HSC Health and Social Care Board

Information Governance Strategy

2021/22

DOCUMENT VERSION CONTROL

Reference Number	**Version** 3.0	**Status** Approved	**Author(s)** Information Governance Manager
Document objectives: Sets out how the HSCBs Information Governance Policy will be delivered			
Intended Recipients: HSCB staff			
Group/Persons Consulted: Information Governance Steering Group			
Monitoring Arrangements and Indicators: Information Governance Steering Group			
Training/Resource Implications: N/A			
Date Approved **Approving Body**	Approved by HSCB Senior Management Team 01/06/2021		
Date of Issue			
Review Date			
Contact for Review	Information Governance Manager		

Version number	Purpose / Changes	Author	Date
1.0	Due for review April 2014	K Moore	April 2014
2.0	Draft	K Moore	June 2014
3.0	Due for review April 2017	K Moore	Mar. 2017
4.0	Reviewed May 2021	K Moore	May 2021

Table of Contents

1.0 Introduction

As part of Health and Social Care within Northern Ireland, the Health and Social Care Board (HSCB) recognises its legal and statutory obligations in relation to the management of information assets within its care, and the need for a balance to be struck between openness and confidentiality in the management and use of those information assets. To this end, the HSCB fully supports the principles of corporate governance and recognises its public accountability, but equally places significant importance on ensuring the confidentiality of patient, client, carers and staff information, as well as corporately sensitive information, and the need to ensure robust security measures are adopted to protect that information from accidental loss or deliberate unauthorised disclosure.

2.0 Purpose

The purpose of this strategy is to provide clear direction to the HSCB in delivering the requirements of Information Governance and associated policies. The Strategy will assist in establishing and maintaining a robust and effective Information Governance framework that allows the HSCB to fully discharge its strategic duties ensuring that overall corporate compliance is met both in relation to legal[1] and statutory obligations and in meeting all relevant codes of practice.

3.0 Scope of Strategy

The Strategy will be used as a vehicle to improve Information Governance within the HSCB. An action plan will be developed each year or over a longer period dependent on the strand. The action plan will be monitored by the Information Governance Steering Group[2]. Reports will be submitted to the HSCB Senior Management Team and the HSCB Governance Committee on a regular basis.

4.0 Objectives

The key objectives of this Strategy are to ensure the effective management of Information Governance by:

- Complying with all legislation;
- Establishing, implementing and maintaining policies for the effective management of information;
- Ensuring a consistent approach within the HSCB with regard to information management;

[1] *Refer to Appendix 1 Page 12 for Legislation/Guidance Documents*

[2] *Refer to Appendix 2 Page 16 for Terms of Reference*

- Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information;
- Ensuring all HSCB staff are sufficiently trained and enabled to follow and promote best practice in regard to the management of information;
- Reducing duplication and looking at new ways of working effectively and efficiently;
- Minimising the risk of breaches and inappropriate use of personal data;
- Have appropriate information management systems and controls in place which allow positive assurance to be provided annually to the Department of Health via the Information Management Assurance process;
- Ensuring the public are effectively informed and know how to access their information and exercise their right of choice
- Providing assurance that all information risks are identified, managed and where possible mitigated.

5.0 Information Governance Framework

The purpose of the Information Governance Framework is to set out and promote a culture of good practice around the processing of information and use of information systems throughout the organisation. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The Board requires all employees to comply with the extant Policies, Procedures and Guidelines which are in place to implement this framework. A summary of the Information Governance Framework[3] is included in this document.

5.1. Information Structure and Reporting Arrangements[4]

- **HSCB Governance and Audit Committee -** as a committee of the HSCB Board with delegated responsibility, the Governance and Audit Committee will formally review progress on the implementation of this Strategy and Action Plan on annual basis.

- **HSCB Senior Management Team -** SMT will receive regular updates on Information Governance matters via the Director of Strategic Performance who fulfills the role of Senior Information Risk Owner (SIRO). The Director of Social Care and Children also sits on the Senior Management Team and fulfills the role of Personal Data Guardian (PDG).

- **Information Governance Steering Group (IGSG)** - Consisting of representatives from all HSCB Directorates the primary function of the IGSG will be to lead the formation of the Information Governance framework across the organisation. To support and drive the broader

[3] *Refer to Appendix 3 Page 18 for Summary Information Governance Framework*
[4] *Refer to Appendix 4 Page 20 for Information Governance Organisation Structure Flowchart*

information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation. The Group will be chaired by the SIRO/IG Manager and will meet on a quarterly basis.

- **Records Management Working Group (RMWG)** – Chaired by the Information Governance Manager this Group will address the Records Management function within the Board implementing an effective system across all offices. Membership will consist of representatives from each Directorate. Members will in turn cascade progress across all teams within their Directorate.

- **Information Governance Team -** The Information Governance Team is operationally responsible for the day to day implementation of all aspects of Information Governance within the HSCB.

5.2. Policies

A clear policy framework is critical to ensuring that a coherent approach to Information Governance is delivered across all HSCB offices. A number of policies have been previously approved by the HSCB Governance Committee[5]. All policies linked to the Information Governance function will be reviewed and updated as necessary on a regular basis.

5.3. Leadership

Effective leadership is essential to create and nurture a corporate culture conducive to effective Information Governance. A culture of both corporate and individual ownership and responsibility is essential when looking to achieve effective compliance with all statues and codes of practice.

5.4. Organisational Processes

It is critical that clear processes are designed to meet Information Governance requirements, that they are properly documented, that they are effectively communicated, that staff receive tailored training relevant to both their need and designation and that compliance with these processes is monitored both locally and on an organisational level. Any learning from this monitoring should be fed back to all staff and the relevant committees of the Board.

5.5. Supporting Staff

Clear accountability arrangements will ensure that HSCB staff are accountable for the work that they do and the information assets they process. There should be an open and supportive environment in which errors, mistakes or concerns can be raised immediately with management, and corrective measures implemented swiftly and processes changed accordingly. This culture will further mitigate risks associated with the

[5] Refer to Page 11 for link to Information Governance Policies on the HSCB Intranet

handling and processing of sensitive information, both corporate and personal in nature.

5.6. Communication

Effective and timely communication of Information Governance matters to all HSCB staff in all locations is essential if the HSCB is to meet all goals associated with this strategy. As well as ensuring compliance with the elements contained within this strategy, the wider Information Governance agenda within the general area of the Public Sector is a fast moving and quickly developing one, and from time to time we are required to communicate new directives or initiatives to staff. Communicating matters to staff must be handled with care to ensure that the message is received and acted upon.

5.7. Training

Whilst it is important to ensure that staff are aware of Information Governance issues it is also essential to ensure that they understand and are confident enough to put into operational use, what they already know and those skills they will attain during the course of the roll out of the Information Governance Strategy. The HSCB will tailor training accordingly, whilst developing new methods to up-skill existing staff and new staff entering the service.

5.8. Monitoring Implementation and Performance

Performance will be monitored annually against Information Management Assurance guidance with annual assurance being provided to the Department of Health. The Information Governance function must also contribute to the Governance Statement providing assurance in respect of information risk. The action plan associated with this strategy will also provide a mechanism by which progress can be monitored. The following reporting arrangements will be put in place:

- An annual report on progress against the Information Governance Action Plan will be provided to the HSCB Governance and Audit Committee for information.
- Annual report on progress will be provided to the Senior Management Team for approval;
- Quarterly updates on progress will be provided at the IGSG meetings;

6.0 Information Governance Action Plan

The Information Governance Action Plan below details actions required to assist the HSCB in meeting the Information Management Assurance requirements. Actions have been broken down into specific work areas. This Action Plan will be reviewed annually to take account of changing demands and focus:

Health and Social Care Board

Information Governance Action Plan

2021/22

Information Governance Action Plan 2021 – 2022

1. Strategic Priority/Theme
To work with DoH, PHA and other stake-holders to ensure the most effective and smooth transition of the HSCB's functions and staff and to ensure staff are fully informed and involved throughout the change.

What will we do	Owner	By When	How will this achieve our objective	Indicative costs
• Participate with the Department led HSCB Migration Programme coordinating and providing regular updates for the Data and Information Management Migration Workstream alongside colleagues in the Department of Health, BSO, PHA and RQIA; – Chair the Data & Information Management Workstream meetings; – Develop a Workstream Plan providing regular updates; – Complete Checkpoint reports on a monthly basis and attend Checkpoint meetings.	HSCB IG Team	Ongoing – monthly meetings	Enable us to implement and monitor agreed actions.	Non recurrent funding provided by DoH Migration Programme for temporary Band 7 Project Manager

• Conduct a review/audit of HSCB Information Assets prior to formal transfer to the Department of Health in April 2022; – In-depth review of Directorate Information Asset Registers in line with regional developments following recent Cyber Security Incidents;	HSCB IG Team	February 2022	Work closely with HSCB Information Asset Owners to review existing IAR and update. This will provide DoH with a comprehensive register of information assets prior to migration.	
• Inform Oasis of the planned closure of the HSCB and update the contract for records held in off-site storage on 01 April 2022.	HSCB IG Team	December 2021	Advise Oasis of changes required in advance of HSCB closure.	
• Review paper records held by HSCB in line with the HSC Retention and Disposal Schedule (Good Management, Good Records) bearing in mind restrictions on disposal due to current/forthcoming Public Inquiries. – Identify records being retained for permanent preservation; – Engage with PRONI to review identified records and establish process for submission; – For all other records review in line with GMGR and take appropriate action.	HSCB IG Team	February 2022	Completing this exercise will enable HSCB to review all paper records and make a decision on retention in line with GMGR, to ensure only those records required are formally transferred to DoH.	
• Review all Information Governance Policies and update prior to migration to	HSCB IG Team /	September 2021	Ensure that all IG policies are aligned to	

the Strategic Planning and Performance Group on 01 April 2022;	Information Management Branch DoH		DoH or where relevant BSO.	
• Develop with colleagues in the Department of Health an Information Governance Framework for the Strategic Planning and Performance Group.	HSCB IG Team / Information Management Branch DoH	December 2021	The Framework will establish Information Governance reporting structures and senior Information Governance roles and responsibilities such as SIRO, PDG, Data Protection Officer, Information Asset Owners.	
• Prior to March 2022 agree procedure for the processing of FOI requests following migration: – Amend current FOI Email Address following HSCB migration; – Develop plans for requests in progress at 31st March 2022; – Agree with colleagues in the DoH how requests for information held by the Strategic Planning and Performance Group (SPPG) will be progressed;	Information Governance Team	December 2021	From 1 April 2022 HSCB will cease to be a public sector organisation for FOI purposes. Requests for information held by SPPG from this date will be formally received by DoH and assigned for processing.	

2. Strategic Priority/Theme
Cyber Security Objective

What will we do	Owner	By When	How will this achieve our objective	Indicative costs
• Work collectively with the regional Information Governance Advisory Group and the Cyber Security Programme Board to review the security processes of HSCB Information Assets in particular where third party sharing arrangements are in place.	HSCB IG Team / Regional IGAG and Cyber Security Programme Board	April 2021 - Ongoing	Updating Information Asset Registers will provide HSCB and the Cyber Security Programme Board with specific details of information sharing which will be required in the event of future cyber incidents.	Regional solution being explored with funding (if available) from DHCNI

3. Strategic Priority / Theme

Maintain sound systems of internal control in relation to corporate and information governance activity including compliance with statutory legislation, equality and human rights.

What will we do	Owner	By When	How will this achieve our objective	Indicative costs
• Ensure key IG roles within the organisation complete appropriate training during 2021/22;	Information Governance Team	September 2021	Given a number of changes in personnel during 2020/21 IG will arrange training for key roles such as Personal Data Guardian, Senior Information Risk Owner, Information Asset Owners and members of the Information Governance Team complete appropriate training during 2021/22.	There will be a cost for training but has not been finalised.
• Ensure HSCB staff have completed mandatory IG training	Information Governance Team	Ongoing	HSCB have adopted a number of mandatory IG e learning programmes. IG Team will monitor staff completion rates and target new starts to ensure HSCB meets statutory requirements for awareness training.	Nominal recurrent cost with HSC Leadership Centre who host the elearning platform.

4. Strategic Priority / Theme

To maintain sound systems of internal control in regard to records management by identifying, procuring and introducing a suitable replacement of the current Meridio Electronic Document and Records Management System to the HSCB.

What will we do	Owner	By When	How will this achieve our objective	Indicative costs
• Continue to work with Digital Health and Care NI and BSO ITS to implement a replacement for the current HSCB EDRMS. This work will align and be dependent on the joint DHCNI/BSO ITS Technology Enablement Project (TEP) which will see the introduction of Office 365; – Awaiting clarification on TEP and when available develop detailed project plan with definitive timescales – Provide bi-monthly highlight reports to the HSCB Information Governance Steering Group (Project Board) and the DHCNI Portfolio Board.	Information Governance Team	March 2022	Enable IG Team to implement a replacement EDRMS which will remove the risk associated with the current unsupported system.	Non recurrent funding allocated by DHCNI
• Engage with third party providers to explore and put in place an emergency support arrangement to address events should the current EDRMS fail during the interim period;	HSCB IG Team / DHCNI	July 2021	Meridio is end of life and unsupported. Explore options with Kainos or other 3rd party to provide support in the event of system failure to	

			enable business continuity.	

- As part of the EDRMS replacement project conduct an in-depth review and develop treatment plans for archived electronic records held in the following repositories:
– Network Drives;
– Email Accounts (Former Staff and Archived Email Accounts);
– My Workspace Accounts for former HSCB staff;
	IG Team / IAO's	February 2022	Conducting an in-depth review of archived records will enable an informed decision to be taken on the large volume of electronic records held in archive repositories. Decisions can then be made to dispose or retain records, and if relevant transfer to the replacement EDRMS for continued management.	Non recurrent funding allocated by DHCNI

7.0 Summary and Conclusions

Information Governance is a vital and integral part of the Boards overall Governance programme. Implementation of this Strategy and its subsequent policies, procedures, protocols and guidelines will help to ensure that the HSCB has the appropriate framework in place to meet legislative and organisational requirements.   A copy of the HSCB's Information Governance Policies and Guidance can be located on the HSCB's intranet site or by clicking here.

Appendix One

Legislation / Guidance Documents

There are a number of pieces of legislation and guidance which have a significant impact on records management. A selection of these is listed below.

Public Records Act (Northern Ireland) 1923

All HPSS records are public records under the terms of the Public Records Act (Northern Ireland) 1923. Chief Executives and senior managers of all Health and Social Care organisations are personally accountable for records management within their organisation. They have a duty to make arrangements for the safekeeping and correct disposal (under the Disposal of Documents Order (Northern Ireland) 1925) of those records under the overall supervision of the Deputy Keeper of Public Records whose responsibility includes permanent preservation.

Data Protection Act 2018

The 2018 Data Protection Act places a statutory responsibility on the HSCB to protect the personal data which is held. In relation to records management this means that the HSCB must implement measures to:

- Maintain the accuracy of records held;
- Protect the security of personal data;
- Control access to the personal data; and
- Make arrangements for secure disposal once the record is no longer required.

Confidentiality and Data Protection Act

All HPSS bodies and those carrying out functions on behalf of the HPSS have a common law duty of confidence to patients/clients and a duty to maintain professional ethical standards of confidentiality. Everyone working for or with the HPSS who records, handles, stores' or otherwise comes across personal information has a personal common law duty of confidence to patients/ clients and to his/her employer. The duty of confidence continues even after the death of the patient/client, or after an employee or contractor has left the HPSS.

The Data Protection Act 2018 (DPA 2018), which replaced the earlier DPA 1998, extended its coverage to include both computer records and manual records of relevant filing systems. The Act, which applies to the whole of the United Kingdom, sets out requirements for the "processing" of personal data (i.e. meaning obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data).

A "data subject", namely, a living individual who is the subject of personal data, has a right of access to their personal data and, in certain circumstances, can have their data corrected or even deleted.
There are 8 basic data protection principles to be followed by anyone "processing"

data, namely:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 to the Data Protection Act 2018 is met, and, in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the same Act is also met;
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under this Act;
- Appropriate technical and HSCB measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedules 2 and 3 to the Act set out conditions, respectively, for the processing of personal data and sensitive personal data. The Information Commissioner, who has responsibility for the enforcement of this legislation, provides guidance on the application of the Act.

Further information on the Data Protection Act is available from the Information Commissioner at: www.informationcommissioner.gov.uk

Freedom of Information Act 2000

The Freedom of Information Act 2000 creates a statutory right of access by the public to all records held by public bodies (with some exemptions). The Act makes provision for the Lord Chancellor to issue guidance on how records systems should be maintained in order to facilitate public access to information held. In particular S46 (1) states:

"The Lord Chancellor shall issue, and may from time to time revise, a *code* of *practice providing guidance to relevant authorities* as *to the practice which it would, in his opinion, be desirable for them to follow in connection with the keeping, management and destruction* of *their records".*

The Act was brought fully into force on 1 January 2005. The HPSS has two main responsibilities under the Act. The HPSS has to maintain its 'Publication Scheme' (effectively a guide to the information which is publicly available) and staff have to deal with individual requests for information.

Anyone can make a request for information, although the request must be made in writing (including email) but an Environmental Information Regulation (EIR) request may be verbal. The request must contain details of name and address of the applicant and the information sought.
The HPSS is obliged to produce information recorded both before and after the Act was passed. It is vital that records are held within a structured Records Management system in order to meet the HPSSs obligations under the Act. It should be noted that the responsibility for responding to information access requests lies with the authority that holds the information. The Act is intended to change the way in which public authorities do business, making them more accountable. The foreword to the Code of Practice on Records Management published by the Lord Chancellor under Section 46 of the Act states:

> "*Any freedom* of *information legislation is only* as *good* as *the quality* of *the records to which it provides* access".

This highlights the importance of good Records Management in the HSCB.

Further information on the Freedom of Information Act is available from:
www.lco.gov.uk

Good Management, Good Records

These guidelines offer an overview of the key issues and solutions, and best practice for HPSS teams to follow when preparing a records management strategy. It represents the joint DHSSPS and PRONI view of how records should be administered and sets the standard required of the HPSS.
The Disposal Schedule has been approved by PRONI. It sets out minimum retention periods for HPSS records of all types, except for GP medical records, and indicates which records are most likely to be appropriate for permanent preservation. It also explains the reasoning behind the determination of minimum retention periods, including legal requirements where relevant.

The Schedule does not replace the requirement for HSCBs to develop and agree their own disposal schedules with PRONI; however, it should form the basis for such schedules.

https://www.health-ni.gov.uk/topics/good-management-good-records

Information Management Assurance Process

The Information Management Controls Assurance Standard sets out criteria by which the HSCB can assess the degree to which it has in place a systematic and planned approach to the management of **all** records which ensures that, from the moment a record is created until its ultimate disposal, the HSCB can control, both the quality and quantity of information it generates; can maintain that information in a manner that effectively services its needs and those of its stakeholders; and can dispose of the information appropriately when it is no longer required.
This standard covers HSC records of all types, both corporate and administrative, including:

- Patient health records (electronic or paper based: including those containing all specialties, but excluding GP medical records).
- Accident and emergency, Birth, and all other Registers.
- Theatre Registers and Minor Operations (and all other related) Registers
- Administrative records (including e.g. personnel, estates, financial and Accounting records; notes associated with complaint handling).
- X-Ray and imaging reports, output and images.
- Photographs, slides and other images,
- Microform (i.e. fiche/film).
- Audio and videotapes, cassettes, CD-ROMs etc.
- Computer databases, output and disks etc and all other electronic records.
- Material intended for short term or transitory use, including notes and 'spare' copies of documents.

Recent legislation, particularly the Freedom of Information Act 2000, is having a significant effect on record keeping arrangements in public authorities. HSC bodies must ensure that records management policies and procedures are fully compliant with this new legislation and with government policy on the management of information.

ISO 15489 International Standard on Information and Documentation - Records Management

The International Standard on managing recorded information, initially based on an earlier Australian standard, was adopted by ISO in 2001 and updated in 2016. The Standard acts as an enabler towards accreditation and renewal of IS09001 and other quality standards. It also provides a specification against which record management practices may themselves be audited.

General Data Protection Regulations (GDPR)

The General Data Protection Regulation (GDPR) 2018 is directly applicable as law in the UK. There is greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance.

The GDPR introduces a principle of ‘accountability’. This requires that organisations must be able to demonstrate compliance. The key obligations to support this include:

- the recording of all data processing activities with their lawful justification and data retention periods
- routinely conducting and reviewing data protection impact assessments where processing is likely to pose a high risk to individuals’ rights and freedoms
- assessing the need for data protection impact assessment at an early stage, and incorporating data protection measures by default in the design and operation of information systems and processes.

- ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights
- ensuring that data subjects' rights are respected - (the provision of copies of records free of charge, rights to rectification, erasure, to restrict processing, data portability, to object, and to prevent automated decision making).
- notification of personal data security breaches to the Information Commissioner
- the appointment of a suitably qualified and experienced Data Protection Officer.

Appendix Two

Information Governance Steering Group
Terms of Reference

1.0 Purpose

The Information Governance Steering Group is an organisation wide group and reports to the HSCB Senior Management Team and the HSCB Governance Committee. Its purpose is to support and drive the broader information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation.

2.0 Composition

2.1 Membership

The members comprise of the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs), Information Governance Staff and on occasions the Personal Data Guardian (PDG).The current membership list can be found at the end of this document.

2.2 The Chair

The Chair of the IGSG will be the SIRO (deputised by the Information Governance Manager) who will represent the Group at both Senior Management Team and Governance Committee.

2.3 Attendance

All members of this steering group are required to attend meetings set or send representation in their absence for continuity purposes.

3.0 Meetings

3.1 Frequency – This group will meet quarterly to fulfill its remit and reports to the Governance Committee every six months. Reports will be taken to the Governance Committee by the Chair.

3.2 Agenda and Papers

The meeting agenda and supporting papers will be distributed at least 3 working days in advance.

3.3 Minutes/Action Points

Minutes/Action Points will be kept as draft and submitted for approval at the next IG Steering Group meeting.

3.4 Other

In order to fulfill its remit, the IG Steering Group may obtain any professional advice it requires and invite, if necessary, external experts and relevant staff representatives to attend meetings.

4.0 Remit

Key responsibilities of the Information Governance Steering Group:

4.1 To ensure that an appropriate comprehensive information governance framework and systems are in place throughout the organisation in line with national standards.

4.2 Develop Strategic solutions to Common Information Governance problems

4.3 Provide a forum to raise awareness and share experience and best practice in Information Governance

4.4 To direct the work of Records Management Working Group and provide advice and support to other projects and groups to ensure best practice.

4.5 Act as Directorate lead for Information Governance related issues such as Freedom of Information, Information Security/Risk, Data Protection and Records Management.

5.0 Management and Accountability

The Chief Executive has overall responsibility for ensuring that the organisation operates in accordance with statutory and legislative responsibilities. These responsibilities will be delegated on a day to day basis to the SIRO who will report progress to the HSCB Senior Management Team, Governance Committee and as appropriate to the Board.

Current Membership of IGSG:

Chair – Director of Performance and Service Improvement (SIRO)
Deputy Chair - Information Governance Manager
Assistant Director Finance (IAO)
Senior Manager Commissioning (IAO)
Assistant Director of Information, PMSI (IAO)
Business Support Manager, Integrated Care (IAO)
Director, SCCD (IAO and PDG)
Assistant Director of EHealth (IAO)
Assistant Information Governance Managers

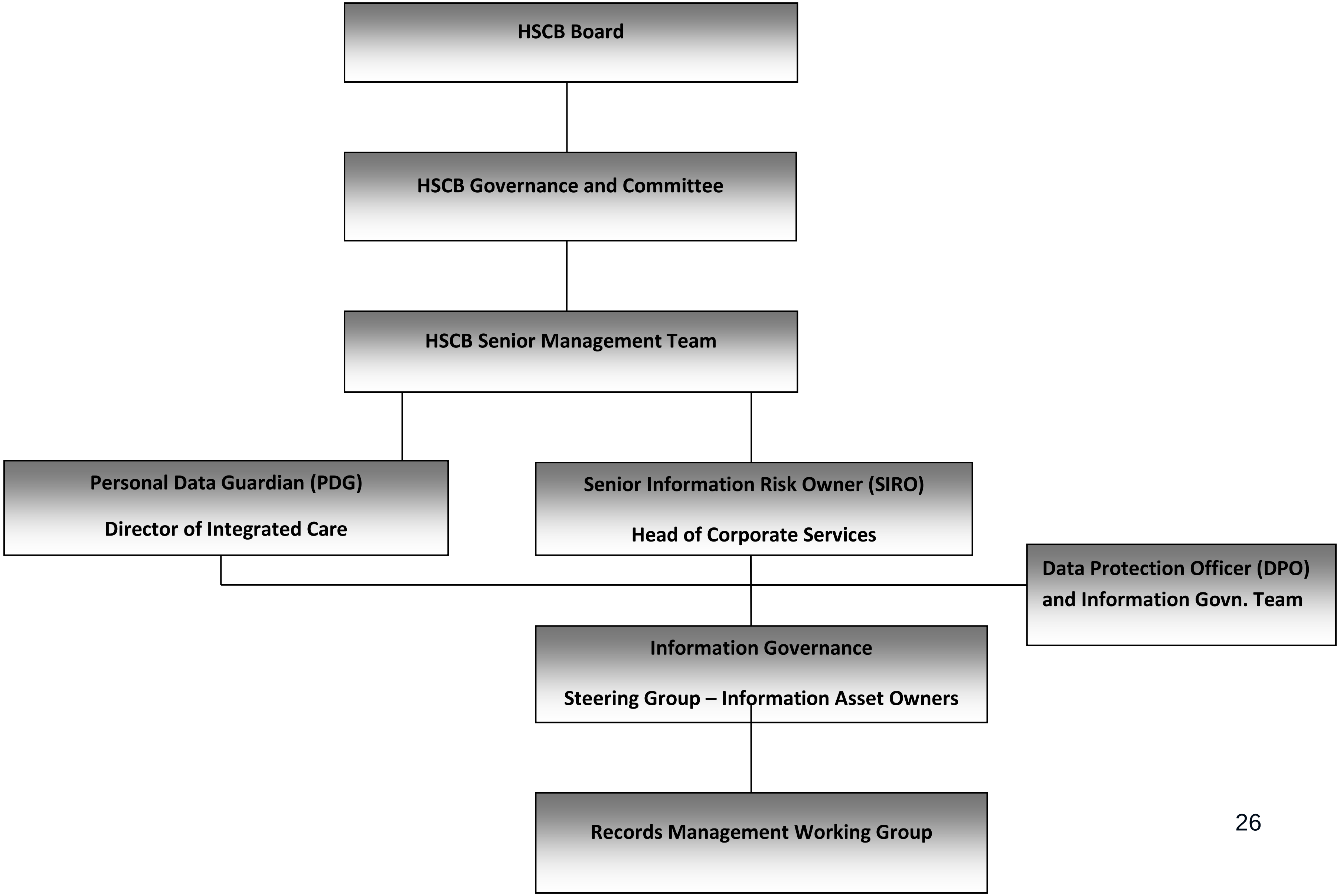
Appendix Three

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	• IG Lead • Senior Information Risk Owner (SIRO) • Personal Data Guardian (PDG)	• The Chief Executive as Accountable Officer has overall accountability for IG and is required to provide assurance, that all risks to the HSCB are effectively managed. • SIRO for the HSCB is Director of Strategic Performance. • PDG for the HSCB is Director of Social Care and Childrens • IAOs for the HSCB are Assistant Directors/Senior Managers within each Directorate
Key Policies	• Over-arching IG Policy • Data Protection Act 2018/Confidentiality Policy • Organisation Security Policy • Information Lifecycle Management (Records Management) Policy • Corporate Governance Policy	• Information Governance Policy • Data Protection/Confidentiality Policy • Information Security Policy) • Information Security Accounts and Passwords • Information Security Asset Management • Information Security Data Transfer • Information Security Email Communications Information Security Use of Internet Information Security Removable Data • Information Security Remote and Mobile Working • Information Security Encryption • Records Management Policy • Access to Information Policy
Key Governance Bodies	IG Board/Forum/Steering Group	• HSCB Governance Committee (meet annually) • HSCB Information Governance Steering Group (meet quarterly) • HSCB Records Management Working Group (meeting quarterly)
Resources	Details of key staff roles and dedicated budgets	• IG Manager x 1 • Assistant IG Manager x 2 • IG Support Officers x 2
Governance Framework	Details of how responsibility and accountability for IG is cascaded through the organisation.	• All staff contracts include IG clauses • Contractors Confidentiality Agreement • Information Asset Register

		• Examples of 3rd party contractors
Training & Guidance	• Staff Code of Conduct **(see criteria's 5, 13 and 12)** • Training for all staff • Organisation Security Policy • Training for specialist IG roles	• Code of Conduct for Employees in Respect of Confidentiality • IG E-Learning Training is mandatory for all staff • HSCB ICT Security Policy • SIRO, PDG and IAO's training completed
Incident Management	Documented procedures and staff awareness	• Information Risk Policy • Information Sharing Protocol • Guidance for reporting IG related incidents • IG Leaflet

Appendix Four

Information Governance Structure and Reporting Lines within the HSCB



HSCB Board

HSCB Governance and Committee

HSCB Senior Management Team

Personal Data Guardian (PDG)

Director of Integrated Care

Senior Information Risk Owner (SIRO)

Head of Corporate Services

Data Protection Officer (DPO) and Information Govn. Team

Information Governance

Steering Group – Information Asset Owners

Records Management Working Group