Information Governance Policy

Document Information	
Document Name/Description/Location	Information Governance Policy o:\asoffice\adminser\records management\policies\finals\information governance policy - v03.00.docx
Version Number *e.g. V1.1*	03.00
Author [Name and Post Title]	Anne Cogle Team Leader – Administration
Lead Officer/Manager [Name and Post Title]	Christine Ferguson Director of Corporate Services / Senior Information Risk Owner
Final Approval Date	22 February 2023
Approved by – Council/Committee/Group/Manager	Shetland Islands Council
Review Frequency	5 years
Date of next planned review start	January 2028
Summary of changes to document	

Date	Version updated	New version number	Brief description of changes
06/01/2023	01.2	02.1	Updated draft for consultation prior to agenda management
22/03/2023	02.1	03.00	Final version for publication.

Contents

1.0 Policy Overview

1.1 The aim of this policy is to provide policy statement about the council's approach to the governance of its information. It aims to promote best practice and to link together the suite of policies and procedures which relate to specific aspects of information management.

1.2 The statements in this Policy supports a cohesive approach to managing the vast and diverse volumes of information assets held by the Council, now and for the future. This Policy provides the Council with the basis upon which it can manage its information assets, to ensure that the Council has data, information and knowledge, which is:

- **Useable**: information will be accurate, up to date, and fit for purpose. The Council will have the information it needs.

- **Accessible**: information will be in the right place, organised appropriately, open wherever possible, protected where required. The Council will have the information it needs, where it needs it.

- **Reliable**: the Council will have access to the information it needs, where it needs it, whenever it needs it and that appropriate business continuity arrangements are in place to protect it.

2.0 Scope

2.1 The Council defines its Information Assets as all data, information and knowledge generated, sent, received or used by it in the undertaking of its functions – whether it be delivering its services, formulating policy, holding meetings, managing budgets or monitoring projects. These Information Assets come in a variety of formats including paper records, electronic mail, spreadsheets, and data in business systems, audio and video recordings and web pages, which are held within a variety of manual and electronic systems. The Council recognises the value of these assets and the importance placed on their proper management throughout their lifecycle as a vital corporate function.

2.2 All employees of Shetland Islands Council (SIC) need information every day in order to do their jobs – the Council cannot function or meet its objectives without it. This Policy is not just for those working on or assigned information management roles, it is for all Council staff, for every role, at every grade, in every part of the Council. It outlines what 'we' as a Council need to do in order to manage our information in a confident and transparent way.

2.3 The Information Governance Policy also supports those Council staff who provide statutory functions on behalf of the Shetland Islands Area Licensing Board, and the Shetland Transport Partnership [ZetTrans] who do not directly employ any staff. The Policy also supports those who provide services on

behalf of the Council under contract or agreement, such as service delivery partners and third party contractors.

3.0   Legislative Context

3.1   The Council, its staff and representatives, have a duty to be compliant with legislation in relation to information management. This legislation includes, but is not exclusively;

- Computer Misuse Act 1990 (CMA 1990)
- Data Protection Act 2018 (DPA 2018)
- Environmental Information (Scotland) Regulations 2004 (EIR 2004)
- Freedom of Information (Scotland) Act 2002 (FOISA 2002)
- INSPIRE (Scotland) Regulations 2009 (INSPIRE)
- Local Government (Scotland) Act 1994 (LGSA 1994)
- Public Records (Scotland) Act 2011 (PRA 2011)
- Re-use of Public Sector Information Regulations 2015 (RPSI 2015)

3.2   All staff have a responsibility to be compliant with the law to reduce the risk to the Council's reputation and subsequent monetary fines.

4.0   Governance and Accountability Management Structure

4.1   The Governance and Accountability Management Structure – Appendix 1 - illustrates those specific job roles that have particular responsibilities, as outlined in detail below:

Senior Information Risk Owner (SIRO)
The Council has designated this role to the Director of Corporate Services, who is responsible for the corporate monitoring and implementation of an Information Management Improvement Programme; managing the risks and assurance measures, maturity level targets and reporting regularly to CMT on the effectiveness of this programme of work and alerting to issues of non-compliance.   The SIRO also acts for the Council as Data Controller, and determines the purposes for which, and the manner in which, any personal data are, or are to be, processed, and has overall responsibility for ensuring the Council's compliance with the Data Protection Act 2018.   The SIRO is also the Council's named officer for the statutory functions and obligations of the Council under all current legislation relating to Freedom of Information, Regulation of Investigatory Powers, and any other relevant legislation or statutory guidance relating to records management, including the Public Records (Scotland) Act 2011.

Monitoring Officer
The Council's Scheme of Administration and Delegations has designated this role to the Chief Legal Officer [Executive Manager – Governance and Law], who is responsible for monitoring any proposal, decision, or omission by the Council, Committee, Sub Committee or Officer that contravenes any legislation or Code of Practice. The Monitoring Officer will inform and advise

the SIRO of any issues regarding compliance with the Freedom of Information (Scotland) Act 2002, or the Public Records (Scotland) Act 2011.

Data Protection Officer
The Chief Legal Officer [Executive Manager – Governance and Law], is also the current designated Data Protection Officer. The Data Protection Officer must inform and advise the Data Controller [the Council] of its obligations under the Data Protection Act 2018, and monitor the implementation and application of the Council's policies and training on personal information management.

Senior Information Asset Owners [Directors]
The authorising person within a Directorate responsible for ensuring information management and improvement targets are implemented and adopted by staff and for the assets within their Departments and Services. They are also the owners of Information Management Risks and for ensuring that the risks are managed in accordance with Council policy and practice.

Information Asset Owners [Executive Managers]
Information Asset Owners are responsible for ensuring information management policies and procedures are followed, recognising actual or potential security incidents, consulting their Senior Information Risk Owner on incident management, and ensuring that information asset registers are accurate and up to date and that appropriate monitoring and reporting is in place.

Records Manager
In support of senior management responsibilities, operational day-to-day information management functions are delegated to the Records Manager [Team Leader – Administration], who is required to promote, monitor and manage the effective control of the Council's records in relation to service and departmental procedures and practice, and ensure corporate wide compliance with the Records Management Plan and associated requirements under the Public Records (Scotland) Act 2011. The Records Manager is the Council's initial point of contact for any Records Management issues.

Information Asset Administrators [Business Support/Admin Teams]
Responsible as part of each Directorate's Business Support for ensuring information management practice and policies are followed by all staff, providing frontline support to Directorate staff to adhere to all information management requirements [Records Management, FOISA and Data Protection] and identifying any issues to their Information Asset Owners.

Information Governance Board
Responsible for ensuring that the Council develops the governance, accountability and strategic direction of all corporate information asset management now and in the future, and that the Information Management Improvement Programme aligns with other relevant strategies, projects and work streams. The terms of reference for the Board is attached as Appendix 2.

6.0   Policy Statements

6.1   Governance and Risk
We will maintain a proactive, planned, and proportionate approach to managing all council information using an approved maturity model which identifies assurance measures that will reduce risk, increase performance and provide the controls and measures where all information management disciplines are compliant. We will be confident and efficient to managing risk, that this is appropriate and balanced with our business needs, enabling staff to do their jobs whilst safeguarding information.

6.2   Information and Records Lifecycle Management
We will provide staff with the right tools and knowledge for managing all information and records throughout their lifecycle, so that all staff know what information is available to them, why it is being held, where it is stored, who has access to it and for how long it should be retained. This will include aligning all management of our records and information with a Corporate Business Classification Scheme and Records Retention Schedule. We will find effective solutions for managing our information and records in all formats, avoiding unnecessary duplication and inefficient dependencies. This will increase the use of shared corporate repositories enabling quicker responses to requests for information, and improving what we publish, demonstrating our commitment to openness and transparency.

6.3   Information Preservation
We will we have clear and consistent, policy and procedures for identifying when council information requires to be transferred and preserved permanently, based on the completeness of the archive record and not the medium in which it is held. We will make sure that we secure this information for future generations by working toward compliance with relevant standards for the storage and curation of both physical and digital archival materials.

6.4   Information Security and Systems Management
We will work to ensure that our information management and information technology requirements are aligned and that information management needs are a key factor in the making of decisions in relation to information technology. This will encompass the business specification and design of new systems, the implementation and management of systems; the management of legacy systems and data migration; and the secure disposal of information and IT equipment. New approaches to technology will have implications for how we manage and protect our information. In working to address these, we must focus on the information and content within systems, the physical and virtual spaces these are held, and not the technology alone.

6.5   Business Continuity and Disaster Recovery
We will ensure that vital information is identified in all Business Continuity and Disaster Recovery Plans, and that such information is appropriately stored

and is accessible. This will ensure that vital information is both suitably protected and readily accessible even in times of crisis.

6.6   Culture and Training

We will work to create an environment where information management skills are recognised and valued in the same way that management, communication, project management and financial skills are; where good information management skills are seen as core skills required by all council staff; and work towards recognising information management skills and behaviours in the performance management process. Similarly, poor information management skills or behaviours will be monitored and training needs identified.

6.7   Knowledge, Re-use and Performance

We will work to ensure that we have the right framework and tools in place to capture and marshal organisational knowledge. Information and knowledge are key corporate assets and we all have a responsibility to share and re-use them to release their value and maximise benefits to the business and the public. Data held by us should be open to re-use unless there is a good reason not to. It is essential that we communicate to staff that the protection and sharing of information are not opposing principles. We will work to ensure that the organisation has accurate and good quality information to support both intelligent decision-making and performance improvement.

Separate policies and procedures that set out responsibilities, guidelines and best practice should be followed to minimise unauthorised use, modification, destruction, disclosure of information or disruption to Council services.

7.0   Policies and Procedures Framework

7.1   The Information Governance Policy and Procedures Framework is a suite of policies required to ensure services manage their information effectively, and to mitigate any information risks.   The current framework is attached as Appendix 3.

7.2   The policy framework will be updated and amended as the Information Management Improvement Plan progresses and, where required, to give effect to legislative requirements, Council or Information Governance Board decisions, or changes in operational procedures.

8.0   Review and Updates

8.1   This Policy will be reviewed annually by the Information Governance Board to ensure that it remains in line with legal and business requirements and corporate priorities.

8.2   Delegated authority is vested in the SIRO by the Council to update the Policy if required by legislation, Council or Information Governance Board decisions, or changes in operational procedures.

END

Appendix 1 - Governance and Accountability Management Structure
Appendix 2 - Information Governance Board - Terms of Reference
Appendix 3 - Policy and Procedures Framework

Information Governance and Accountability Management Structure

Director Corporate Services
Senior Information Risk Owner

- Overall Responsibility
- Reports to Council and corporate Management Team (CMT)
- High Level Review / Advice of Risk Management

Senior Information Asset Owners [Directors]

- Approval
- Ownership and Quality Assurance
- Risk Management
- Performance Reporting

Monitoring Officer / Data Protection Officer

- Risk Reporting
- Strategic legal and operational advice
- Policy compliance & incident reporting
- Training & development

Executive Manager - ICT

- IT Strategy
- IT Operations
- IT Security

Executive Manager – Human Resources

- Risk Assurance
- Risk Management

Team Leader - Legal

- Operational Legal advice
- Manages Information Management Legal Team

Team Leader – Admin [Records Manager]

- Develop policies and procedures
- Reports information statistics
- Operational Admin advice
- Co-ordination of FOI/EIR/DP/RM

Information Asset Owners [Executive Managers]

- Info Asset Register
- Quality Assurance
- Policy Compliance
- Assessing Risks
- Asset Access
- Improvements
- FOI/EIR/SAR Approval

Information Asset Administrators

- FOI/EIR Co-ordinators
- DP Liaison Officers
- Information Asset Co-ordination, Advice and Assistance
- Networking

Information Governance Board - Members
Information Governance Board - Advisors

- Approves Procedures
- Manages Risk
- Strategic Direction
- Reviews Incidents
- Reviews Training

Governance and Accountability Management Structure

The Governance and Accountability Management Structure illustrates those specific job roles that have particular responsibilities, as outlined in detail below:

Senior Information Risk Owner
The Council has designated this role to the Director of Corporate Services, who is responsible for the corporate monitoring and implementation of the Information Management Strategy and Improvement Programme; managing the risks and assurance measures, maturity level targets and reporting regularly to CMT on the effectiveness of this programme of work and alerting to issues of non-compliance. The SIRO also acts for the Council as Data Controller, and determines the purposes for which, and the manner in which, any personal data are, or are to be, processed, and has overall responsibility for ensuring the Council's compliance with the Data Protection Act 2018. The SIRO is also the Council's named officer for the statutory functions and obligations of the Council under all current legislation relating to Freedom of Information, Regulation of Investigatory Powers, and any other relevant legislation or statutory guidance relating to records management, including the Public Records (Scotland) Act 2011.

Monitoring Officer
The Council's Scheme of Administration and Delegations has designated this role to the Chief Legal Officer [Executive Manager – Governance and Law], who is responsible for monitoring any proposal, decision, or omission by the Council, Committee, Sub Committee or Officer that contravenes any legislation or Code of Practice. The Monitoring Officer will inform and advise the SIRO of any issues regarding compliance with the Freedom of Information (Scotland) Act 2002, or the Public Records (Scotland) Act 2011.

Data Protection Officer
The Chief Legal Officer [Executive Manager – Governance and Law], is also the current designated Data Protection Officer. The Data Protection Officer must inform and advise the Data Controller [the Council] of its obligations under the Data Protection Act 2018, and monitor the implementation and application of the Council's policies and training on personal information management.

Senior Information Asset Owner [Directors]
The authorising person within a Directorate responsible for ensuring the Information Management Strategy and improvement targets are implemented and adopted by staff and for the assets within their Departments and Services. They are also the owners of Information Management Risks and for ensuring that the risks are managed in accordance with Council policy and practice.

Information Asset Owners [Executive Managers]
Information Asset Owners are responsible for ensuring information management policies and procedures are followed, recognising actual or potential security incidents, consulting their Senior Information Risk Owner on incident management, and ensuring that information asset registers are accurate and up to date and that appropriate monitoring and reporting is in place.
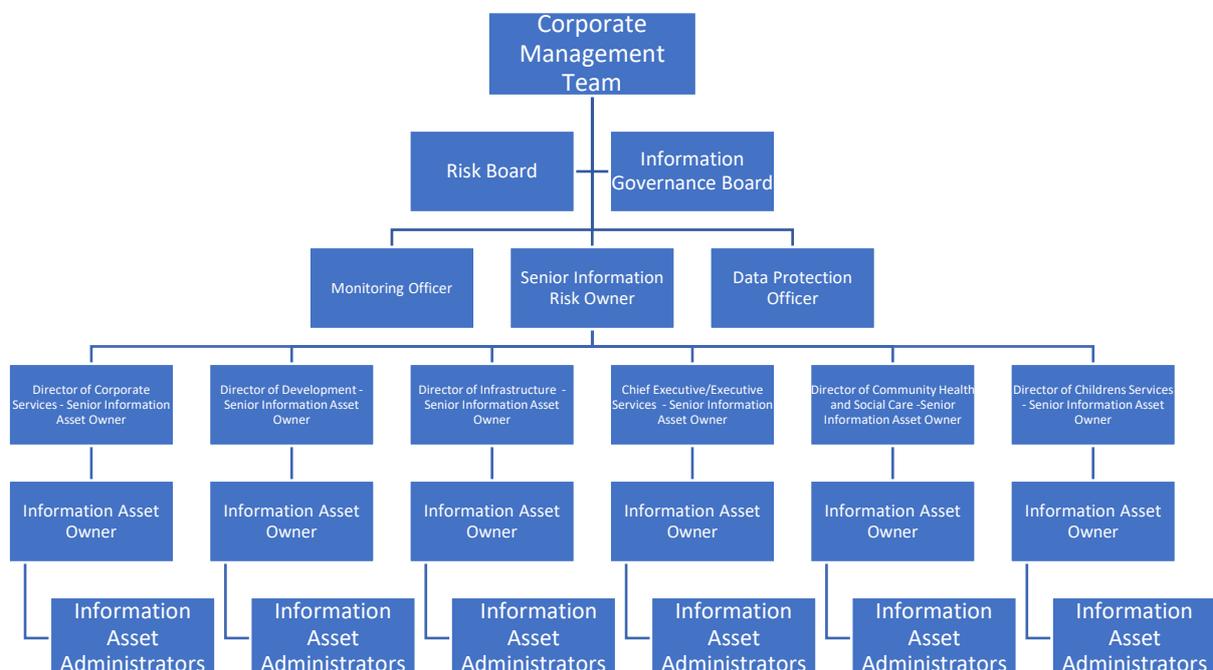
Records Manager

In support of senior management responsibilities, operational day-to-day information management functions are delegated to the Records Manager [Team Leader – Administration], who is required to promote, monitor and manage the effective control of the Council's records in relation to service and departmental procedures and practice, and ensure corporate wide compliance with the Records Management Plan and associated requirements under the Public Records (Scotland) Act 2011. The Records Manager is the Council's initial point of contact for any Records Management issues.

Information Asset Administrators [Business Support/Admin]

Responsible as part of the Directorate Business Support Team for ensuring information management practice and policies are followed by all staff, providing frontline support to Directorate staff to adhere to all information management requirements [Records Management, FOISA and Data Protection] and identifying any issue to their Information Asset Owners.

Information Governance Board

Responsible for ensuring that the Council develops the governance, accountability and strategic direction of all corporate information asset management now and in the future, and that the Information Management Strategy and Improvement Programme aligns with other relevant strategies, projects and work streams, such as the ICT Strategy and Business Transformation Programme.

END

SIC Information Management – Policy and Procedures Framework	
Policy	**Procedures**
Information Governance Policy	• Governance and Accountability Management Structure • Information Governance Board - Terms of Reference • Policy and Procedures Framework
Records Management Plan	• Information Management Improvement Plan • Information Management – Annual Self Assessment Procedures
Information Security Policy *[to be developed]*	• ICT Security Policy • Incident Management Procedures [Data Breach reporting] • Vital Records and Business Continuity Guidelines *[to be developed]*
Records Management Policy	• Business Classification Scheme • Retention and Destruction Schedule • Information Asset Register Guidelines *[to be developed]* • SIC Information Classification and Protective Marking Scheme • Information Handling Rules • Guidelines for Naming Conventions and Version Control • Social Media Guidelines • Freedom of Information - Standards and Guidance
Data Protection Policy	• Individual Rights Procedures • Privacy Impact Assessment Procedures • CCTV Procedures *[to be developed]*
Shetland Data Sharing Framework	• Information Sharing Guidelines • Data Processor Agreements – Guidance • Contracts and Agreements – Guidance *[to be developed]*
Information Preservation Policy *[to be developed]*	• Archives Transfer Procedures • Joint Protocol - SIC Minute Books to Shetland Archives – Closure Periods and Access Procedures • Archive Records Review Procedures *[to be developed]* • Digital Migration and Preservation Procedures *[to be developed]*

The policy framework will be updated and amended as the Information Management Improvement Plan progresses and, where required, to give effect to legislative requirements, Council or Information Governance Board decisions, or changes in operational procedures.

END

Information Governance Board - Terms of Reference

Core Members
Senior Information Risk Owner [Director of Corporate Services] – Chair
Data Protection Officer/Monitoring Officer [Executive Manager, Governance and Law] – Vice-Chair
Senior Information Asset Owners [Directors x 5]
Executive Manager - ICT
Executive Manager – Human Resources

Advisors/Attendees
Information Asset Owners [Executive Managers] – as appropriate to agenda
Project Managers, Change Programme – as appropriate to agenda
Risk Management Officer
Team Leader – Legal Services
Team Leader – Administration [Records Manager]

Purpose
To support and drive the information governance agenda, and provide the Council with assurance that that there is legal compliance and that there are effective information governance best practice mechanisms in place.

Remit
- To ensure that the Council has effective policies and management arrangements covering all aspects of information governance, and that these are in line with the Council's information governance policies and procedures.
- To ensure that regular assessments and audits of information governance policies and arrangements are carried out.
- To ensure a core programme of training and development on information governance is embedded in all workforce development plans.
- To secure the establishment of the Information Governance Improvement Programme including the necessary implementation of resources, and monitor implementation of the Programme.
- To receive and consider breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.
- To report to the SIC Policy and Resources Committee on information governance issues.
- To liaise with other internal and partnership groups in order to promote information governance issues, especially: Data Sharing Partnership, ICT Management Board and Corporate Management Team.

Assessment and Review
The Senior Information Risk Owner will provide an **annual** performance and planning report to Corporate Management Team covering the following matters:
- Information Management Improvement Programme and related activities;
- Information risks and incidents;
- Information Audits and Actions Plans; and
- Information Policies and Procedures.

Meetings
- The Board as often as deemed necessary by the Chair, but will meet a **minimum** of 4 times per year.

Quorum
- The Board will be quorate when either the Chair or Vice-Chair are present **AND** 3 other core members. Named substitutes are permitted in place of core members.

Administration
- The Chair shall arrange for all meetings of the Board to be minuted and circulated internally as appropriate and agreed by the Board.
- Minutes shall be clearly marked if there is any matter which is deemed confidential and may impact on the health, safety or welfare of Council employees, contractors, service users or assets [information or property].

END