

Information Management Strategy



READING BOROUGH COUNCIL
March 2022

Contents

Foreword	2
1. Introduction and purpose	3
1.1 What is information?	4
1.2 Definition of Information Management	5
1.3 Information Management capabilities	5
Information governance	5
Document, content and records management	6
Data management and quality	6
Business intelligence	6
Information Risk and Security	6
2. Drivers for change	7
2.1 RBC challenges	7
2.2 Drivers for change	7
Achieving Customer Service Excellence - Our Customer Experience strategy	7
The way we work - flexible and remote	7
Use of Big Data	8
EU General Data Protection Regulation (GDPR)	8
3. Information management vision	8
Information Management Key Principles	9
4. Delivering the Strategy	10
4.1 Information Governance - Who	10
4.2 Roles and Responsibilities	11
All Staff	13
Information Governance Board (IG Board)	13
Information Governance Team	13
Information Asset Owners	13
Data Stewards	13
4.3 Information architecture - what	14
4.4 Information management policy framework - how	15
Records Management policies	15
Retention policies	15
Information security and assurance policies	15
Data protection policies	16
Records of Processing Activities (ROPA)	16
Information sharing policies	16

Foreword

Reading Borough Council (RBC) is looking towards a future where working closely with Customers through new digital platforms and Services, has never been so important. In order to progress our Connected Reading Digital Transformation Strategy and our Customer Service Excellence Strategy, we need to better organise and consolidate our information.

RBC has set out its ambition to create a sustainable, future-proof model of local public services. The Council seeks better customer insight to empower staff to deliver improved Services. The Council wishes to promote opportunities to create financial savings, new value propositions for customers and commercial opportunities. To achieve this staff need access to better data and information. This information needs to be available to our partners too, if we are to increase the potential to deliver effectively through partnerships. With these objectives in mind, we have been proactive in identifying and addressing some of the relevant sector challenges, particularly around how we harness the digital agenda to improve services to the community, tackling an ever-growing constraint on operating budgets to maximise efficiencies, improve service effectiveness and reduce waste.

Like people, buildings, money or infrastructure, information has an intrinsic value that we need to harness to deliver better, faster and more cost-effective services to our residents. Information is critical in understanding and delivering internal and external business functions. We will use these 'Information Assets' to more effectively design our future services. We will recognise the value of knowledge by investing in capabilities and leadership in this area.

Currently our information is often locked away in function, service or departmental silos with the value only released for a primary and invariably narrow, reactive operational requirements. We want to change this. In the future, information will be used to predict likely future citizen behaviour and offer alternative courses of action to the benefit of both the resident and cost of council services.

1. Introduction and purpose

Information comes in many forms - policy documents, case files, reports, minutes, operational data and personal data - and is held in a variety of printed and electronic formats. Across RBC, we use this information in our daily working lives, as we work to achieve our own objectives and those of the Council - whether delivering services, formulating policy, managing budgets, holding meetings or undertaking commercial activities.

Increasingly, organisations are looking at how they can use the information they hold in more creative and imaginative ways, to improve the customer experience, drive efficiencies and gain commercial benefits. Organisations across the world have demonstrated that digitising services, cross-matching data sets and using information in different ways is both producing new ways of addressing a range of challenges and presenting opportunities.

This strategy provides a foundation to help us on our journey of continuous improvement, through promoting better management and use of our information, ensuring appropriate transparency, data security and compliance with data protection legislation.

It also outlines principles which the Council will adopt through the development and implementation of supporting policies and standards.

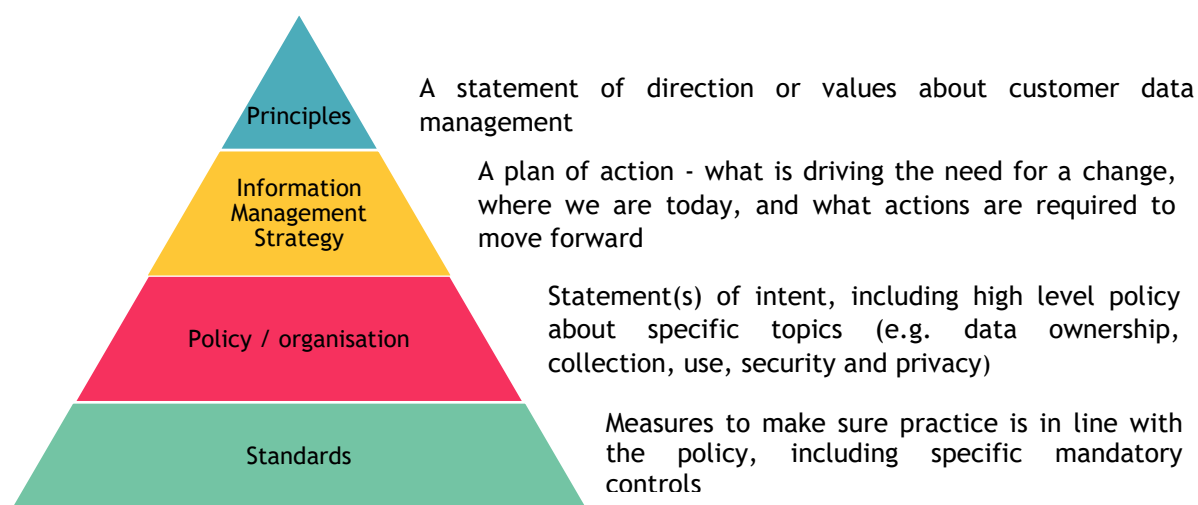


Figure 1:Information Management Framework

1.1 What is information?

For the purpose of this Strategy, information is defined as any printed or electronically held document or data stored or used by the Council.

This includes:

- Any printed or handwritten document, including correspondence generated and received by the Council.
- Any electronically held document, including media images, email, office documents, social media, audio and video information.
- Any information in transit or held in a repository, such as customer relationship management information, asset management information or finance information.
- Informal or tacit information held by individuals in notes of meetings, diaries, site visit notes or knowledge banks.

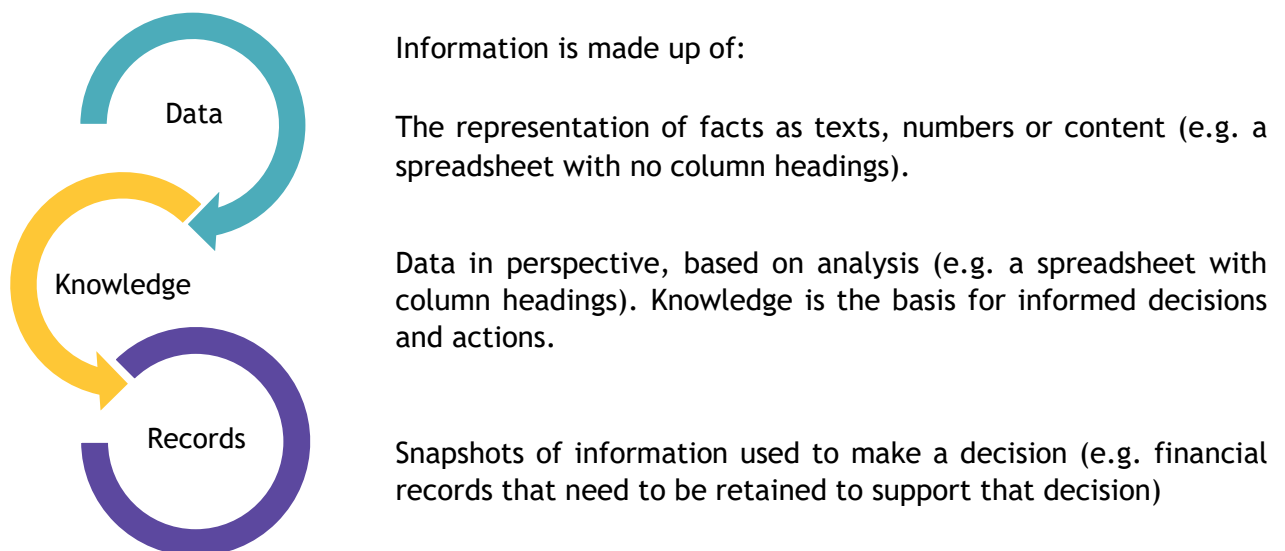


Figure 2: Information Formats

This broad and wide-ranging definition has the implication that any information, in whatever shape or form, needs to be managed with the appropriate level of care and attention.

As part of this Strategy, we must develop a culture that understands there is a balance between the costs of maintaining the information held, versus the value of that information to the Council and the services that it delivers.

1.2 Definition of Information Management

Information is essential to all staff, at all levels, and across all services of the Council, so that they can carry out their day to day duties. The Council needs, within its regulatory obligations, to safely manage and secure the information created or managed. It also needs to dispose of information that is no longer needed and which holds little or no value to the Council.

Information Management is made up of policies, governance, processes and information handling behaviours which seek to control information throughout its lifecycle. The information lifecycle runs from capture or creation, through its handling, storage, retrieval and use, and ultimately to its disposal (either destruction or disposition in an historical archive).

Our approach should ensure that all live information is accurate and up-to-date. Records should reflect an accurate account of Council activity at the time they were created. They should achieve compliance with legislative and regulatory constraints and support the effective delivery of services. Good accurate information should be at the heart of all decision making.

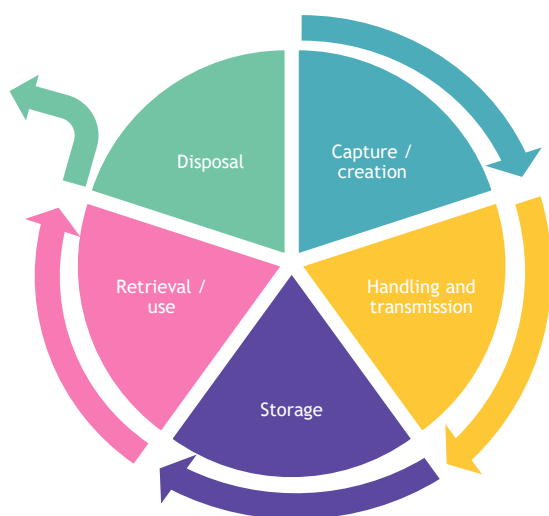


Figure 2: Information Lifecycle

1.3 Information Management capabilities

The Council has identified the following activities that are required to support the information management lifecycle:

Information governance

A governance structure with an accountability framework that sets out accountability, roles and responsibilities and expected behaviours of staff. It includes the development and maintenance of this Strategy, the Information Management Policy Framework, information management standards, processes, controls and procedures, which together

support the Council in achieving its aims and activities. The presence of appropriate Information Architecture, as outlined below, that supports the Council's management of its information assets is a vital enabler for this.

Document, content and records management

The management of information in the form of documents and other containers of content throughout their lifecycle from creation to disposal. This aims to create structure using effective storage, filing and indexing systems (both paper and electronic based) that enable the effective search and retrieval of information, making it available to the right people in the right format and right place at the right time.

Data management and quality

The identification, management and exploitation of data held predominantly within database driven business systems and other data stores. Data quality is synonymous with information quality, since poor data quality results in inaccurate information which could have a material impact on business performance. Business expectations need to be translated into data quality rules, which concern accuracy, completeness, consistency, integrity, timeliness, uniqueness, and validity. These can then be used to assess, improve and sustain data quality across the organisation.

Business intelligence

Business Intelligence (BI) is a set of techniques, tools and technologies that can transform data into useful information which the Council can understand and act upon. It is also about exploiting that information to enable further understanding and value to be obtained from it through analysis and linking of data. This ranges from static internal performance reporting to bespoke analytics through to predictive customer insight analytics.



Figure 3: Business intelligence activities

Information Risk and Security







Protecting the Council's information assets ensuring the confidentiality, integrity and availability of information, as well as meeting legislative, statutory and best practice requirements. Central to this is a risk-based approach that identifies the information risks and takes appropriate action to mitigate them through the risk classification of information.

2. Drivers for change

A number of internal challenges have been identified which need to be addressed to enable effective Information Management. Our strategic direction and other external factors are also driving the need for change.

2.1 RBC challenges

Key challenges and issues driving this Strategy include:

 Silos of data	Even within single systems, there are instances of a lack of integration between related datasets.
 Managing data instead of delivering a Service	Lack of automated data flow integration between systems requires laborious, preventable manual processing.
 Data ownership	Lack of effective ownership is recognised as a challenge by every area of the business.
 Buried in the long text	Information is captured and stored as unstructured. This reduces the capability to search, analyse and otherwise leverage the data.
 Data Quality	High dependency on individuals capturing data accurately. The cause of poor data quality can often be traced back to the point of capture.
 Retention policies	Lack of clear guidelines about what information we retain and for how long.

2.2 Drivers for change

Achieving Customer Service Excellence - Our Customer Experience strategy

It is recognised in our Customer Experience Strategy that a step change is required in the way we deliver services to our customers and use information about our customers to enable better targeting and tailoring of Council services. This will be aided by the drive to move customers away from face to face and phone contact with the Council to 'self-serve', primarily through digital services and automated processes.

The way we work - flexible and remote

Flexible working is key for a modern workforce, and for this it is vital that information is accessible to all those that require it where ever they are working. Therefore, it is essential we understand the information lifecycle for our processes and consider how we can reduce the use of paper across services and where possible digitise at source.

Use of Big Data

Councils are often said to be sitting on ‘an untapped goldmine’ of data which could offer valuable insight into understanding the needs of their residents by matching data sets across service areas. Joining up public sector data sources can make public services more efficient, save money, improve service outcomes, tackle crime (particularly identify fraud) and help public bodies better serve their citizens. Police forces are using data to undertake predictive modelling on how best to deploy resources, transport authorities use data to change driver behaviour and London and New York city governments have pioneered new approaches to using data, including promoting fire prevention and recycling. To make best use of the data requires systems that can talk to each other, the right skills and resources to undertake analysis and a framework for the Council to develop its approach.

EU General Data Protection Regulation (GDPR)

The introduction of GDPR was the most significant change in data protection legislation for 20 years. Despite Brexit, the law remains essentially the same. GDPR was designed to create a uniform approach to data protection across Europe, empowering citizens and enhancing economic growth by removing barriers that restrict data flows. Continued compliance poses significant challenges to local authorities in meeting their desired information management needs. As the core legislation behind data protection and information sharing, we need to ensure that GDPR is embedded in everything that we do.

3. Information management vision

Our vision for information management is driven by the following Key Principles. These principles are the cornerstone of the Information Management Strategy and provide the direction to ensure it is consistent with, and effective in support of, the broader strategic objectives of RBC such as our digital and customer satisfaction strategies.

Information Management Key Principles

1. Information is compliant

- Information is managed in line with all applicable statutory, legal and regulatory requirements to encourage good working practices and compliance with legislation

2. Information, data and records are strategic assets

- Regardless of where information is held, it is a corporate resource and the property of RBC
- All information, resources and processes should add value to the work of RBC and demonstrate value for money

3. Information is shared appropriately

- Information is treated as shareable unless it is personal or commercially confidential
- RBC staff can access information for the effective performance of their role, and there is the opportunity for the free flow of information
- Information is secured based on the risk and impact to the subject. It is classified for handling, how it should be stored, and who can access it.

4. There will be one version of the truth

- Wherever possible, one data source will be recognised as authoritative. Any other versions will reference that source.
- Consistent definitions are used for data to ensure integrity and ease of understanding

5. Customers and businesses access and maintain information about themselves

- Personal, sensitive and commercial information is kept secure and confidential, but it will be accessible to the individuals it relates to

6. Information architecture enables data

- Data is retained in repositories and architectures that enable the Information Strategy and those repositories are documented
- Self-service of data will be the expected way of working for all services and our data technologies should support this

7. Information is fit for purpose

- Information is not collected unless we have consent and a business reason for doing so
- Information is accurate, reliable, timely and provides value
- Quality is maintained throughout the lifecycle and quality issues are addressed proactively

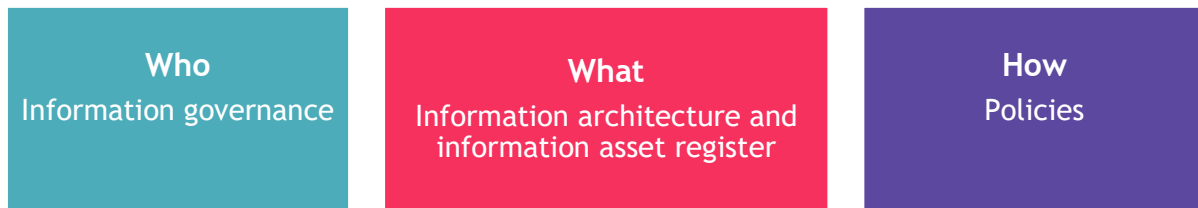
8. Information is owned and managed securely throughout its lifecycle

- Information has a defined Owner who is responsible for the management of it through its lifecycle
- Information is stored and managed in one place, and accessed many times (rather than duplicated in different locations)



4. Delivering the Strategy

To help achieve the desired vision and meet the challenges outlined, we must consider:



For example, GDPR would require a governing body to make critical decisions on the management of personally identifiable information through a clearly defined GDPR policy.

4.1 Information Governance - Who

The key foundation block in embedding information management across RBC and ensuring clear ownership and accountability for Information Assets is to establish a robust information management framework. Every directorate, service, team and member of staff creates information; therefore, all are responsible for effective information management and this Strategy relies on engagement from staff at all levels across the Council to succeed.

The overall governance structure should reflect the 3 lines of defence model:

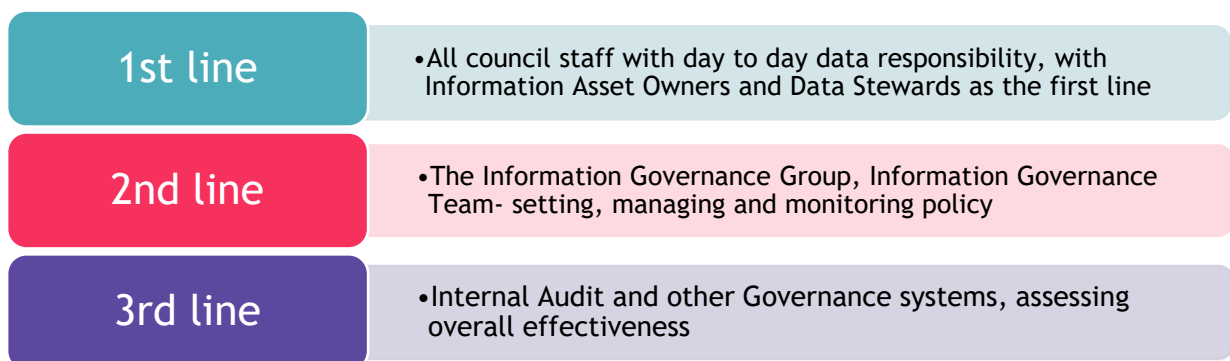


Figure 4: Three lines of defence governance model

Information Governance must be embedded into wider business governance and be supported by clear and senior sponsorship.

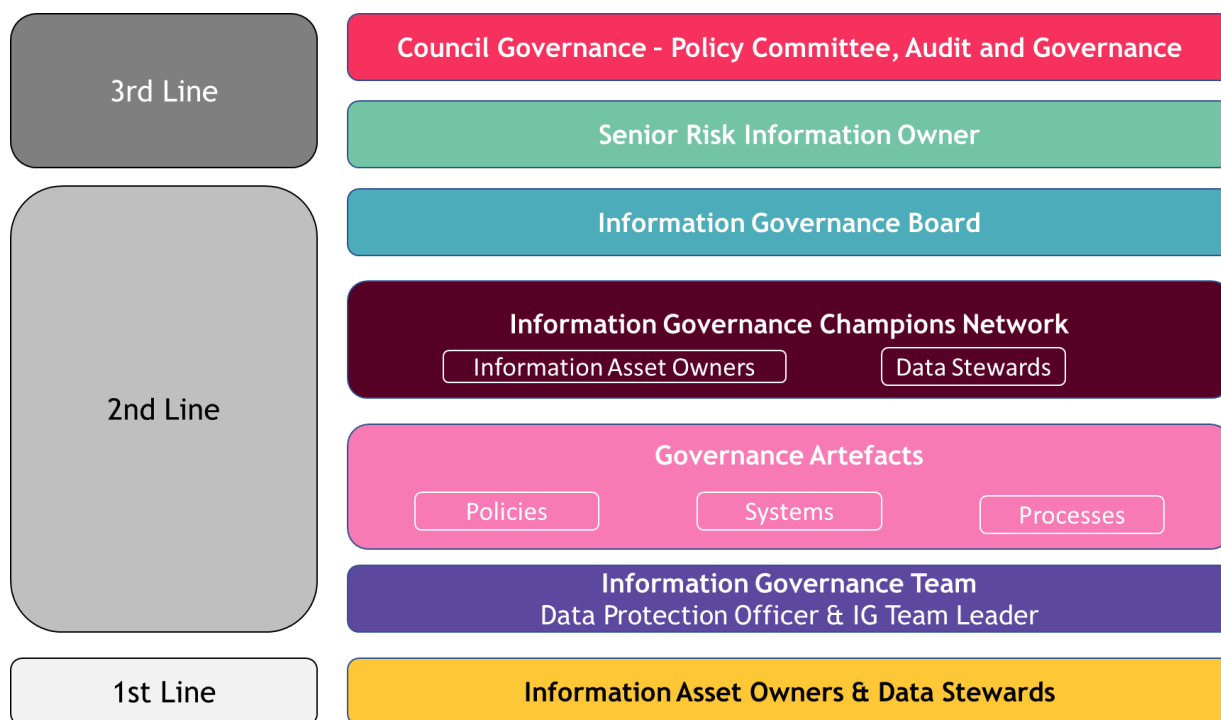


Figure 6: Reading BC Information Governance Framework

4.2 Roles and Responsibilities

Title	Role
Senior Information Risk Officer (SIRO) RBC responsibility: Assistant Director of Legal and Democratic Services	The SIRO will: <ul style="list-style-type: none"> ensure information risks which affect business objectives are highlighted to the IG Board, CMT and councillors and addressed act as a champion/sponsor for information governance within the organisation be responsible for ensuring the IG Board recognises the importance of information assets in delivering corporate objectives
Chief Data and Information Officer (CDIO)	The CDIO will: <ul style="list-style-type: none"> provide a critical interface between the business and Digital and ICT reinforce a commitment to technology develop the ICT strategy and budgetary information to support business requirements
Caldicott Guardian RBC responsibility: Executive Director of Adult Care and Health Services	The Caldicott Guardian is a senior-level executive who is responsible for: <ul style="list-style-type: none"> protecting the confidentiality of people's health and care information making sure it is used properly

Data Protection Officer (DPO) RBC responsibility: Customer Relations and Information Governance Manager	The DPO is responsible for: <ul style="list-style-type: none"> ensuring the organisation's compliance to its Data Protection requirements developing and implementing the organisation's Data Protection Policy through training and advise processing and responding to all requests for information by data subjects providing advice and guidance on ensuring data remains up-to-date and is destroyed when necessary.
Information Governance Team Leader	The IG Team Leader will: <ul style="list-style-type: none"> support the DPO and SIRO in their roles lead the Information Governance Champions Network (IGCN) to cascade Council policy and support Services to comply identify best practice and highlight training needs within Services coach and mentor Data Stewards maintain policy on behalf of the Council
Information Asset Owners RBC Responsibility: Assistant Directors and equivalent	Each IAO will: <ul style="list-style-type: none"> be responsible for information assets within their service, managing risk and ensuring compliance with Council policy champion the use of Information as an asset - making plans within their Service to better create, store and use data and improve Services for residents champion and support the Data Stewards to perform their role
Data Stewards RBC responsibility: Nominated individuals within each service area	<p>Data Stewards will act as a first line of defence throughout the organisation, helping staff to follow policy and procedure in their service areas.</p> <p>Data Stewards will cascade policy requirements from the Information Governance Champions Network (IGCN) highlight practical issues for resolution to the IGCN</p>

All Staff

To embed the Strategy successfully in all parts of the organisation requires understanding from staff of the value of information as an asset in the same way that they value people, technology and other resources. In order to help this shift, there needs to be a comprehensive set of activities around learning, development, communication and monitoring. We will work to embed a 'no blame' culture around information governance, so that meaningful learning can be taken from data breaches and the organisation can learn from its mistakes.

Information management will be embedded as part of the induction process, both at corporate level and departmental level. Guidance around the key issues of information management should be easily accessible for all. A significant programme will be required to embed ongoing culture change throughout the organisation

Information Governance Board (IG Board)

Determines the priorities for implementing governance, sets information governance requirements, and reviews compliance and remedial actions. It "owns" the Information Management Framework. This group is responsible for oversight of breaches, and actions learning opportunities arising from breaches. It will also act in an advisory capacity to programme boards to ensure that change around processes and digital transition are fully understood and the wider implications around information management are monitored.

Information Governance Team

Co-ordinates activity in support of the vision which includes defining the policy and standards to support the Key Principles defined in the Information Management Strategy and monitors compliance across the organisation. It will also be the point of reference for Information Asset Owner for best practice guidance. The IG Team Leader will Chair the Information Governance Champions Network and promote best practice across the Council through the Data Stewards.

Information Asset Owners

Supported by the **Data Stewards**, each AD is accountable and responsible for the operation and compliance with the requirements of the IM strategy and supporting policies and procedures. They will need to be trained and they will need support and guidance in implementing these policies. This is often the most difficult component to get right as it requires careful management and communication and sometimes cultural and behavioural change to be successful.

Data Stewards

A network of officers used to working with the Information Assets who can act as a conduit between the Service and the Information Governance Champions Network cascading requirements, reporting progress, highlighting problems for resolution and best practice to

encourage others. The role will be a significant opportunity for sharing best practice and learning across Services.

4.3 Information architecture - what

Information architecture deals with where we store information, and the structuring and definition of information.

RBC will establish a common language for information management, to define:

- what information we need in order to provide our services
- where it is to be stored
- how it is handled and shared
- who can use it
- how access is controlled
- how information is protected

This is the key enabling step for this Information Management Strategy. The benefit is increased coordination of information management across the Council.

A large number of local authorities are moving towards off-premise data storage. Any move from a traditional on-premise data storage model to the use of multiple cloud / external based storage hosts can initially create a more complex information architecture, and therefore increased information management challenges. These challenges need to be overcome through careful management and understanding of the location and interconnections of data stores, along with enabling technology to bring this information together in as close as possible to a single view.

The Information Asset Register (IAR) is a key component of the information architecture as it defines information that is held, provides details on the management of that information, and identifies an owner and manager for each information asset type. This information is required to provide a single view of the RBC's information holdings and to support development of the information architecture. Compiling the Information Asset Register is the responsibility of the Data Protection Officer with the support of the Information Governance Team Leader and the Information Governance Champions Network.

The IAR also provides information on the high-level risk profile of the information assets. This enables resources to be prioritised in making information management improvements where they will deliver maximum value for RBC. A council-wide Information Asset Register is being created and a process for its maintenance is under development.

Services also need to document information assets within their Business Continuity Plans and Disaster Recovery Plans to ensure protection and recovery of these assets.

4.4 Information management policy framework - how

The Council needs to ensure it has up to date policies and practice to support this Strategy.

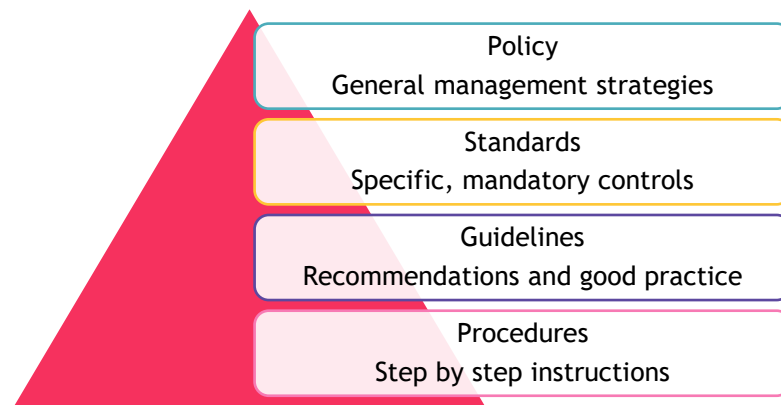


Figure 7: Hierarchy of information management documents

Below are the key supporting information management policies that the Council requires, their content and their purpose. Policy setting is led corporately, and these apply to all areas of the Council. The collection of policies is known as the information management policy framework.

Records Management policies

These policies expand the Council's information management principles and provide supporting policy statements that encompass the Council's statutory and regulatory requirements for managing information.

Retention policies

The Council's retention policies set out our approach to information management, roles, responsibilities and governance. The policies set out the Council's approach to the setting and enforcing of retention periods for different information types and the disposal approach that Information Asset Owners must follow. Corporate retention schedules ensure that the Council is maintaining necessary records for the appropriate length of time. These are made available to staff through the intranet and are governed by the Information Governance Board.

Information security and assurance policies

To ensure the confidentiality, integrity and availability of the Council's information assets and to support the information security management system there are a range of policy positions that need to be set out. Information security and assurance policies provide the Council statement of policy on a range of security issues (such as passwords, encryption, clear desk environment etc). These also set out the Council's commitment to taking a risk-

based approach to the management of its information and through this enabling the Council to take managed risks to minimise cost whilst protecting the confidentiality, integrity and availability of its information assets.

Data protection policies

These set out how the Council will comply with GDPR and the Data Protection Act 2018. Data protection policies are supported by the other information management policies that direct the handling of personal data and information. In each Service, there will be a record of all the **Data Protection Impact Assessments (DPIAs)** which consider the risks of changes to data processing activities and new projects which involve data.

Records of Processing Activities (ROPA)

Documentary assessments of compliance with the GDPR and the handling of personal data. Each business process will be a separate processing activity. Completion of the ROPA enables the IGCN to come to a view on the risks associated with any processing activity and maintain the **Information Risk Register**.

Information sharing policies

These outline the guiding principles for the two-way sharing of information, based on legal and ethical requirements. It aims to provide a framework on how we securely share information between partner organisations both in terms of contractually and operationally, and also covers wider issues of disclosing and receiving information from third parties. In each Service, there will be **Data Sharing Agreements** to evidence how data is safely shared with other partners.