Information Governance Policy

Approval date:	**3 March 2026**
Version number:	**1.0**
Author:	**Sam Collier-Sewell, Head of IG, FOI Lead and DPO**
Review date:	**3 March 2029**
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: FIPOL008

NHS Shetland Document Development Coversheet*

Name of document	Information Governance Policy		
Document reference number	FIPOL008	**New or Review?**	New
Author	Sam Collier-Sewell, Head of IG, FOI Lead and DPO		
Information Asset Owner	Sam Collier-Sewell, Head of IG, FOI Lead and DPO		
Executive lead	Colin Marsland, Director of Finance and SIRO		
Review date	3 March 2029		
Security classification	OFFICIAL – Green: unclassified information		

Proposed groups to present document to:		
IGG	DGG	FPC

Date	**Version**	**Group**	**Reason**	**Outcome**
13/01/2026	0.1	IGG	PI	PRO
03/03/2026	0.2	FPC	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
30/12/2025	Rewrite of IG Policy – marked as new given the extent of changes. Saved as version 0.1
09/02/2026	Minor changes following review by IGG. Completed RIC. Saved as version 0.2

Contents

1. Introduction

NHS Shetland recognises that high-quality information is essential to deliver safe, effective, person-centred health and care services. Information governance provides the framework for handling information lawfully, securely, efficiently and effectively, enabling NHS Shetland to deliver the best possible care whilst respecting individuals' rights to privacy and confidentiality.

This policy establishes NHS Shetland's commitment to maintaining sector-leading information governance standards in the design and delivery of health and care services. It sets out the overarching principles and framework for managing information throughout its lifecycle, from creation to disposal, ensuring that information is always available, always accessible and always secure.

The Board recognises that effective information governance requires an appropriate balance between openness and confidentiality, supporting both transparency and accountability whilst safeguarding personal information about patients and staff and protecting commercially sensitive information. This policy demonstrates NHS Shetland's commitment to corporate governance, clinical governance and information governance principles.

2. Purpose and scope

2.1. Purpose

This policy provides the strategic framework for information governance across NHS Shetland. It establishes the Board's approach to managing information assets, sets out governance structures and accountabilities, and provides the foundation for the suite of operational policies that support day-to-day information management.

The policy aims to ensure that NHS Shetland:

- Handles all information in accordance with legal, regulatory and ethical requirements
- Protects the confidentiality, integrity and availability of information assets
- Enables appropriate access to and sharing of information to support safe, effective care
- Maintains public trust through transparent and accountable information practices
- Embeds information governance principles in service design and delivery
- Supports staff to fulfil their information governance responsibilities
- Manages information risks effectively

2.2. Scope

This policy applies to all information held, processed or managed by NHS Shetland, regardless of format (paper, electronic, audio, video, etc.) or location. It applies to both clinical and corporate information, including but not limited to:

- Patient health records and care information
- Staff personal information and employment records
- Financial, procurement and commercial information
- Governance, quality and performance information

- Research and innovation information
- Estates, facilities and infrastructure information
- Communications and correspondence

The policy applies to all individuals who access, use or manage NHS Shetland information, including:

- All directly employed staff (permanent, fixed-term, bank, temporary)
- Contractors, agency staff and locum workers
- Students, trainees and volunteers
- Third-party service providers and processors
- Partner organisations working on behalf of NHS Shetland
- Independent practitioners with access to NHS Shetland systems

3. Definitions

Information Governance: The framework of policies, procedures, standards and accountabilities that ensures information is handled lawfully, securely, efficiently and effectively.

Information Asset: A defined body of information, managed as a single unit, that can be understood, shared, protected and exploited effectively. Information assets include databases, data sets, records, files and physical documents.

Information Asset Owner (IAO): An individual accountable for ensuring that specific information assets are handled and managed appropriately, including identifying and managing risks to the asset.

Personal Data: Any information relating to an identified or identifiable living individual (a data subject). This includes names, identification numbers, location data, online identifiers and information about a person's physical, physiological, genetic, mental, economic, cultural or social characteristics.

Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation. This data requires additional protections under data protection law.

Data Controller: The organisation that determines the purposes and means of processing personal data. NHS Shetland is a data controller for information it processes.

Data Processor: An organisation that processes personal data on behalf of a data controller. Processors must be carefully selected and contracted.

Processing: Any operation performed with someone’s personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

Information Security: The preservation of confidentiality, integrity and availability of information, along with other properties such as authenticity, accountability, non-repudiation and reliability.

Privacy by Design: An approach to systems design and operation that embeds privacy and data protection considerations throughout the entire lifecycle of technologies, processes and services.

Privacy by Default: Ensuring that personal data is processed with the highest privacy protection as standard, so that by default, only necessary personal data is processed and personal data is not made publicly/widely accessible.

Data Protection Impact Assessment (DPIA): A systematic process to identify and minimise data protection risks in new projects or systems. DPIAs are legally required under UK-GDPR for any processing that is likely to result in high risk to individuals' rights and freedoms. This includes most processing of health data and special category data. DPIAs must be conducted before commencing any such high-risk processing.

Information Governance Incident: Any event that could have, or did, compromise the confidentiality, integrity or availability of information, including actual or suspected breaches of policy, loss or theft of devices, unauthorised access or disclosure, ransomware attacks or system failures.

4. Legal and regulatory framework

NHS Shetland's information governance arrangements are developed and maintained in compliance with a comprehensive legal and regulatory framework. Key legislation and regulations include:

4.1. Primary legislation and regulations

- Data Protection Act 2018 and UK General Data Protection Regulation (UK-GDPR)
- Data (Use and Access) Act 2025
- Public Records (Scotland) Act 2011
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- Human Rights Act 1998
- Computer Misuse Act 1990
- Network and Information Systems Regulations 2018
- Adults with Incapacity (Scotland) Act 2000
- Age of Legal Capacity (Scotland) Act 1991
- National Health Service (Scotland) Act 1978
- Public Services Reform (Scotland) Act 2010
- Equality Act 2010

4.2. Common law and professional obligations

- Common law duty of confidentiality
- Duty of Candour

- Professional codes of conduct
- NHS Scotland Code of Practice on Protecting Patient Confidentiality

4.3. Standards and codes of practice

- Records Management: NHS Scotland Code of Practice (2024)
- Section 60 Code of Practice (Freedom of Information)
- Section 61 Code of Practice (Records Management under FOISA)
- ICO Data Sharing Code of Practice
- ICO Employment Practices Code
- Caldicott Principles
- ISO/IEC 27001 (Information Security Management)
- ISO 15489 (Records Management)
- BS 10008 (Evidential weight and legal admissibility of electronic information)
- Cyber Essentials and Cyber Essentials Plus
- Scottish Public Sector Cyber Resilience Framework

4.4. National and regional strategies and guidance

- Scottish Government Digital Health and Care Strategy (and associated annual delivery plans)
- Scottish Government Data Strategy for Health and Social Care
- National Information Governance Plan for Health and Care
- NHS Scotland Information Governance Standards
- Scottish Information Sharing Toolkit
- Spending time where it counts: An Artificial Intelligence Strategy for Health & Social Care in the North of Scotland 2024-2027

4.5. NHS Shetland strategic alignment

This policy is developed in support of, and is aligned with:

- NHS Shetland Information Governance Strategy 2022-2027
- NHS Shetland Clinical and Care Strategy 2021-2031
- NHS Shetland Strategic Delivery Plan 2024-2029
- NHS Shetland Digital Strategy and Delivery Plan 2024-2029

5. Roles and responsibilities

Effective information governance requires clear accountabilities at all levels of the organisation.

5.1. NHS Shetland Board

The Board has overall responsibility for governance of the organisation, including information governance. The Board ensures that appropriate structures, policies and resources are in place to manage information effectively and lawfully.

5.2. Chief Executive

The Chief Executive is the Accountable Officer for NHS Shetland.

Accountable for:

- Overall statutory responsibility for ensuring NHS Shetland complies with its legal obligations regarding information management
- Ensuring appropriate governance structures are in place
- Demonstrating leadership and commitment to information governance and information security management

Responsible for:

- Ensuring adequate resources are allocated to information governance
- Reporting significant information governance issues to the Board

5.3. Senior Information Risk Owner (SIRO)

The Director of Finance is designated as the Senior Information Risk Owner.

Accountable for:

- Information risk and incident management framework
- The organisation's information risk policy and information risk register
- Ensuring information risks are identified, assessed and mitigated

Responsible for:

- Leading and fostering a culture that values and protects information
- Providing a focal point for resolution and management of information risk
- Providing oversight of information governance incidents and near misses
- Reporting to the Board on information risk management
- Advising the Chief Executive on information risk
- Identifying Information Asset Owners for all assets and ensuring they understand their responsibilities
- Oversight and prioritisation of information governance activities

5.4. Caldicott Guardian

The Medical Director is designated as the Caldicott Guardian. The Caldicott Guardian's role is advisory in nature, acting as the 'conscience' of the organisation for patient confidentiality matters.

Responsible for:

- Safeguarding the confidentiality of patient information
- Ensuring compliance with the principles contained within the NHS Scotland Code of Practice on Protecting Patient Confidentiality
- Ensuring staff are made aware of individual responsibilities regarding confidentiality through policy, procedure and training
- Providing routine reports to senior management on confidentiality and data protection issues
- Enabling appropriate information sharing in accordance with Caldicott principles
- Representing and championing confidentiality and information sharing requirements
- Providing strategic leadership and advice on all matters relating to patient confidentiality
- Reviewing and approving information sharing arrangements involving patient data
- Supporting the organisation to apply the common law duty of confidentiality
- Identifying and addressing any barriers to appropriate information sharing for care
- Ensuring the confidentiality and data protection work programme is successfully coordinated and implemented

5.5. Head of Information Governance

Responsible for:

- Leading and managing the Information Governance Department
- Providing strategic advice to the SIRO, Board and senior management on information governance matters
- Oversight of information governance performance and compliance
- Escalating significant information governance risks and issues

5.6. Data Protection Officer (DPO)

The Head of Information Governance is designated as the Data Protection Officer.

Responsible for:

- Monitoring compliance with UK-GDPR and Data Protection Act 2018
- Advising on data protection obligations and best practice
- Conducting or overseeing Data Protection Impact Assessments
- Acting as point of contact for the Information Commissioner's Office
- Cooperating with supervisory authorities
- Advising on privacy by design and privacy by default
- Maintaining awareness of data protection developments
- Providing training and raising awareness of data protection

- Managing and investigating data protection complaints and breaches

Note: The DPO monitors and advises on compliance. Accountability for achieving and maintaining compliance sits with the Board and Chief Executive as data controller.

5.7. Executive Directors and Senior Managers

Responsible for:

- Embedding information governance into service delivery and decision-making
- Ensuring staff within their areas understand and comply with information governance policies
- Identifying and managing information governance risks within their areas
- Allocating sufficient resources for information governance activities
- Supporting a culture that values and protects information
- Ensuring information governance is considered in service redesign and digital transformation
- Promoting privacy by design and privacy by default in all new initiatives

Information Asset Owner (IAO) role

Executive Directors and senior managers are designated as Information Asset Owners for specific information assets within their areas of responsibility.

Accountable to the SIRO for:

- Ensuring information risks are managed effectively for the information assets within their remit
- Understanding what information assets they own and why they are valuable
- Understanding and addressing risks to the confidentiality, integrity and availability of information assets

Responsible for:

- Ensuring information assets are appropriately classified and protected
- Ensuring compliance with legal and policy requirements for their information assets
- Making decisions about access to and sharing of their information assets
- Ensuring appropriate retention and disposal of information assets
- Reporting information governance incidents relating to their assets
- Providing assurance to the SIRO on information asset management

5.8. Information Governance Department

The Information Governance Department provides specialist support, advice and guidance on all aspects of information governance.

Responsible for:

- Developing, maintaining and reviewing information governance policies and procedures
- Monitoring compliance with legal and regulatory requirements
- Providing advice and support on data protection, freedom of information, records management and information security
- Conducting Data Protection Impact Assessments and privacy reviews
- Managing information governance incidents and breaches
- Delivering information governance training and awareness programmes
- Maintaining relationships with regulators and external bodies
- Reporting on information governance performance and compliance
- Supporting information asset management
- Coordinating internal and external information governance audits
- Supporting the SIRO, Caldicott Guardian and DPO in the delivery of their responsibilities

5.9. All staff and contractors

Every individual who accesses, uses, or manages NHS Shetland information has a duty to protect and handle it appropriately.

Responsible for:

- Complying with all information governance policies, procedures and guidance
- Handling information lawfully, securely and professionally
- Creating accurate, timely and complete records
- Protecting the confidentiality of personal and sensitive information
- Only accessing information necessary for their role
- Not disclosing information inappropriately
- Using information systems responsibly and in accordance with acceptable use requirements
- Reporting information governance incidents promptly
- Completing mandatory information governance training
- Seeking advice when unsure about information governance requirements

6. Information Governance principles

6.1. Accountability and governance

NHS Shetland maintains clear governance structures for information governance, with defined roles, responsibilities and reporting lines. Oversight is provided by the Finance and Performance Committee (FPC), which reports to the NHS Shetland Board. Operational information governance is managed through the Information Governance Group (IGG).

The Board demonstrates leadership and commitment to information governance by ensuring policies, objectives and an information security management system are established, implemented and maintained. NHS Shetland is committed to effective information security management in line with ISO 27001 standards.

6.2. Privacy by design and privacy by default

NHS Shetland embeds privacy considerations from the outset in all service design, system development and business change activities. Privacy by design and privacy by default are fundamental principles that ensure:

- Data protection is considered throughout the lifecycle of projects and services
- Only necessary personal data is processed
- Personal data is not made accessible without appropriate controls
- Technical and organisational measures are implemented to protect information
- Data Protection Impact Assessments are conducted for high-risk processing

6.3. Lawful and fair processing

NHS Shetland processes information lawfully, fairly and transparently. The Board:

- Identifies and documents appropriate lawful bases for processing personal data
- Provides clear privacy notices explaining how information is used
- Respects individuals' rights under data protection law
- Ensures processing is necessary and proportionate
- Maintains records of processing activities

6.4. Information quality and integrity

NHS Shetland recognises that high-quality information is essential for safe, effective care and sound decision-making. The Board ensures that information is:

- Accurate, complete and up to date
- Created, captured and recorded at the point of care or business activity
- Maintained in accordance with standards and procedures
- Subject to appropriate quality assurance processes
- Validated and verified where appropriate
- Corrected when errors are identified

6.5. Information security

NHS Shetland implements appropriate technical and organisational measures to protect the confidentiality, integrity and availability of information. Security measures are proportionate to the risks and include:

- Access controls and authentication
- Encryption of data in transit and at rest

- Network and perimeter security
- Physical security for devices and paper records
- Secure disposal and destruction
- Business continuity and disaster recovery arrangements
- Regular security testing and monitoring
- Incident detection and response capabilities

More detailed information security requirements are set out in the Information Security Policy.

6.6. Appropriate access and information sharing

NHS Shetland ensures that information is available to those who need it, when they need it, for legitimate purposes. The Board supports appropriate information sharing whilst safeguarding confidentiality by:

- Implementing role-based access controls
- Applying the need-to-know principle
- Following Caldicott principles for patient information
- Establishing formal information sharing agreements where appropriate
- Providing staff with guidance and training on appropriate sharing
- Respecting individuals' rights to object to sharing where applicable

Information sharing arrangements are addressed in the Information Sharing Policy and Data Sharing Framework.

6.7. Records management

NHS Shetland manages all records, in any format, in accordance with legal requirements and best practice throughout their lifecycle. The Board ensures that:

- Records are created to provide evidence of activities and decisions
- Records are maintained securely and can be retrieved when needed
- Records are retained for appropriate periods in accordance with retention schedules
- Records are disposed of securely at the end of their retention period
- Vital records are identified and protected to support business continuity
- Records management arrangements comply with the Public Records (Scotland) Act 2011

Detailed records management requirements are set out in the Records Management Policy and Health Records Policy.

6.8. Subject rights

NHS Shetland respects and facilitates the exercise of individuals' rights under data protection law, including:

- Right of access to personal data (subject access requests)
- Right to rectification of inaccurate data

- Right to erasure in specific circumstances
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights related to automated decision-making

Procedures for responding to individuals exercising their rights are documented in the Subject Access Request Procedure and staff receive appropriate training.

6.9. Transparency and openness

NHS Shetland is committed to transparency and openness in accordance with freedom of information legislation. The Board:

- Operates a publication scheme to proactively publish information
- Responds to information requests within statutory timescales
- Only withholds information where appropriate exemptions or exceptions apply
- Maintains an ethos of openness whilst protecting privacy and confidentiality

Freedom of information arrangements are set out in the Freedom of Information Policy.

6.10. Training and awareness

NHS Shetland ensures that all staff understand their information governance responsibilities through:

- Mandatory information governance training at induction
- Annual refresher training covering key topics
- Specialist training for staff with specific responsibilities
- Regular communications and awareness-raising activities
- Clear, accessible policies and guidance
- Monitoring of training compliance

6.11. Risk management

NHS Shetland identifies, assesses and manages information risks systematically. Information governance risks are:

- Identified through risk assessments, audits and incident reviews
- Recorded in relevant risk registers
- Assessed for likelihood and impact
- Mitigated through appropriate controls
- Monitored and reviewed regularly
- Reported through governance structures

6.12. Incident management

NHS Shetland has robust processes for managing information governance incidents. All actual or suspected incidents must be reported promptly through the organisation's incident reporting system. Incidents are:

- Assessed for severity and impact
- Investigated to determine cause and consequences
- Reported to regulators where required
- Used as opportunities for learning and improvement
- Monitored for trends and patterns

Information governance incidents may result in reporting to the Information Commissioner's Office where there is a breach of data protection law, particularly where there is a risk to individuals' rights and freedoms.

6.13. Monitoring, audit and assurance

NHS Shetland maintains robust arrangements for monitoring, auditing and providing assurance on information governance compliance. These include:

- Regular audits of compliance with policies and procedures
- Monitoring of key performance indicators
- Internal and external audit reviews
- Self-assessment against national standards
- Review of information governance incidents
- Annual reporting to the Board on information governance

6.14. Third-party management

NHS Shetland recognises that third parties may process information on behalf of the Board or may require access to information to deliver services. The Board ensures that:

- Third parties are carefully selected and subjected to due diligence
- Appropriate contracts and data processing agreements are in place
- Third parties comply with information governance requirements
- Regular reviews and audits of third-party compliance are conducted
- Exit arrangements ensure information is returned or securely destroyed

Requirements for third-party information processing are addressed in the Information Security Policy and through data processing agreements.

6.15. Digital transformation and emerging technologies

NHS Shetland recognises that digital transformation and the adoption of new technologies bring both opportunities and challenges for information governance. The Board ensures that:

- Information governance is integral to digital transformation programmes

- New technologies are assessed for privacy and security implications
- Cloud services and SaaS applications meet security and compliance requirements
- Artificial intelligence and automated decision-making systems are ethically deployed
- Remote and mobile working arrangements maintain information security
- Digital collaboration tools are used in accordance with policy

7. Information governance policy framework

This Information Governance Policy is supported by a suite of policies that provide detailed requirements for specific aspects of information management:

- Information Security Policy
- Records Management Policy
- Information Sharing Policy and Data Sharing Framework
- Health Records Policy
- Data Quality Policy
- Freedom of Information Policy

All policies within the information governance framework are developed consistently, reviewed regularly and approved through appropriate governance processes. Staff must comply with all relevant policies.

An information governance policy map showing the relationships between policies is maintained and published on the NHS Shetland intranet.

8. Related documents

This policy should be read in conjunction with:

- NHS Shetland Information Governance Strategy 2022-2027
- IT Acceptable Use Policy
- Email and Communication Policy
- Social Media Policy
- Mobile Device Policy
- Business Continuity Policy
- Incident Reporting and Management Policy

Supporting guidance, procedures and templates are available on the NHS Shetland intranet.

9. Non-compliance

Compliance with this policy is mandatory for all staff and contractors. Failure to comply may result in:

- Disciplinary action in accordance with NHS Scotland conduct policies

- Removal of access to information systems
- Referral to professional regulatory bodies where appropriate
- Civil or criminal liability in cases of serious breach
- Regulatory action by the Information Commissioner's Office or other bodies

All staff should be aware that unauthorised access to, use of, or disclosure of information may constitute:

- A breach of the Data Protection Act 2018 (criminal offence)
- A breach of the Computer Misuse Act 1990 (criminal offence)
- Professional misconduct
- Gross misconduct justifying dismissal

10. Monitoring and review

10.1. Monitoring and reporting

Compliance with this policy is monitored through:

- Information governance incident reports reviewed quarterly
- Key performance indicators reviewed quarterly
- Internal and external audits
- Annual information governance report to the Finance and Performance Committee
- Regular reporting to the Information Governance Group

The Information Governance Department maintains oversight of policy compliance and supports improvement activities.

10.2. Policy review

This policy is reviewed every three years or sooner if:

- There are significant changes to legislation or regulation
- Organisational restructuring affects governance arrangements
- Significant information governance incidents highlight policy gaps
- Internal or external audits identify areas for improvement
- New national guidance or standards are issued

Reviews are conducted by the Information Governance Department in consultation with Information Asset Owners and key stakeholders. Substantive changes require approval by the Finance and Performance Committee.

Appendix 1 – Rapid Impact Checklist

An equality and diversity impact assessment tool:

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 *the word proposal is used as shorthand for the policy, procedure, strategy or proposal that is being be assessed This policy applies to all groups listed. It describes expectations for how information is handled across NHS Shetland and therefore affects anyone whose information is created, used or managed by the organisation, including patients, staff and members of the public. No differential impacts have been identified at this stage.	
In the following sections, please consider what positive and negative impacts you think there may be and which specific groups will be affected by these impacts?	
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	No direct impacts on lifestyle factors have been identified. The policy concerns organisational expectations for managing information and does not change service delivery or care pathways.

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	No direct impacts on the social environment have been identified. The policy sets organisational expectations for information governance and does not alter employment arrangements, social support, or factors that influence income or social status.
Will the proposal have any impact on the following? • Discrimination? • Equality of opportunity? • Relations between groups? • Fairer Scotland Duty	The policy is designed to apply consistently across all staff and service areas and does not introduce any changes that would directly affect equality of opportunity or create differential impacts for specific groups. It supports compliance with equality duties by promoting fair, transparent and accountable handling of information. No negative impacts relating to equality or discrimination have been identified.
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?	No impacts on the physical environment have been identified. The policy does not introduce changes to physical working conditions, facilities, or environmental risk factors. It focuses on the governance of information rather than operational or environmental matters.
Will the proposal affect access to and experience of services? For example: • Health care • Transport • Social services • Housing services • Education	The policy does not directly change access to services. By strengthening organisational expectations for the management of information, it supports consistent, reliable information handling, which may indirectly benefit service users through improved accuracy and availability of information. No negative impacts on access or experience have been identified.

Summary sheet

<table>
<tr><td><b>Positive Impacts (note the groups affected)</b>
The policy promotes consistent, transparent and accountable handling of information across NHS Shetland. This supports confidence in how information is managed, protects individual rights, and contributes to safe and effective service delivery by strengthening organisational expectations for information governance. These impacts apply across all population groups.</td><td><b>Negative Impacts (Note the groups affected)</b>
No negative impacts have been identified. The policy does not introduce changes that would adversely affect any specific group or alter access to services.</td></tr>
<tr><td colspan="2"><b>Additional Information and Evidence Required</b>
No additional evidence is required at this stage. The impacts identified are proportionate to the scope of the policy, which relates to organisational governance rather than service redesign.</td></tr>
<tr><td colspan="2"><b>Recommendations</b>
A full Equality Impact Assessment is not required because the policy does not introduce changes that would differentially affect specific groups or alter access to services.</td></tr>
<tr><td colspan="2"><b>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?</b>
No negative impacts have been identified.
A full Equality Impact Assessment is not required because the policy does not introduce changes that would differentially affect specific groups or alter access to services.</td></tr>
</table>

Signature(s) of Level One Impact Assessor(s): Sam Collier-Sewell, Head of IG, FOI Lead and DPO

Date: 9 February 2026

Signature(s) of Level Two Impact Assessor(s):

Date: