Information Governance Framework

Information governance is a generic term for the way in which an organisation manages its information. An organisation needs to consider its environment, laws and regulations, to put in place the right accountability, policies and procedures, and officer training and awareness

25 July 2019 **Release** Version 2.0

Document Review

Title	Name(s) / Board	Role / Responsibility
Document Owner	Mark Gannon	Director, Business Change and Information Solutions (BCIS), Senior Information Risk Owner
Change requests to	Mark Jones	Senior Information Management Officer and Data Protection Officer
Key stakeholder review	Information Governance Board	Authority for information-related council policies
	Information Governance Working Group	Portfolio representatives

Document approval

Authorising Body	Date of acceptance
Information Governance Board	25/07/2019

Version History

Version	Issue Date	Comments / Summary of changes
0.1	24/03/2014	First draft amended following feedback from IGB members and other portfolio stakeholders.
1.0	25/03/2014	Version Approved
1.1 & 1.2	17/04/2019	Version update. Removed reference to the Systems and Processes as they are covered under policy, standards and procedures.
1.3	17/07/2019	Version update following IGB feedback
2.0	25/07/2019	Minor change to IAO Role following IGB comments

Introduction

1. Sheffield City Council provides services to over half a million people and relies on good quality information to be able to plan, make and be accountable for the decisions it takes and the business activities it carries out.

2. Information comes in many forms, can span many years and vary in sensitivity, but the common factor is that if the Council holds the information it is because it needs it for reference or evidence of its activities.

3. Information must be processed consistently from the moment the information is first captured until its disposal, with due regard to its value and risk. We need a framework to set out the Council's approach to governing council information.

4. The aim of this Framework is to describe the information governance arrangements in regards to officer accountability, key principles, policies and procedures, staff awareness and training.

Scope

5. This Framework applies to all staff, including casual workers, agency staff, contractors, volunteers and self-employed people, engaged in work for the Council, who process or have access to Council information or its associated systems.

6. Information governance is a broad term, but the following themes are key:

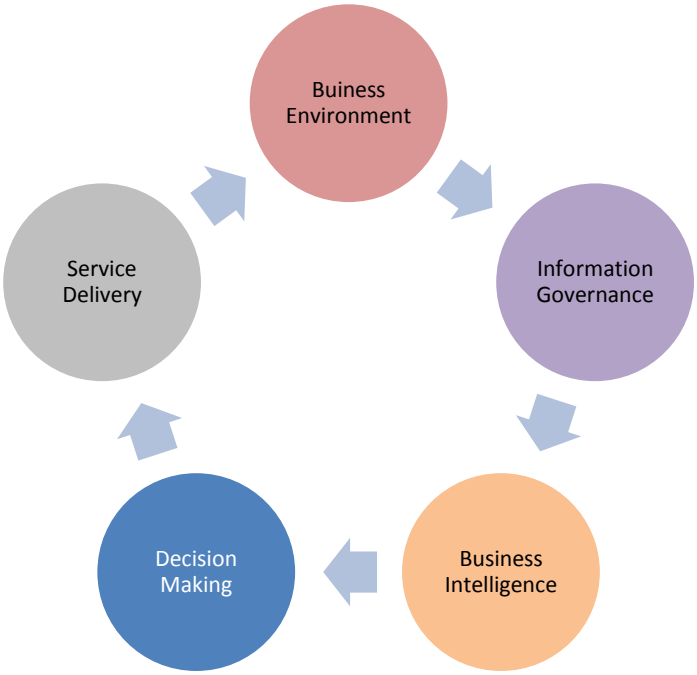
- Access Rights: legal rights and customer experience
- Records Management: business rules, retention and opportunity
- Data Protection: safeguarding individual privacy and compliance
- Information Security: safeguarding systems and operations
- Information Asset Management: existence, classification and use
- Transparency: public trust and open data

Principles

7. The fundamental ask of all staff is to ensure they understand what information they need to do their job and as a matter of routine to: collect the relevant information; make sure it is accurate and complete, easy to find and understand; share it lawfully; keep it safe from loss, damage,

accidental, deliberate or unauthorised access, alteration, disclosure or disposal; dispose of it when it is no longer needed.

8. It follows that the Council needs an approach to exploit the experience, skills and knowledge it has within the Council to make decisions and improve services. The following model depicts the fundamental process required:



- ***Business Environment***: Services understand their business environment and the legal, operational and administrative requirements and information needs;

- ***Information Governance***: Policies and procedures are defined to ensure the right information is processed and sufficient for business needs (relevant, reliable, re-usable);

- ***Business Intelligence***: Information, people and tools are in place to analyse information and report on business needs, performance and trends;

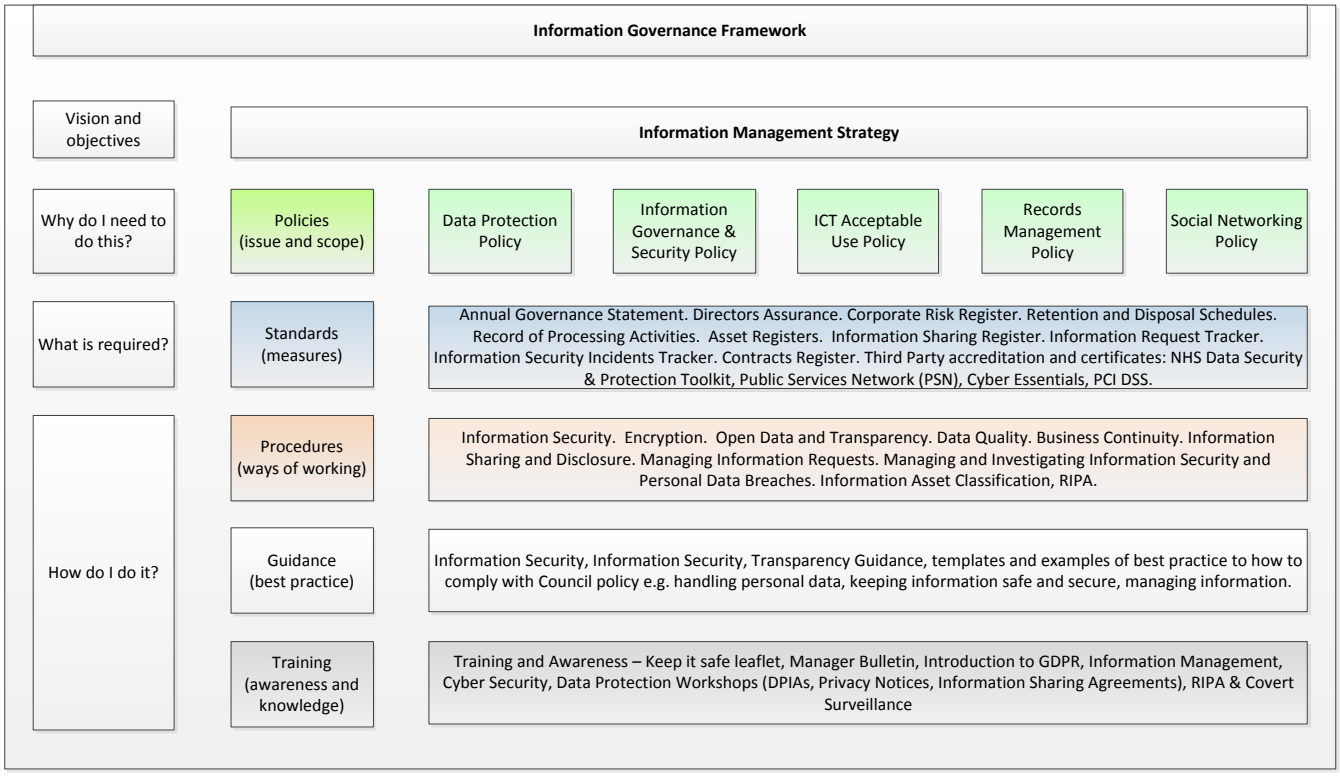
- ***Decision Making:*** Information and analysis is available and exploited to make timely and meaningful decisions;

- ***Service Delivery*****:** Information shapes and influences plans and ambitions to deliver joined-up, affordable, timely and quality services.

9. This approach relies on the commitment to identifying information assets and assigning ownership to the assets with clear management responsibilities to help ensure the information held by the Council can be and remains an important asset.

Key Policies & Procedures

10. The key policies and procedures to support the principles are shown in the diagram below and are available to read on the Information Management SharePoint Site via the Intranet:



11. The Council's Information Management team provide expert advice and guidance about information governance and other information related matters such as information rights, data protection, information and records management, and information security incidents.

12. The team work with key stakeholders across the Council to develop, produce and embed the policies, procedures and standards needed to comply with laws, standards and best practice, see (**46**).

Accountability

13. Everyone working for or on behalf of the Council has an information governance responsibility and therefore required to adhere to the key principles, policies and procedures.

14. The Council has identified and nominated officers to key information governance roles and decision making bodies in accordance with legal, regulatory or best practice requirements; these roles are explained below (**15**) to (**34**).

Accounting Officer

15. The Council's Accounting Officer, the Chief Executive, is ultimately responsible for ensuring the appropriate information governance arrangements are in place across the Council.

Senior Information Risk Owner (SIRO)

16. The SIRO is a nationally recognised role with the overall responsibility for information risk within an organisation. The SIRO chairs the Information Governance Board to

    - Foster a culture for protecting information
    - Provide a focal point for information governance compliance and managing information risks and security incidents
    - Is concerned with the management of all information assets
    - Provides advice, guidance and updates to the Council's Executive Management Team

Portfolio Information Risk Owners (PIRO)

17. The PIRO is a Council appointed role intended for Directors of Business Strategy to oversee and manage information risks within their portfolios. The PIRO supports the SIRO by directing key messages and initiatives across their Portfolio to manage and mitigate information risk.

Caldicott Guardians

18. The Caldicott Guardian role is a mandated requirement for local authorities that have social care responsibilities and its incumbents are required to register on the public National Register of Caldicott Guardians (Local Authority Circular LAC 2002/2).

19. The Guardians act as the conscience of the organisation and help to make decisions about the processing of social and health care information, which includes approving information sharing agreements and other disclosures.

Data Protection Officer

20. The Data Protection Officer role is a legal requirement for the Council under Article 37 of the General Data Protection Regulations 2016 with the remit to ensure the Council understands and complies with its data protection responsibilities, to provide data protection advice and support, and be the Council's key liaison officer with the Information Commissioner's Office.

Surveillance Camera System Senior Responsible Officer

21. The Surveillance Camera Commissioner has asked local authorities to nominate a Senior Responsible Officer to help ensure the organisation complies with Section 33 of the Protection of Freedoms Act 2012 and the management and use of surveillance camera systems.

Information Asset Owners

22. The Information Asset Owner is a nationally recognised role to act as the responsible owner for information being processed. This responsibility includes knowing what information is held and why and what rules apply for its use, disclosure and security.

23. These responsibilities are generally met through other governance arrangements, for example the Annual Governance Statement, so the IAO responsibility is assigned to the Directors. .

24. The Information Asset Owner will delegate the operational tasks and seek assurance from staff that sufficient governance is in place to ensure information is handled in accordance with the key principles, policies, standards and procedures.

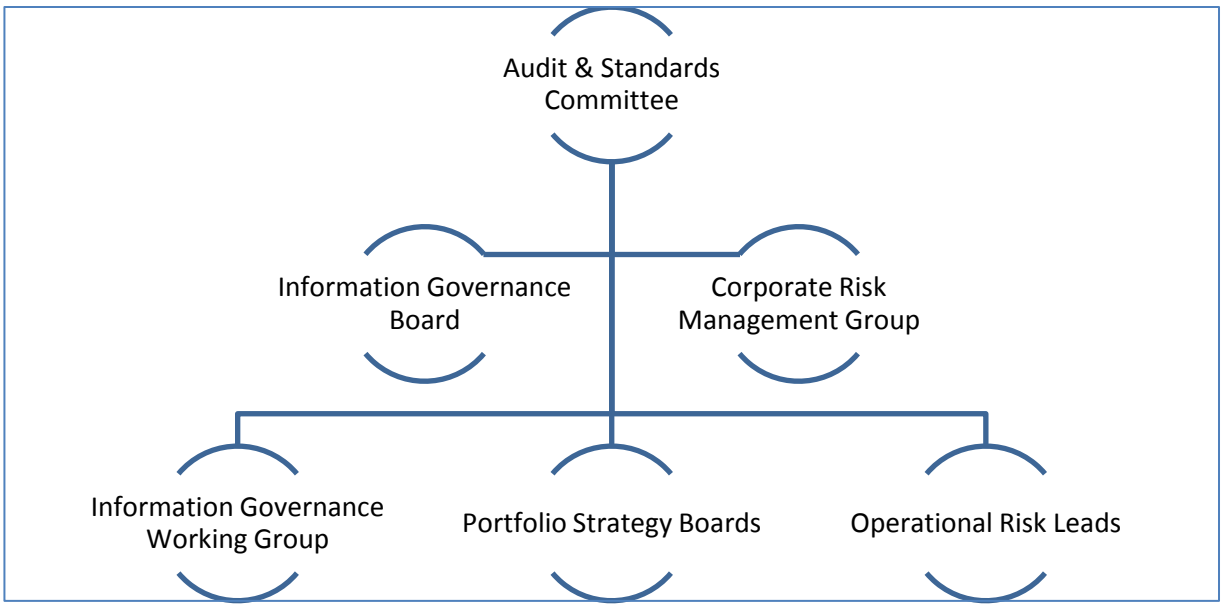
Application Owners

25. The Application Owner (aka System Administrators) is a Council appointed roles assigned to individuals that help to manage ICT applications used to carry out Council business.

26. Application Owners duties will vary depending on the system and its functionality, but in essence they will ensure systems operating procedures are in place and followed; user accounts are managed and up to date; technical security controls enabled; faults, issues and incidents reported; users trained.

Key Governance Bodies

27. Key governance bodies are in place to help ensure information governance is in place across the Council. The diagram shows the key stakeholders:



Audit & Standards Committee

28. The Committee, attended by Councillors and Council Officers, assesses and oversees the Council's risk management, control and corporate governance arrangements and advises the Council on the adequacy and effectiveness of these arrangements.

Information Governance Board

29. The Board, attended by Council officers from all Portfolios including the Senior Information Risk Owner, Portfolio Information Risk Owners, Caldicott Guardians, Data Protection Officer and subject matter experts from Facilities Management, HR, IT and Risk Management.

30. The Board is responsible for:

- Helping to set and shape the information governance agenda and strategic ambition
- Ensuring appropriate policies and strategies are written, communicated and updated
- Monitoring statutory performance i.e. information requests compliance
- Reviewing the key information governance risk, issues and security incidents
- Ensuring information governance training and awareness is sufficient and embedded
- Reporting to the Executive Management Team or Audit and Standards Committee

Corporate Risk Management Group

31. The Group provides strategic leadership for risk management to ensure risk is managed effectively through the ongoing development of a comprehensive risk management strategy and to escalate risks and report on outcomes.

Portfolio Strategy Boards

32. Since 2010, Portfolios have been asked to include information governance as a standing agenda item at their Portfolio Strategy Board or Risk Group. The Boards are chaired by the Portfolio Information Risk Owner or equivalent representative.

Information Governance Working Group

33. The Group is an operational group intended to identify the key information governance requirements and help develop and embed the procedures, guidance and awareness needed help the services comply with their governance obligations e.g. respond to requests, manage incidents, etc.

Operational Risk Leads

34. The Leads review and monitor the risks on the Corporate Risk Register, including information risks, and work with services to ensure the risks are being treated. Risks that cannot be resolved and reported to the Portfolio Strategy Board and Corporate Risk Management Board as appropriate.

Culture, Training and Awareness

Culture

35. The Council wants to foster a professional culture where staff take the necessary precautions when processing information and know when the information can be used and disclosed.

36. The Information Commissioner identifies that a limited knowledge about information governance amongst staff can have an adverse impact on the way organisations work, for

instance information is not shared, is not available, is held in different systems, is kept for too long, etc.

37. The Information Commissioner also recognises the majority of information security incidents are due to human error and wants organisations to educate its staff through staff induction, training and awareness, especially in data protection, information and records management, to embed good practice.

38. Failure to educate staff or anyone else processing Council information can have significant consequences for customers, the Council, and the individual responsible. The Information Commissioner publishes details of the enforcement action they have taken when the law or personal information has breached: https://ico.org.uk/action-weve-taken/.

Training and Awareness

39. The Council has over 8000 staff. Training and awareness has to be proportionate and realistic. The table below shows the requirement for all staff to complete the introductory information governance / management training and the availability of more specialised training and awareness for officers based on their roles and responsibilities:

	Keep it Safe Leaflet	**Information Management (Introduction)**	**Cyber Security Videos**	**RIPA / Surveillance**	**Information Management (Managers)**
Workers not using ICT	√	√			
Workers using ICT	√	√	√	√	
SIRO / PIROs	√	√	√	√	√
Caldicott Guardians	√	√	√	√	√
Data Protection Officer	√	√	√	√	√
Information Asset Owners	√	√	√	√	√
Application Owners	√	√	√	√	√
Additional Key Roles					
IGWG / CRMG / Information Management Team	√	√	√	√	√
Business Change / Project Officers / Contract Officers	√	√	√	√	√

40. This training can be delivered via hard copy materials, e-learning or taught courses designed to suit the need of the audience.

41. There is a requirement that the basic Information Management training, Cyber Security and RIPA e-learning is completed by all relevant staff within the first 6 weeks of them starting with the City Council and then to refresh once every two years. However, in Adult Social Care and Public Health, the requirements of the NHS Data Security and Protection Toolkit, are for a mandatory annual refresher every 12 months.

Specialist Training

42. Some officers and roles may need additional specialist training and this is offered inhouse, for example: Privacy Notices, Data Protection Impact Assessments, Information Sharing Agreements, Managing Incidents, etc. Enquiries can be made to the Information Management team at informationmanagement@sheffield.gov.uk.

43. Line Managers must ensure their staff and other authorised users are aware of information governance and any duties specific to their role and record any specific training as part of the Personal Development Review.

44. In addition colleagues with specialist roles should receive the benefit of specialist training in the data security and protection. ICT staff in critical roles, such as the Technical Solutions Architect (Security), is supported to undertake training outside the organisation. Likewise, the Council officers that process data for research and analysis to help exploit the data held and support strategic and operational decision making.

Reporting and Monitoring

45. Information about the completion of training will be available to the Portfolio Information Risk Owners and reported to the Information Governance Board. It will also be used as evidence in the annual submission of the NHS Data Security and Protection Toolkit, and possibly used as evidence to the Information Commissioner's Office in the event of a personal data breach.

Compliance Factors

46. The Council is required to comply with a range of laws, regulations, standards and best practice. The Council may also be required to demonstrate its compliance in support of self-assessments and submissions to obtain access to information, systems or for regulatory, service or contractual purposes.

47. It is not possible to list them all, so the table below lists and provides a brief summary of the ones relevant to the Framework.

Law	Brief Description
Access to Health Records 1990	Disclosure of records created by health professionals, e.g. occupational health nurse.
Computer Misuse Act 1990	Inappropriate and misuse of the ICT.
Common Law Duty of Confidentiality	Information given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent, unless there is a lawful reason to do so (safeguards, public interest, legal duty).
Environmental Information Regulations 2004	Disclosure of environmental information.
Freedom of Information Act 2000	Disclosure of recorded information unless another law applies e.g. data protection, EIR.

	Requirement for a publication scheme to set out what publicly available and where. Section 46 also refers to the Lord Chancellor's recommended code of practice for the proper management of records to support compliance with the Act.
Regulation of Investigatory Powers Act 2000	Law regulating the powers of public bodies to carry out surveillance and investigation and covering the interception of communications.
Health and Social Care Act 2012 (Part 9, Chapter 2)	Set out the responsibilities for the Health and Social Care Information Centre (now NHS Digital) to act as the central, authoritative source of health and social care information.
Human Rights Act 1998	Disclosure of information, especially Article 8 and the right to privacy.
Protection of Freedoms Act 2012	Safeguarding civil liberties and reducing government intrusion, such as retention of DNA, powers of entry, CCTV regulation, fingerprinting of children in schools. With regards information governance, it adds new provisions to the FOI Act 2000 (sections 11 and 19) and the way datasets are released and re-made reusable as well as extending FOI to cover companies wholly owned by two or more public authorities.
General Data Protection Regulation 2016	EU Regulation modernising data protection law, introducing new individual rights and laws, in particular the need for accountability, as well as greater fines and penalties – not just personal data breaches, but other non-compliance.
Data Protection Act 2018	Introduced to align with the General Data Protection regulations and replaced the Data Protection Act 1998.
Standards	
ISO 15489 Information Management	Provides a framework to manage records based on the lifecycle model from creation to disposal with appropriate controls at each stage to ensure records are captured, organised, reliable and retrievable. Relies on classification, metadata and retention.
ISO 27000 series Information Security	Provides a framework intended to establish systems and risk-based controls to ensure the balance between access to information and information systems without compromising their confidentiality, integrity and availability. Relies on an up to date Information Security Management System, controls and risk assessments.
EN 15713:2009 Secure confidential waste	Recommendations for the physical disposal of confidential waste, including reference to the appropriate shredding sizes based on the sensitivity of the information and physical

	format of the item (paper, tape, disk etc.).
Key Current Drivers	
NHS Data security and Protection Toolkit	Annual submission to NHS Digital to confirm the information governance arrangements in place to obtain NHS data.
Public Services Network Connectivity Accreditation	Annual ICT Health Check for PSN accreditation to continue to access the PSN network.
Local Government Transparency Code 2015	Making local council's more transparent and accountable to local people (Ministry of Housing, Communities and Local Government (MHCLG)
Cyber Essentials & Cyber Essentials +	National Cyber Security Centre certification schemes to help organisations understand and reach the minimum information security controls to better protect their ICT hardware, systems and information. A self-assessment and / or independent audit to obtain certification.
Payment Card Industry Data Security Standards	PCI DSS is an industry standard to ensure appropriate information security controls, process and procedures are in place to protect cardholder payment data. Organisations submit an annual self-assessment questionnaire to obtain accreditation.

Audit and Review

48. Information governance is as continuous improvement process. The Information Governance Board will directly, and together with the Internal Audit Team, ensures a process of review in the annual work programme. This will include consideration of relevant reports for ICT, data quality, business continuity exercises, compliance with information security.

This page is intentionally left blank