitment to and recognition of the importance of information governance in day to day working practices
- Provide evidence of compliance to support continuous improvement
- Identify information governance risks to enable, practical, pragmatic and operational specific recommendations to be considered
- Provide a way of sharing knowledge

The focus of audits will be to determine organisational compliance across the information governance agenda.

8.3 Communication

The ICB has several communication channels that support Information Governance. These include:

- A Publication Scheme which complies with the ICO's Code of Practice in relation to the Freedom of information Act 2000
- Intranet and internet pages
- Information Governance all staff communications provided regularly with key messages shared
- Targeted communication for specific projects or messages

- Fair Processing Notices
- The use of staff questionnaires to test understanding
- The completion of annual e learning IG training sessions to support understanding and the practical application of information governance principles

8.4 Contracts

Procurement and contracting services are commissioned by the ICB from NHS AGEM. The Information Governance team work with this team as appropriate, to support ensuring the procurement and contracting processes meet the required IG standards.

8.5 Corporate Records

The ICB will ensure it is managing Corporate Records effectively and in line with the DSPT Toolkit requirements. The Board Secretary is responsible for records management in the ICB, supported appropriately by the IG team.

8.6 Data Subjects Information Rights

The ICB contracts with NHS AGEM for the provision of a subject access request service under the Data Protection Act 2018. Through this service responses are made to all requests received within agreed KPI and statutory timescales. The ICB has separate policy documentation that provides further details of this service.

8.7 Information Security Management

Information Security management covers all aspects of information, whether spoken, written, printed, in electronic format or transferred to any other medium across its lifecycle. It includes the provision of IT security and governance management.

Following good practice there are six basic outcomes measures of effective IT security and governance management:

- Supports organisational objectives and aligns with strategic direction
- Risk management – executing appropriate measures to mitigate risk and reduce potential impacts on information resources to an acceptable level
- Value delivery – optimizing security investments in support of the ICB business objectives
- Resource optimization – using information security knowledge and infrastructure efficiently and effectively
- Performance measurement – monitoring and reporting on information security processes to ensure that objectives are achieved
- Integration – integrating all relevant assurance factors to ensure that processes operate as intended from end to end.

8.7.1 Cyber Security

The technical threats to services are constantly changing with new technologies and services presenting a widening profile over which a malicious attacker could operate. This 'threat landscape' is magnified by the constant introduction of new vulnerabilities into existing and legacy technologies, especially as the ICB explores the use of technology to find efficiencies in working. This presents a challenging management environment where the balance between the provisions of ICT functionality must be tempered by the risk exposure to technical threats and malicious attack

The ICB through commissioned IT support services is part of the CareCERT programme which provides alert notification of threats both nationally and locally where any specific threat has been identified so that appropriate action can be taken.

8.8 Policies

Information governance policies are presented to the SIRO through the Lincolnshire Commissioning support forum. Following presentation to the Audit and Risk Committee on their recommendation they will be submitted to Governing Body for approval. All policies are made available to staff via the ICB intranet/internet site and are communicated in line with the ICB communication policy requirements.

Existing policies are updated, and new policies introduced in line with the current information governance agenda. These policies provide the organisation's code of conduct and must be read in conjunction with the organisation's Staff Handbook and staff employment contracts.

Policies outline scope and intent and provide staff with a robust IG framework whilst setting out their responsibilities as employees of the ICB. The ICB is committed to ensuring that all staff and those working with the ICB are familiar with the organisation's objectives and what is expected of staff in order to achieve these objectives. Policies and procedures are one of the key means the ICB uses to communicate these expectations to staff.

8.9 Registration Authority and Staff Identity Service

The Registration Authority Service and Care Identity Service is provided by NHS AGEM who are responsible for the registration process by which users of Smartcard-enabled IT applications are authenticated.

The Registration Authority is the governance framework within which the ICB can register individuals as users to access the NHS Smartcard enabled system(s) to maintain the confidentiality and security of information.

Having a common and rigorous approach to how users are registered and are given access to the national services, and other services, is an integral part of protecting the confidentiality and security of personal and other health care details.

8.10 Risk Assessment and Incident Management Process

Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisation's computer systems, loss of system availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process person identifiable data of sensitivity, which needs to be protected from loss or inappropriate disclosure.

Clear guidance has been documented and issued to staff and all staff must be made aware of the organisation's incident reporting and management procedures (managed via the Datix system). This process is supported by ICB policies and procedures regarding information risk management. The process for the investigation of Information Governance Serious Incidents (SI's) is in line with NHS England's "Guide to the Notification of Data Security and Protection Incidents" published in May 2018. Reference is made to this checklist in the ICB Incident Reporting Policy.

The Director of Finance and Contracting, with the appropriate support of the Information Governance team in NHS AGEM is responsible for ensuring that adequate arrangements are in place for:

- Reporting IG events or incidents
- Managing IG Risks
- Analysing, investigating and escalation reporting of events/incidents and recommendations in line with NHS reporting requirements.
- IG work plans progress recommendations and lessons learnt

8.11 Training and Development

Information Governance Training and Development is essential for the development and improvement of staff knowledge and skills relating to IG not only within the IG Team but across the ICB.

Staff must understand the value of information and their responsibilities which include data quality, information security, records management, confidentiality, legal duties, information law and rights of access, and patient's rights to privacy and choice.

Training is available through mandatory annual e – Learning in line with DSPT requirements.

Information Governance training is an annual statutory mandatory requirement for all staff. Line managers are responsible for ensuring specific IG role related training is delivered on induction.

The organisation utilises the following additional methods to ensure staff are

trained in Information Governance:

- Articles in ICB staff communications
- Regular IG Campaigns
- Staff Questionnaires
- Policies, Procedures and Guidelines – staff have clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. IG awareness and mandatory training procedures are in place and all staff received training appropriate to their role.
- Confidentiality – staff are provided with clear guidance on keeping information secure and on respecting confidentiality
- Consent – is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the use of such information are appropriately respected
- Fair processing – individuals are informed about the proposed use of personal information.

The Director of Finance and Contracting, with the support of the Information Governance team in NHS AGEM, is responsible for monitoring training compliance.

9.0 Management of the Information Governance Framework

The organisation will be responsible for implementing the Information Governance Policy and Framework.

The Director of Finance and Contracting will manage and monitor compliance with this policy and report to the Audit and Risk Committees as appropriate.

10.0 References

10.1 Legal Framework

The organisation is bound by the provisions of several items of legislation and regulation affecting the stewardship and control of information. The main relevant legislation regulations are:

- Data Protection Act 2018
- UK General Data Protection Regulation
- Human Rights Act 1998
- Access to Health Records Act 1990

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health and Social Care Act
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations)
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974
- Re-use of Public Sector Information Regulations 2005

This list is not exhaustive

10.2 Regulatory Framework

In relation to many of the above the NHS has set out and mandated several elements of regulation that constitute “Information Governance” through a national programme. This area is developing at a fast-changing pace and the focus to meet these requirements is regularly reviewed by the Director of Finance and Contracting supported by the Information Governance team in NHS AGEM.

Regulatory Elements are:

- The DSPT which requires ICB’s to assess their progress against set criteria
- Caldicott Reports and Recommendations
- Standards for Information Security Management
- Information Quality Assurance
- NHS Confidentiality: Code of Practice (2003)
- NHS Guidance on Consent to Treatment

- Care Quality Commission Regulations
- Information Commissioner's Office

10.3 Ethical Framework

The right to expect privacy ethically entitles individuals to exercise of control over the content, uses of and disclosures of information about them as an individual. Respect for that privacy by staff is essential for maintaining trust in, and integrity of any services provided by the ICB.

Three official sources provide basic principles that underpin ethical frameworks and which form part of staff working practices in implementing this policy. These are:

A. Department of Health Code on Confidentiality which includes the following important principles:

Staff must:

- Protect – look after patient's information
- Inform – ensure patients are aware of how their information is used; there should be no surprises
- Provide Choice – allow patients to decide whether their information can be disclosed and used in particular ways
- Improve practice – by always looking for better ways to protect, inform and provide choice

So that the Public/patient will:

- Understand the reasons for recording and processing information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way the NHS handles information
- Understand their rights to access information held about them

B. Caldicott principles, applying to the disclosure of patient-identifiable information are:

- Justify the purpose(s) of every proposed use or transfer
- Don't use it unless it is absolutely necessary, and

- Use the minimum necessary.
- Access to it should be on a strict need to know basis
- Everyone with access to it should be aware of their responsibilities; and
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality

C. The Information Commissioner's Office has specific responsibilities under the Data Protection Act 2018. This Act provides a framework to ensure that personal information is handled properly. The Act works in two ways:

1. It states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:
    - Processed with transparency, fairly and lawfully
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Not kept for longer than is necessary
    - Processed in line with individual rights
    - Secure
    - Not transferred to other countries without adequate protection
2. The Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Additionally, all staff must be familiar with their own professional codes relating to ethical aspects of information governance.

11.0 Information Governance Management Strategy

This strategy sets out the approach taken within the ICB to provide a robust Information Governance Framework for the current and future management of information.
Information Governance currently encompasses the following initiatives or work areas:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Uses Assurance
- Corporate Information Assurance

Others may be included as the scope of the Information Governance agenda widens. Information Governance has the following fundamental aims:

- To support the commissioning of high-quality care by promoting the effective and appropriate use of information
- To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- To enable organisations to understand their own performance and manage improvements in a systematic and effective way.

11.1 Purpose of the Strategy

The purpose of this strategy is to set out the approach that the ICB will take to provide a robust Information Governance Framework for the future management of information assets.

This strategy has been developed taking into consideration:

- ICB self-assessment against national Information Governance requirements including the DSPT, NHS Operating Framework and CQC Registration.
- Relevant legislative framework
- Guidelines for Caldicott Guardians
- NHS England's priority areas for Information Governance including compliance with the National Opt Out Programme
- External audit expectations and recommendations

There are two key components underpinning this strategy:

- A focus on the risks associated with information assets
- An annual action plan arising from an assessment against requirements set out in the NHS DSPT

11.2 Responsibilities for delivering this strategy

- The Senior Leadership Team is responsible for ensuring that sufficient resources are made available to support the requirements of this strategy.
- The Senior Leadership Team will be responsible for the overseeing of the delivery, evaluation and monitoring of outcomes of this strategy.
- The Director of Finance and Contracting will be responsible for the operational delivery and monitoring the implementation of the strategy and subsequent action plans reporting to the Audit and Risk Committee.

11.3 Wider Implications of Information Governance

This strategy cannot be seen in isolation as information plays a key part in Corporate Governance; Strategic Risk; Clinical Governance; service commissioning, planning and redesign; service delivery and performance management. The continual implementation of this strategy will undoubtedly reduce the level of risk.

The focus on the risks associated with information assets will be captured on the Information Asset Register. This will include the identification of Information Assets and the Information Asset Owner and Information Asset Administrators, information governance risk assessments, control measures, and the completion of Data Protection Impact Assessments and the agreement of Information Sharing Protocols and Agreements.

Inbound and outbound data flows will be ‘mapped’ assessed and revised to mitigate risks of breaches to confidentiality and data security.

11.4 Associated Information Governance Policies/Strategies

Key policy documents include

- Freedom of Information Policy
- Information Lifecycle and Records Management Policy and Strategy
- Data Protection, Caldicott and Confidentiality Policy

This is not an exhaustive list and all IG related policies and procedures are available on the ICB website and staff intranet.

11.5 Information Governance Action Plan

The ICB Information Governance work plan is the framework developed to establish the overall direction of information governance and the baseline principles and objectives for a robust information handling culture that permeates throughout the organisation. It sets out a programme of development to achieve and inform staff approaches on the performance of duties relating to the management of information and its security regardless of seniority. An IG action plan aligned to IG principles supports the delivery of the DSPT requirements.

Fundamental to the success of delivering the Information Governance Strategy is developing a robust and positive Information Governance culture within the organisation. Awareness and training will be provided to all staff to promote this. To deliver this the ICB will utilise Data Security Awareness Level 1 e-Learning package.

12.0 Dissemination

Copies of this Policy will be made available to all staff via the intranet/ internet. All staff will be notified of new or reviewed Policies via the communication arrangements detailed in the ICB communications plan.

This document will be included in the ICB Publication Scheme in compliance with the Freedom of Information Act 2000.

13.0 Monitoring and Audit

- The organisation will monitor compliance with this policy through the ICB Audit and Risk Committee.
- As assessment of compliance with requirements, within the DSPT will be undertaken each year
- Annual reports and proposed action/development plans will be presented to the Governing Body or its delegated committee for approval prior to submission of the DSPT
- The organisation will ensure that the support infrastructure for the SIRO is in place, and is kept under regular review

Ref	Minimum Requirements	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	All staff have all completed Data Security Awareness Mandatory Training in the last 12 months	Data Security Awareness Training compliance	Head of Corporate Governance	Monthly

	Information Assets have a designated owner	Review of Information Asset Register	Head of Corporate Governance	Annually
	Staff understand their duties in relation to Information Governance	Confidentiality spot check	Head of Corporate Governance	Annually
	Information Governance SIRIs managed in line with NHS E standards	SI Reports	Head of Corporate Governance	Quarterly

14.0 Links to Standards/Performance Indicators

This policy links directly to work required as part of the annual DSPT return.

Standards/Key Performance Indicators

Target/Standards	Key Performance Indicator
Meet each of the mandatory DSPT requirements	Overall DSPT assessment

15.0 Review of Policy

This policy will be reviewed every 3 years unless there are changes to the requirements within the DSPT, any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

15.1 Archiving

The Board Secretary is responsible for ensuring that superseded versions of policies and procedures are retained in accordance with the Records Management: Code of Practice for Health and Social Care.

Appendix 1 Structure Chart: Information Governance Management Framework