Information Governance Strategy 2022-27

Approval date:	**23 June 2022**
Version number:	**1.1**
Author:	**David Morgan, Head of Information Governance, FoI Lead and Data Protection Officer (DPO)**
Review date:	**June 2027**
Security classification:	**OFFICIAL – Green: unclassified information**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: HRSTR002

NHS Shetland Document Development Coversheet*

Name of document	Information Governance Strategy 2022 – 2027		
Document reference number	HRSTR002	**New or Review?**	New
Author	David Morgan, Head of Information Governance, FoI Lead and Data Protection Officer (DPO)		
Executive lead	Colin Marsland, Director of Finance and SIRO		
Review date	2027		
Security classification	**OFFICIAL – Green: unclassified information**		

Proposed groups to present document to:		
IGSG	DISG	CGC
Shetland NHS Board		

Date	Version	Group	Reason	Outcome
12/04/2022	0.4	IGSG	PI	PRO
03/05/2022	0.5	DISG	PO & C/S	PRO
15/06/2022	0.5	CGC	PO & C/S	PRO
23/06/2022	0.6	Board	FA	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document
28/02/2022	Initial draft created (adapted, with permission, from the NHS Orkney IG Strategy).
11/03/2022	Changes made to Version 0.1 – editing to reflect NHS Shetland priorities, addition of local policy framework (Appendix 1), correction of 'typos' and to improve compliance with document accessibility standards. Saved as version 0.2
10/04/2022	Changes made to Version 0.2 – editing of content, addition of missing local content, editing/addition of Appendices (2, 3 and 4). Standardisation of terminology and formatting styles. Saved as version 0.3
12/04/2022	Changes made to version 0.3 – formatting and updates to Appendix 4 and 5. Saved as version 0.4
28/04/2022	Changes made to version 0.4 – strategy increased to cover 5 years. Changes made to the content of the Background section. Minor adjustments to the content of the Training section. Added content to the Governance section and moved the table of governance roles to the appendices. Removed names from Appendix 1. Removed Appendix 6. Renumbered the appendices. Saved as version 0.5
15/06/2022	Changes made to version 0.5 – acted on feedback from CGC by including a reference to 'people first' in the vision statement. Correction of minor typographic errors. Saved as version 0.6
23/06/2022	Approved by NHS Shetland Board. Coversheet update and 'Draft' watermark removed. Saved as version 1.0
24/10/2022	Reporting structure in Appendix 2 updated – DiSG now reports to the Finance and Performance Committee (FPC). Saved as version 1.1

Contents

Foreword

In the midst of the Covid-19 pandemic, 93% of the people who contributed to the 2020/21 Scottish Household Survey said the health system was the most trusted public institution.[1]

Digital and information technology solutions have been at the forefront of Scotland's health and care response to the pandemic and digital technologies will remain central to how we re-build and remobilise our systems.

Whilst recognising the many benefits and opportunities available from the expansion of digital technology, people are rightly concerned about how these new technologies store, share, secure and protect their personal health and care data.

To help maintain trust in our protection of personal information, NHS Shetland is investing resources to support the delivery of this Information Governance Strategy. We are building a team of staff to oversee the implementation of operational policies, controls, and processes in key areas of information governance such as, records management, data protection and information security.

We will ensure that data privacy and effective information management are at the heart of our service design and at all stages of the information lifecycle. We will have an efficient and integrated end-to-end model of information management, practice and governance.

Our aim is to ensure the information we manage is always available, always accessible and always secure.

Our vision is for NHS Shetland to establish and maintain sector-leading information governance standards for the design and delivery of remote and rural health and care services for the people of Shetland.

Colin Marsland

Senior Information Risk Owner (SIRO), Director of Finance

NHS Shetland

[1] Scottish Household Survey 2020 - Key Findings

Background

NHS Shetland, Scotland's most northerly Health Board, employs approximately 1,000 staff and is responsible for the delivery of health and care to a remote and rural population of around 23,000 people. Local hospital and community services are provided from the Gilbert Bain Hospital. In addition, visiting consultants provide out-patient clinics as well as in-patient and day-case surgery to supplement the services provided by our locally-based Consultants in General Medicine, General Surgery, Anaesthetics and Psychiatry.

NHS Shetland's Clinical and Care Strategy 2021 - 2031 sets out how we will continue to provide high quality care to our population.

Our aims:

- Integration of services around the needs of local communities
- Making sure the care provided in our NHS is the right care for an individual, that it works, and that it is sustainable
- Making best use of new technologies to improve access, promote person-centred care and reduce inefficiencies

National and local context

The rapid deployment of digital and information technologies has been at the forefront of our response to the pandemic. The Scottish Government's recently refreshed **Digital Health and Care Strategy** is making digital technology central to how Scotland re-builds and remobilises the health and social care system as part of the recovery from Covid-19. The digital strategy also commits to the development of Scotland's first ever dedicated **Data Strategy for Health and Social Care**. In Shetland, this paradigm shift in the delivery of services will be guided by the Health Board's **Clinical, Digital, Digital Security** and **Communication** Strategies.

Whilst recognising the many benefits and opportunities available from the expansion of digital technologies, people are rightly concerned about how their personal health and care data is stored, shared, secured and protected.

Historically, the emphasis has been on how the health and care system uses technology, as opposed to how people use technology. These Digital and Data Strategies put people first.

They recognise the importance of health and care services being integrated and built on people-centred, safe, secure and ethical digital foundations. This allows staff to record, access and share relevant data across the health and social care system, encouraging them to feel confident in their use of digital technology in order to improve the delivery of care.

To ensure the expanding use of health and care information remains safe, secure and ethical, the Scottish Government is developing a **National Information Governance Programme for Health and Care**. With stakeholder engagement scheduled to commence in Quarter 1 of 2022, the aim is to establish a federated, national information governance framework for Scotland.

It is against this rapidly changing background that the **NHS Shetland Information Governance Strategy** describes our local vision for this increasingly important aspect of health and care delivery.

Our vision

‘To establish and maintain sector-leading information governance standards in the design and delivery of remote and rural health and care services that put people first’

Aims

To work in partnership with stakeholders to implement information governance ‘best practice’ in the design and delivery of people-centred health and care services. To ensure the information we manage is always available, always accessible and always secure.

Available

Health and Care providers in Shetland have access to the data they need in order to deliver safe, effective and efficient health and care

Accessible

Patients have access to, and greater control over, their own health and care information – as well as access to the digital tools and services to support their wellbeing

Secure

Data Security is embedded in the design and delivery of all services and technologies. Access and sharing of information is secure across Health and Care in Shetland

Our priorities

To achieve our aims, we will focus on seven priority areas.

1. **Privacy by Design** – will be the default approach for all services and technology. We will use 'state of the art' technology and infrastructure to develop and deliver services.
2. **Availability** – Records will be maintained in accordance with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 and the right information is available to the right people, in the right place and at the right time.
3. **Access** – People will have access to information, their own data, and the digital tools they need to support their health and wellbeing. Information will be accessible to authorised people in all health and care settings.
4. **Sharing and processing** – Information sharing will be undertaken in an open and transparent way, ensuring that people are informed of when, how, and why their information is shared. Records of processing activities, compliant with Article 30 of UK-GDPR, will be created and maintained.
5. **Security** – Information will only be accessed or modified by authorised people, and regular audits will be used to monitor access. People will be able to update information contained in their records.
6. **Training** – All staff will receive appropriate training starting from induction. Training will be refreshed at the frequency recommended by the data protection regulator.
7. **Incident management** – Awareness of, and learning from, incidents will be used for the benefit of people, services and to support the secure use of technology.

By focusing on these seven priority areas we will transform the way health and care information is created, processed and stored. This includes but is not limited to:

- Committing to constant improvement, innovation, and evolution
- Making better use of the data we have now and that we may benefit from in the future
- Involving specialists in Information Governance in the design, assessment and delivery of information tools, technologies, and services

1. Privacy by Design

Privacy by design will be our default position for all services and technology. We will use 'state of the art' technology and infrastructure to develop and deliver services.

UK-GDPR requires the NHS to put in place appropriate technical and organisational measures to implement data protection by design and by default.

This means data protection will be part of our processing activities and business practices from the design stage right through every part of the information lifecycle.

Our approach to system and service development will require data privacy to be considered throughout the system and service development process. Only personal data that is necessary for each specific purpose of any process will be used and all systems must meet the concept of data minimisation (Article 25(2) UK-GDPR).

We will work with services, third sector partners and providers of digital technology to ensure that data is automatically protected with integrated safeguards to protect individuals' rights and freedoms.

Our commitments:

- We will consider data protection issues as part of the design and implementation of systems, services, and business practices. Privacy by Design checklists will be incorporated into project documentation
- We will only process personal data that we need to deliver health and care services
- We will only use technology and partners that provide sufficient guarantees of their technical and organisational measures for data privacy by design and by default
- We will provide information in 'plain language' to the public so that individuals understand what we are doing with their personal data
- We will use state-of-the-art technologies and implement appropriate technical and organisational measures to protect the rights of individuals

2. Availability

Records will be maintained in accordance with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 and the right information is available to the right people, in the right place and at the right time.

We will implement best practice in records management to ensure health and care records and operational information are complete, accurate, up to date and available where and when needed.

The NHS delivers a wide range health and care services. Some of these services are available in Shetland, others are delivered by partner organisations across Scotland and beyond. For health and care delivery to be safe and effective, the right information needs to be available in the right place at the right time.

As required by the Public Records (Scotland) Act 2011 (PRSA 2011), NHS Shetland has agreed a Records Management Plan (RMP) with the Keeper of the Records of Scotland. The RMP describes how NHS Shetland will establish and improve its processes for creating, storing, retrieving and disposing of its physical and digital records.

Our commitments:

- Our Records Management Plan will be agreed by the Keeper of the Records of Scotland
- Information to support health and care delivery will be available where and when it is needed
- Information will be complete, accurate and up to date
- Our Business Continuity Plans describe and test how essential health and care information will be protected and/or quickly restored when services are disrupted

3. Access

People will have access to information, their own data, and the digital tools they need to support their health and wellbeing.

Technology has changed how people access our services and the ways in which they are offered. People want and expect to have access to their own information and tools to support their health and wellbeing. The response to COVID-19 has presented challenges that have been met by the innovative use of technology and information, supporting the care and services provided by NHS Shetland.

For our staff, it has meant the rapid adoption of new technologies and for our patients it has provided access to technology enabled services closer to home. Access to, and availability of, health and care information has driven our local response to the pandemic.

Our commitments:

- People will have secure access to their records wherever and whenever they request it
- We will increase the number of ways people can access information about the care and support they need
- People will understand their data rights and responsibilities when accessing and using health and care information and services
- Information will be accessible to authorised staff in all health and care settings

4. Sharing and processing

Information sharing will be undertaken in an open and transparent way, ensuring that people are informed of when, how, and why their information is shared. Records of processing activities compliant with Article 30 of UK-GDPR will be created and maintained.

To provide world class health and care to the people of Shetland, personal data will be shared, in accordance with the law, with local and wider health and care providers in Scotland. People should feel confident that NHS Shetland shares and processes data in a transparent way that complies with data protection law.

NHS Shetland will keep records of data sharing and processing activities. When sharing information within Scotland and the rest of the United Kingdom, NHS Shetland will use the Scottish Information Sharing Toolkit and the statutory code of practice prepared by the information commissioner's office. We will always consider whether or not data sharing achieves a benefit and is necessary.

Data Protection Impact Assessments (DPIA) will always be carried out even when not legally required, ensuring we embed openness and transparency in processing.

Our commitments:

- We will build and maintain a comprehensive record of processing activities
- We will ensure all data sharing is open and transparent
- Data Sharing Agreements will set out the purpose, process, and standards at each stage

5. Security

Information will only be accessed or modified by authorised people, and regular audits will be used to monitor access. People will be able to update information contained in their records.

The integrity and confidentiality of data is a key principle of UK-GDPR. People have a right to expect appropriate technical and organisational measures to protect their personal data. Access to data must ensure the confidentiality, integrity and availability of systems and services.

Services will comply with Article 5(1)(f) of the UK-GDPR so that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

NHS Shetland will consider the state-of-the-art and the cost of implementation when deciding what measures to take, but it will always be appropriate to the circumstances and risks the data processing poses.

Our commitments:

- We will take ensure information security is regularly reviewed and, where necessary, security measures will be improved
- We will ensure that any data processor we use also implements appropriate technical and organisational measures
- Analysis of risks presented by our processing will be used to identify measures that can be implemented to ensure an appropriate level of security is in place

6. Training

All staff will receive appropriate training starting from induction. Training will be refreshed at the frequency recommended by the data protection regulator.

Our staff are provided with data protection training as an essential part of our mandatory training program. Training reduces the risks to our data and demonstrates a culture compliant with the principles UK-GDPR and the Data Protection Act 2018 (DPA 2018).

Having completed training, staff will be empowered and confident to report anything that might compromise data protection, privacy, and security.

Training will be provided using a range of methods and awareness-raising information will be shared through appropriate communication channels. Everyone who contributes to the health and care of the people of Shetland will understand their information governance responsibilities and what they should do if they believe data protection is being compromised.

Our commitments:

- Training will be provided to all staff starting from induction and refreshed regularly
- Awareness of Information Governance and Security issues will become 'business as usual'
- Additional training will be deployed to health and care partners in Shetland when needed
- NHS Shetland will work with health and care partners at local, regional and national level to build and maintain a people-centred, data and information security culture

7. Incident Management

Awareness of, and learning from, data incidents will be harnessed for the benefit of people, services and to support the secure use of technology.

Staff will be empowered and confident to report anything they think might compromise data protection, privacy, and security.

Incident response plans will be in place and routinely tested. Action will be taken swiftly to manage and report data incidents. Following an incident, processes will be reviewed and amended to reduce the risk of recurrence and to protect the rights and freedoms of individuals.

We understand that incidents can have a range of adverse effects on individuals. These can include emotional distress and physical and material harms. With the exception of a limited number of legal exclusions, we will always inform those involved, directly and without delay, when an incident occurs that is likely to result in a high risk to their rights and freedoms.

Our commitments:

- We will have response plans in place to support swift action following reports of an incident
- We will promote and support learning from incidents and use this to improve processes across health and care services
- Staff will have confidence to challenge behaviours that risk compromising data security
- Risks to data will be anticipated and we take proactive steps to prevent harm to individuals and their data

Subject Access Requests

An individual's right of access to the personal information an organisation holds about them is enshrined in the Data Protection Act 2018. It gives people the right to know how and why we are using their data and obliges NHS Shetland to process their data lawfully, fairly and in a transparent manner.

We will ensure that everyone who accesses health and care services in Shetland can request access to the personal data we hold about them. An individual can make a request verbally and in writing, including via social media.

NHS Shetland will have processes in place across all services to ensure that we can comply with requests within one month or extend the time to respond to two months if the request is complex. NHS Shetland will invest in technology to provide an efficient request and response process to allow timely access to personal information, delivered in a way that meets the requestor's needs and wishes.

We recognise that both patients and staff have a right to request access to the personal data we hold and that personal data can refer to both paper and digital records.

Freedom of Information

NHS Shetland operates in an open and transparent way.

The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EISR) give the public the right to request and (with some legally defined exemptions) receive, copies of information held by public authorities, including NHS Shetland. This could be information about decisions we made, services we provide and how we are spending public money.

Requests must be made in a format which allows them to be stored for later reference, for example, a letter, email, or audio file and not verbal requests. If people need help to make a request, we will provide advice and assistance.

NHS Shetland has adopted the Scottish Information Commissioner's model publication scheme. In keeping with the principles of the scheme, we will increase the amount of information we make publicly available via our website. This will make information available to people without the need to make a request. Where NHS Shetland holds information that is not publicly available, we will respond promptly to FOISA and EISR requests and do so within the timescales set out in legislation. In most cases, this will be within 20 working days.

Shetland has a small population, therefore we may need to answer a request in a way that protects individual identities. In some cases this may mean we need to redact information or mask the number of individuals who have received a particular treatment or diagnosis.

If NHS Shetland does not hold the information requested, or it is exempt from release, we will inform the requester of the exemption we have applied.

Governance

Information governance is an essential component of corporate governance, the structures and processes for decision making, accountability and behaviour at the highest level of an organisation. Good governance in the public sector includes a clear commitment to effective public performance, reporting on the quality of the services being delivered and planning for future service delivery.

Oversight of information governance functions is provided by the Clinical Governance Committee, a standing committee of the Board. Together with the Audit Committee and Staff Governance Committee, these three committees form the full governance framework.

NHS Shetland is committed to the effective governance of its information resources and is working towards ISO27001 accreditation. ISO27001 is an international standard for information governance that places an obligation on Boards and Chief Executives to demonstrate leadership and commitment to information security management by ensuring that information security policies, security objectives and an information security management system (ISMS) are established and supported.

Appendix 1 describes the main roles and responsibilities of those who contribute to NHS Shetland's information governance arrangements. These roles, together with the governance groups they report to (Appendix 2), the policy implementation they oversee (Appendix 3) and the stakeholders they engage (Appendix 4) describe our arrangements for effective information governance.

Legal and strategic alignment

This strategy has been developed in alignment with applicable laws, regulations, standards and strategies. Its purpose is to support improvements in the care and wellbeing of people in Shetland by making safe and effective use of data and digital technologies in the design and delivery of health and care services.

Applicable laws, regulations and standards

(see Appendix 5 for more detail)

- The Data Protection Act 2018
- Data Sharing Code of Practice
- UK General Data Protection Regulation
- Data Protection Principles
- Guide to the UK General Data Protection Regulation (UK-GDPR)
- Scottish Public Sector Cyber Resilience Framework
- Scottish Information Sharing Toolkit
- Public Records (Scotland) Act
- Scottish Government Records Management: Health and Social Care Code of Practice (2020)
- Freedom of Information Legislation
- Caldicott Principles
- Privacy and confidentiality when using the NHS
- Duty of Candour

Scottish Government strategies

- Digital Health and Care Strategy
- Data Strategy for Health and Social Care
- National Information Governance Programme for Health and Care

NHS Shetland strategies

- Clinical Strategy
- Digital Strategy
- Digital Security Strategy
- Communication Strategy

From strategy to delivery

NHS Shetland will use digital technology to improve the lives of the people of Shetland. Digital technology provides opportunities to transform the way we deliver safe, sustainable and

inclusive health and care. We will transform our culture by implementing robust information governance and security measures throughout the lifecycle of our services and projects.

We will ensure this strategy contributes to the overall strategic aims of NHS Shetland by recognising that safe, effect and people-centred care requires us to treat our information resources with the same level of importance as our clinical, care and wellbeing resources.

People in Shetland want and expect their services to be joined up and 'speak' to each other. We will break down the barriers that hinder service integration. We will support the delivery of health and care in traditional settings, such as the Gilbert Bain Hospital, whilst recognising future care will increasingly take place closer to people's homes or in community settings.

This strategy recognises that to deliver the services of the future, we must uphold the rights and freedoms of individuals and place privacy by design and default at the heart of service design.

Our deliverables:

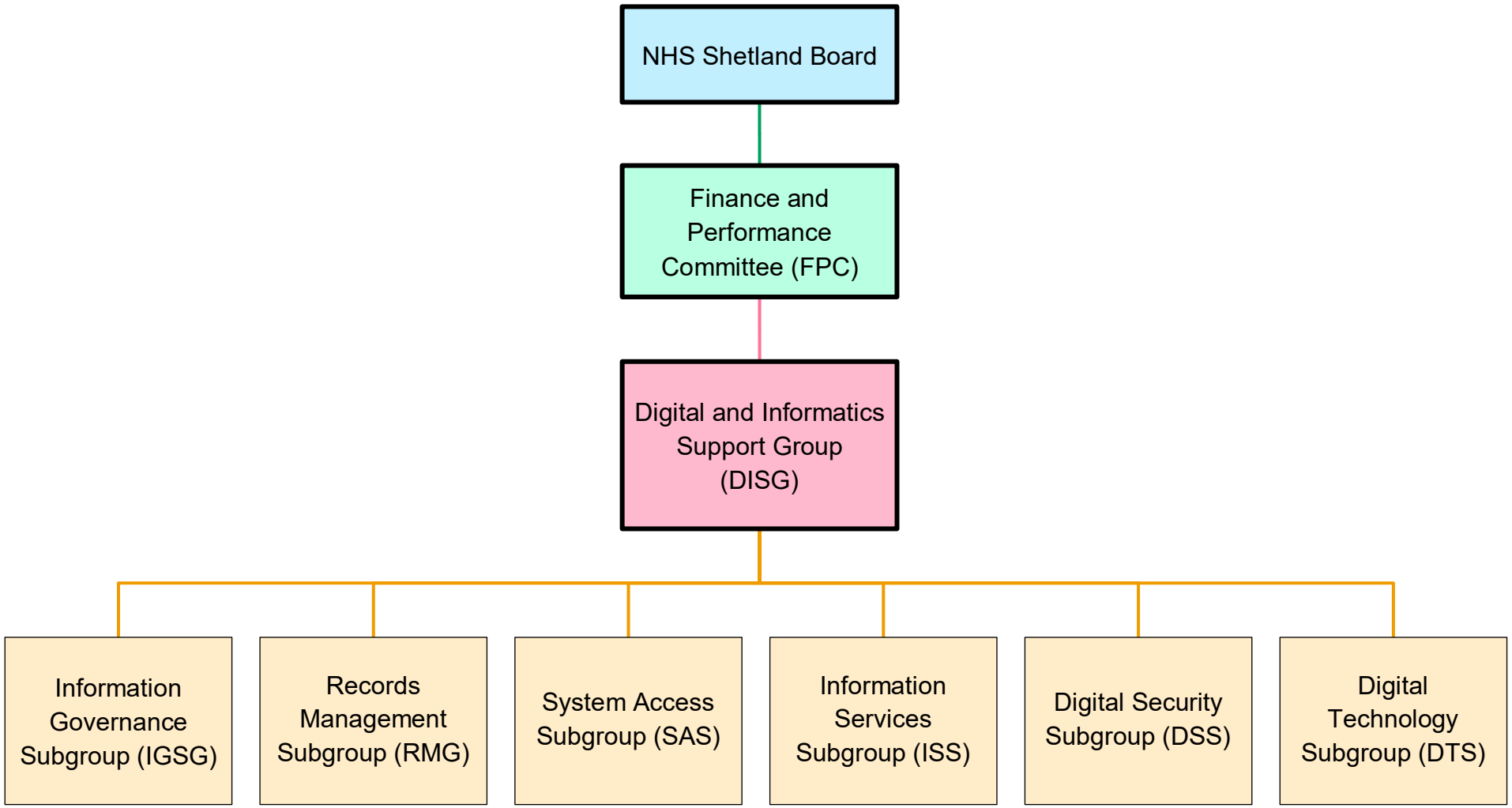
- Information access requests will be identified by each service and logged via OneTrust
- Each processing activity will have a unique privacy notice and information about it will be available on the NHS Shetland website
- Privacy by Design Checklists and DPIAs will be completed for all projects
- Data processors will be asked to provide evidence of their ongoing compliance with UK-GDPR
- Supplier selection will include an assessment of their Information Security and Data Protection measures
- Full records of processing activities across health and care will be established and maintained
- Our staff will be well trained. They will recognise the need for, and be able to initiate, appropriate operational data security measures.
- Our Records Management Plan will be 'Agreed' by the Keeper
- Our Publication Scheme will be 'Approved' by the Scottish Information Commissioner

Appendix 1 Information Governance roles and responsibilities

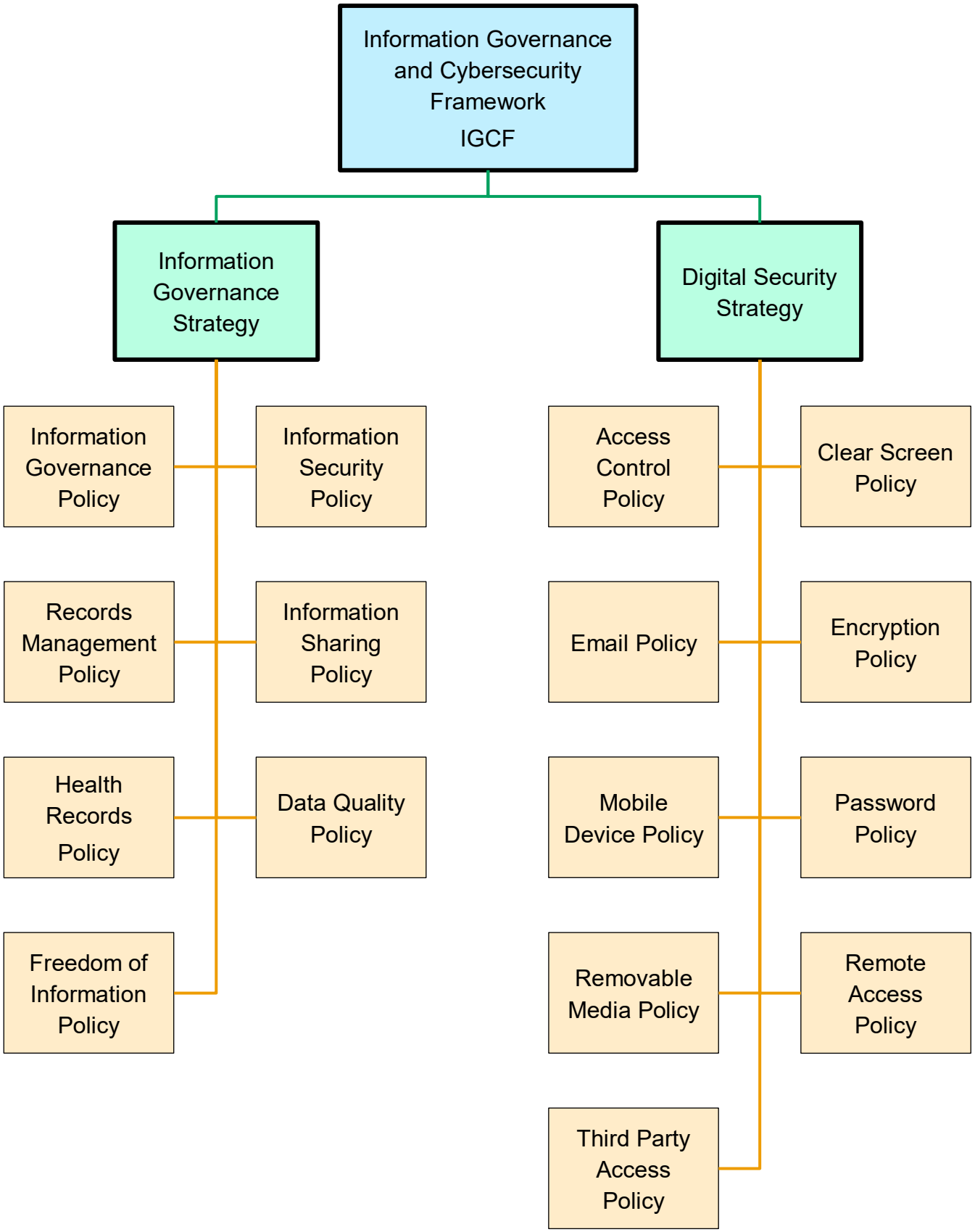
Role	Role Holder	Description
Accountable Officer	Chief Executive Officer	The CEO of NHS Shetland has overall accountability for Information Governance. As Accountable Officer, the CEO is accountable for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery.
Senior Information Risk Owner (SIRO)	Director of Finance	The SIRO acts as a champion for information risk on the Board and provides written advice to the Accountable Officer on the content of the Organisation's Statement of Internal Control regarding information risk. The SIRO will implement and lead the NHS Information Governance risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation.
Caldicott Guardian (CG)	Medical Director	The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. When making decisions or giving guidance, the Caldicott Guardian will refer to the Caldicott principles. The Caldicott Guardian has a key role in ensuring that NHS Shetland satisfies the highest practical standards for handling personal data.
Data Protection Officer (DPO)	Head of Information Governance	Monitors internal compliance, informs, and advises NHS Shetland on its data protection obligations. Provides advice regarding Data Protection Impact Assessments and acts as a contact point for data subjects and the Information Commissioners Office. The Data Protection Officer is an independent expert in data protection who reports to the Executive Management Team and NHS Shetland Board.

Role	Role Holder	Description
Information Security Officer (ISO)	Head of Information and Digital Technology	The Information Security Officer designs and enforces policies and procedures that protect NHS Shetland's critical infrastructure from all forms of security breaches. The ISO identifies vulnerabilities and works with subject matter experts to resolve them, ensuring that our network infrastructure, applications, and data remains secure.
Executive Management Team (EMT)	Executive Management Team members	EMT members are familiar with this strategy and associated policies and demonstrate the application of these through service design and delivery. All EMT members have completed information governance and security training and ensure that staff in their area of responsibility have completed training and have awareness of the need to ensure the lawful, secure and effective use of information.
Information Governance Team (IGT)	Information Governance Manager Records Manager Information Governance Officers	The IGT monitor compliance with NHS Scotland Information Governance Standards and applicable legislation and regulations, including: Public Records (Scotland) Act, UK-GPDR, Freedom of Information (Scotland) Act and Environmental Information (Scotland) Regulations. The IGT provides subject matter expert support to NHS Shetland and its partners.

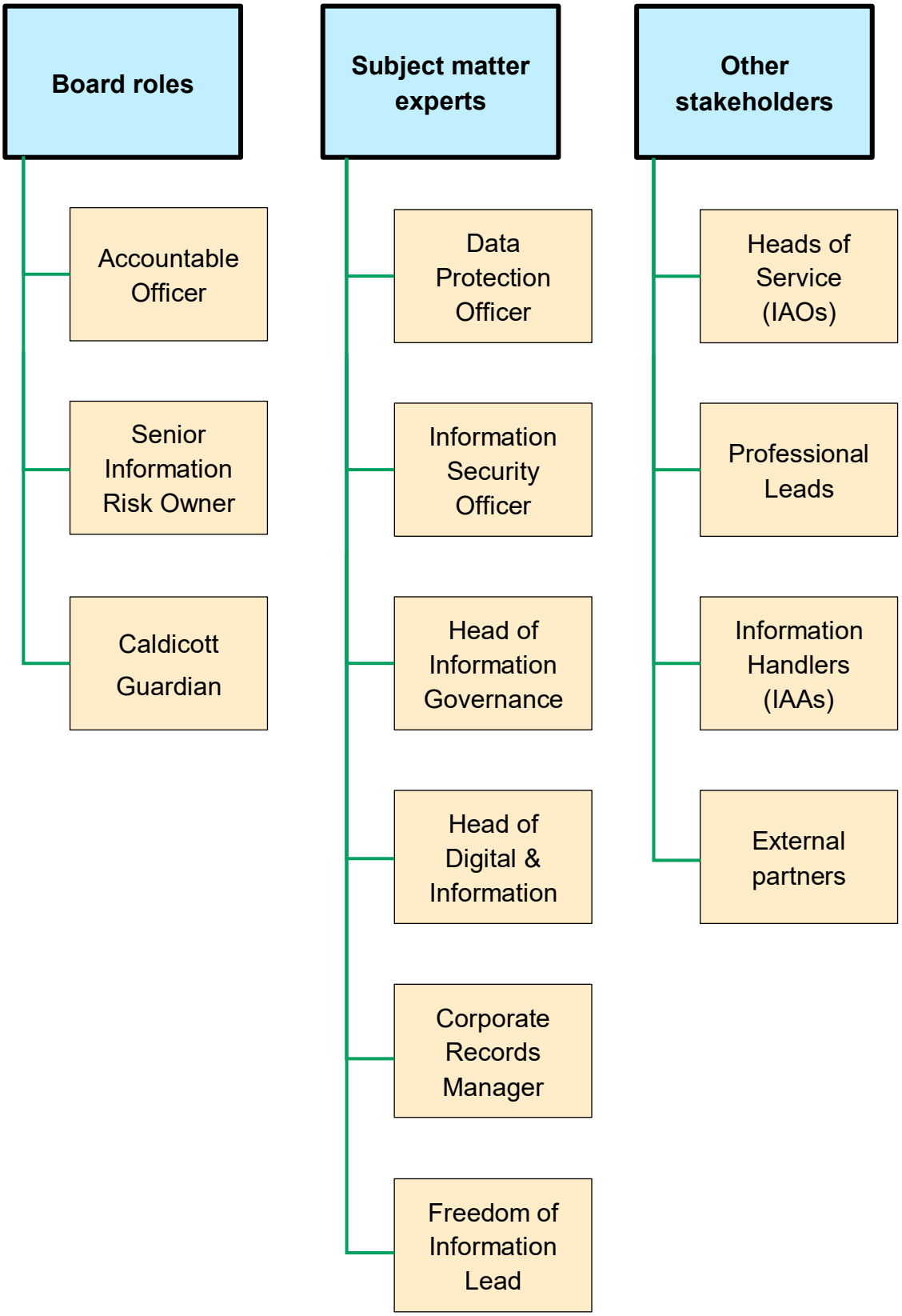
Appendix 2 NHS Shetland Information and Digital Technology Governance structure



Appendix 3 NHS Shetland Policy Framework



Appendix 4 NHS Shetland Information Governance stakeholders



Appendix 5 Applicable laws, regulations and standards

The Data Protection Act 2018

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK-GDPR, for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

The 'applied GDPR' provisions (that were part of Part 2 Chapter 3) enacted in 2018 were removed with effect from 1 Jan 2021 and are no longer relevant. The processing of manual unstructured data and processing for national security purposes now fall under the scope of the UK-GDPR regime.

Data Sharing Code of Practice

This is a statutory code of practice prepared under section 121 of the Data Protection Act 2018.

It is a practical guide for organisations about how to share personal data in a way that complies with data protection law. It aims to give organisations confidence to share data fairly and proportionately.

In accordance with section 127 of the DPA 2018, the Commissioner must take the code into account when considering whether an organisation has complied with its data protection obligations when sharing data. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the UK-GDPR or the DPA 2018 and in the use of their enforcement powers.

The code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.

UK General Data Protection Regulation

The UK-GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

Overseas data collected before 1 January 2021 (referred to as 'legacy data'), is subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). In the short term, there is unlikely to be any significant change between the frozen GDPR and the UK-GDPR.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025.

Data Protection Principles

The UK-GDPR sets out seven key principles for the processing of personal information:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Everyone responsible for using personal data must abide by these principles.

Guide to the UK General Data Protection Regulation (UK-GDPR)

The Guide to the UK-GDPR is for Data Protection Officers (DPOs) and others who have day-to-day responsibility for data protection.

It explains the general data protection regime that applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK-GDPR), tailored by the Data Protection Act 2018.

It explains each of the data protection principles, rights and obligations. It summarises the key points, answers frequently asked questions, and contains practical checklists to help with compliance.

Where relevant, the guide also links to more detailed guidance and other resources, including ICO guidance and statutory ICO codes of practice. Links to relevant guidance published by the European Data Protection Board (EDPB) are also included for reference purposes.

Scottish Public Sector Cyber Resilience Framework

Provides a common, effective way for Scottish public sector organisations to assess their cyber resilience arrangements, identify areas of strength and weakness, gain reasonable confidence that they are adhering to minimum cyber resilience requirements, and take decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.

Scottish Information Sharing Toolkit

The toolkit is part of a framework that applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector and who provide services involving the health, education, safety, crime prevention and social wellbeing of people in Scotland. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

Public Records (Scotland) Act 2011

The Act obliges Public authorities to prepare and implement a records management plan (RMP) which sets out proper arrangements for the management of their records. RMPs are agreed with the Keeper and must be regularly reviewed. Where authorities fail to meet their obligations under the Act, the Keeper has powers to undertake records management reviews and issue action notices for improvement.

Scottish Government Records Management: Health and Social Care Code of Practice (2020)

This updated version takes into account many changes in legislation and best practice since 2012, including the UK-GDPR and the Data Protection Act 2018, and changes in records management practice across various specialities.

It aims to improve compliance and consistency across the variety of organisations within health and care, particularly from the citizen's perspective, and the evolution of traditional "health records" into wider "health and care" records and the increasing use of digital records.

Freedom of Information Legislation

The Freedom of Information (Scotland) Act 2002 is an Act of the Scottish Parliament which gives everyone the right to ask for any information held by a Scottish public authority.

The Environmental Information (Scotland) Regulations 2004 (the EIRs) give everyone the right to ask for environmental information held by a Scottish public authority (and some other bodies).

Caldicott Principles

Caldicott Guardians share a common function, which is to make wise decisions about the use of people's information. They balance the need to protect people's confidentiality with the need to protect their welfare by ensuring that information is safely communicated among the various professional teams caring for an individual, sometimes across organisational boundaries. They bring to bear ethical as well as legal considerations, making judgements about real life human situations that could not be done by a machine.

The Manual for Caldicott Guardians describes a set of principles that are accepted across the UK, however it is important to note there are differences in how they apply because of Scotland's different legal system and the devolution of health provision.

Privacy and confidentiality when using the NHS

All health and care staff have an ethical and legal duty to keep patient information confidential. The Charter of Patient Rights and Responsibilities summaries the standards of privacy and confidentiality that must be maintained by all staff who work in, or are under contract to, the NHS in Scotland. The standards should be read alongside the codes of practice or conduct of the staff member's regulatory body (if applicable) and the policies and procedures of their employing organisation.

Duty of Candour

The Duty of Candour Procedure (Scotland) Regulations 2018, came into force on 1 April 2018. The regulations were made in accordance with the powers available to Scottish Ministers set out in the Health (Tobacco, Nicotine etc. and Care) (Scotland) Act 2016.

The purpose of the duty of candour legislation is to ensure that organisations tell those affected that an unintended or unexpected incident has occurred; apologise; involve them in meetings about the incident; review what happened with a view to identifying areas for improvement; and learn (taking account of the views of relevant persons).

Appendix 6 Information Governance Strategy on a Page

Information Governance in Action

Our vision

To establish and maintain sector-leading information governance standards in the design and delivery of remote and rural health and care services that put people first.

Our priorities

- **Privacy by Design** – will be the default approach for all services & technology. We will use 'state of the art' technology and infrastructure to develop and deliver services.
- **Availability** – records will be maintained in accordance with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 and the right information is available to the right people, in the right place and at the right time.
- **Access** – People will have access to information, their own data, and the digital tools they need to support their health and wellbeing. Information will be accessible to authorised people in all health and care settings.
- **Sharing and processing** – Information sharing will be undertaken in an open and transparent way, ensuring that people are informed of when, how, and why their information is shared. Records of processing activities, compliant with Article 30 of UK-GDPR, will be created and maintained.
- **Security** – Information will only be accessed or modified by authorised people, and audits will be place to monitor access. People will be able to update information contained in their records.
- **Training** – All staff will receive Information Governance & Security training at induction. Training will be refreshed at the frequency recommended by the data protection regulator.
- **Incident management** – Awareness of, and learning from, incidents will be harnessed for the benefit of people, services and to support the secure use of technology.

Our deliverables

- ✓ Information access requests will be identified by each service and logged via OneTrust
- ✓ Each processing activity will have a privacy notice and it will be available on the NHS Shetland website
- ✓ Privacy by Design Checklists and DPIAs will be completed for all projects
- ✓ Data processors will be asked to provide evidence of their ongoing compliance with UK-GDPR
- ✓ Supplier selection will include an assessment of their Information Security and Data Protection measures
- ✓ Full records of processing activities across health and care will be established and maintained
- ✓ Our staff will be well trained and be able to initiate appropriate data security measures
- ✓ Our Records Management Plan will be 'Agreed' by the Keeper
- ✓ Our Publication Scheme will be 'Approved' by the Scottish Information Commissioner

NHS Shetland

Our commitments

- Data protection is at the heart of the design and implementation of systems, services, and business practices
- Information we provide is in 'plain language' so people can understand how we are using their data
- Information supporting health and care delivery is available where and when it is needed
- Information is complete, accurate and up to date
- People have secure access to their records wherever and whenever they request it
- We have and maintain a comprehensive record of processing activities
- All data sharing is open and transparent
- Information security is regularly reviewed and, where necessary, security is improved.
- Training is provided to all staff at Induction and refreshed every eighteen months.
- We work with health and care partners at local, regional and national level to build and maintain a people-centred, data and information security culture.
- Response plans are in place to support swift action following reports of an incident.
- Learning from incidents is used to improve processes across health and care services.
- Staff have confidence to challenge anything that risks compromising the privacy and security of information.

Appendix 7 Equality and Diversity Impact Assessment

Rapid Impact Checklist

An Equality and Diversity Impact Assessment Tool:

<table>
<tr><td colspan="2">Which groups of the population do you think will be affected by this proposal?*
Other groups:
• Minority ethnic people (incl. Gypsy/travellers, refugees & asylum seekers)
• Women and men
• People with mental health problems
• People in religious/faith groups
• Older people, children and young people
• People of low income
• Homeless people
• Disabled people
• People involved in criminal justice system
• Staff
• Lesbian, gay, bisexual and transgender
No population group or groups will be adversely affected by the Information Governance Strategy.</td></tr>
<tr><td colspan="2">*the word proposal is used as shorthand for the policy, procedure, strategy or proposal that is being be assessed</td></tr>
<tr><td>What positive and negative impacts do you think there may be?</td><td>The Information Governance Strategy will have a positive impact on individual privacy and data protection rights for patients and staff.</td></tr>
<tr><td>Which specific groups will be affected by impacts?</td><td>All population groups.</td></tr>
<tr><td>What impact will the proposal have on lifestyles?
For example, will the changes affect:
• Diet and nutrition
• Exercise and physical activity
• Substance use: tobacco, alcohol and drugs
• Risk taking behaviour
• Education and learning or skills</td><td>The Information Governance Strategy will not have an impact on individual lifestyles.</td></tr>
</table>

Will the proposal have any impact on the social environment? Things that might be affected include: • Social status • Employment (paid or unpaid) • Social/Family support • Stress • Income	The Information Governance Strategy will not have an impact on the social environment.
Will the proposal have any impact on the following? • Discrimination? • Equality of opportunity? • Relations between groups?	The Information Governance Strategy will not give rise to discrimination, reduce equality of opportunity or adversely affect relations between groups.
Will the proposal have an impact on the physical environment? For example, will there be impacts on: • Living conditions? • Working conditions? • Pollution or climate change? • Accidental injuries or public safety? • Transmission of infectious disease?	The Information Governance Strategy will not have an adverse impact on the physical environment.
Will the proposal affect access to and experience of services? For example: • Health care • Transport • Social services • Housing services • Education	The Information Governance Strategy will support the introduction of digital technologies that can have a positive impact on individual access to, and experience of, health and care services.

Summary Sheet

Positive Impacts (Note the groups affected)	**Negative Impacts (Note the groups affected)**
• Staff – the strategy will support staff with their legal obligations and professional responsibilities in respect of data protection legislation and duty of confidentiality. • Patients - the strategy will support improved patient access to their health and care information and in the exercise of their data protection rights. • NHS Shetland – the Strategy will support the Board and Senior Managers with legal compliance and good governance.	
Additional Information and Evidence Required None	
Recommendations None	
From the outcome of the RIC, have negative impacts been identified for race or other equality groups? Has a full EQIA process been recommended? If not, why not? No negative impacts have been identified for race or other equality groups therefore a full EQIA process is not required.	