Rushcliffe
Borough Council

Rushcliffe Borough Council

Information Management and Governance Strategy 2022-25

Greg Dwyer – ICT Services Chief Information Officer

RUSHCLIFFE - GREAT PLACE ▪ GREAT LIFESTYLE ▪ GREAT SPORT

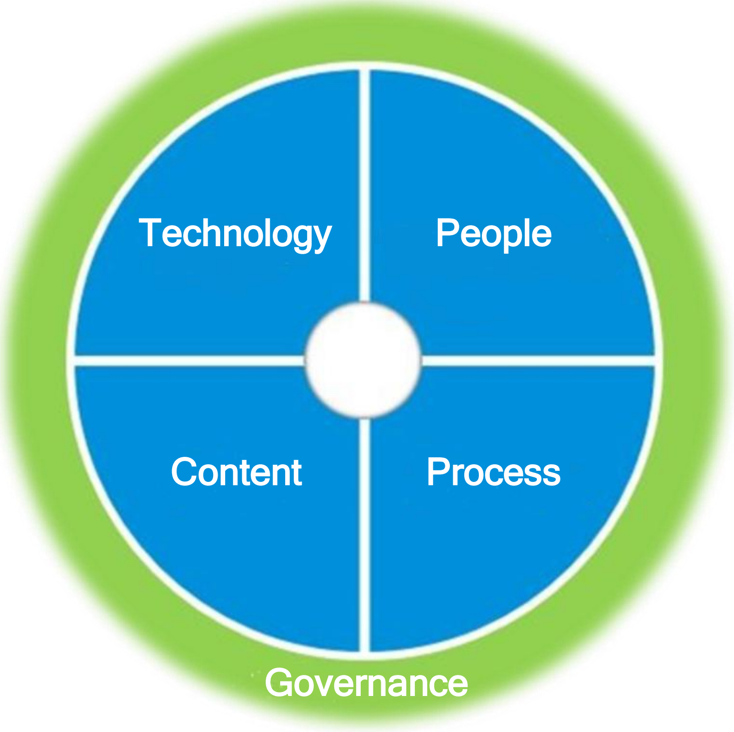
Table of Contents

Purpose

Information comes in so many different forms that it can sometimes be overwhelming. This Information Management and Governance strategy strives to ensure all the information the Council has (called Information Assets) is relevant, available, reliable, and secured for it to be used as an asset to benefit the Council and our residents, and not seen as a burden.

The wide adoption of cloud-based technologies such as Office365 can add more confusion and uncertainty when managing your information. For example, to allow employees to save data in multiple locations outside of your organisation or have unrestricted access to share and collaborate with other parties. All these scenarios could easily lead to a data breach if cloud-based technologies are left ungoverned. There are tools and controls to help, but Information Management is much more than just technology. Business processes and practices underpin the creation of information, and employee involvement is necessary to successfully delivery Information Management projects, as well as maintain compliance. Therefore, included in this strategy are four areas of focus.

- **people**
- **process**
- **technology**
- **content**



Strategic Vision

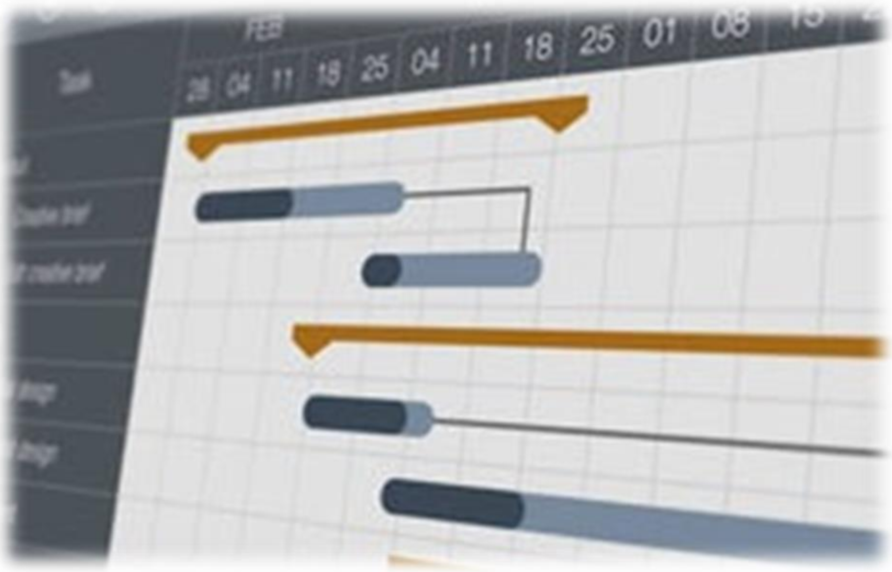
The **vision** of this strategy is to continue embedding high-quality Information Management practices and effective Governance controls across all service areas within the Council. This will ensure the Council continues to maintain high standards when handling and processing Information Assets, and for good Information Management practises to be embedded into the Council’s culture. Our goal is to simplify practices and use technology to provide efficiencies and automation where possible to lessen the burden of data management. To ensure that our residents’ privacy and personal data are handled appropriately, maintaining trust and confidence in the Council. These are the Council’s strategic Information Management and Governance goals:

- Ensure that Information assets are **actively** and **strategically** managed.
- Maintain **confidence** and **trust** our residents have in the Council.
- **Reduce** data management burden and complexities.
- **Simplify** data management process and procedures.
- Continue to embed **good practices** with our employees when handling and processing information assets.
- Ensure all information is **openly** and **easily accessible** to those who need it (respecting appropriate privacy, security, and confidentiality).
- **Automate** data management complexities where possible.
- Take advantage of **Cloud platforms** and technologies for **greater security, availability, and resilience**.
- Undertake **Engaging** and **informative** staff **awareness** campaign.

Project Objectives

This strategy will be delivered in a series of projects. Each of these projects are chosen carefully to have the greatest impact on Information Management challenges. Selected projects will be prioritised according to business need, strategic significance, and practical feasibility. Each project shown in this strategy will deliver a solution and will therefore see positive outcomes.

These are the projects the Council aim to deliver during the life of this strategy:



- Taking back control of unstructured data.
- Compliance made easier.
- Protecting Information Assets.

Rushcliffe
Borough Council

Take back control of unstructured data

Overview

Electronic data can be characterised as either structured, or unstructured data. The difference between them is how information is stored and governed (rules applied). Structured data stored in a database will have set rules applied, which determine how information is entered and stored. Unstructured data has no set rules and can be any file type or format stored in any way. The advantage of unstructured data is the speed in which it can be collected due to the lack of rules to follow. The downside is unstructured data can be overwhelming to manage, and the cost for storing it can quickly increase exponentially. The nature of unstructured data does pose risks to the Council the larger and more unmanageable it becomes. For this reason, it is important to adopt structured data principles when storing and processing unstructured data.

Deliverables

- To assist the Council’s policy ‘Smarter ways of working’, to ensure information assets are easy to access, manage, and provide agility and flexibility.
- Ensure that all information assets are stored for as long as necessary.
- Reduce the burden of manual data purges.
- Ensure information assets do not take up unnecessary capacity.

Project Actions

1. Implement a default retention policy for all unstructured data. A default retention policy will **simplify** process and procedures and **reduce** the risk of storing unnecessary data.
2. Implement automatic retention policies that allow employees **flexibility** to assign appropriate retention levels to their own information assets.
3. Set reasonable and appropriate storage limits to maintain **efficient** storage levels.
4. Migrate unstructured data to cloud platforms, taking advantage of **availability, flexibility,** and **automated** tools.

Compliance made easier

Overview

There are many things to consider when handling or processing information assets, which can be overwhelming; roles and responsibilities, information risks, storage duration, retention and disposal, protection and more… Sometimes process and procedures can also be over-complicated, which could lead to incorrectly processed data or at worst, a data breach.
There are also legal obligations to adhere to such as Freedom of Information Act, UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 that influence how data must be handled, processed, or shared. This project aims to simplify how employees handle and process data, whilst remaining compliant with UK Data Protection Law.

Deliverables

- Annually track UK GDPR compliance across all service areas to ensure the Council continues to meet its legal obligations.
- Continue to embed good practices to maintain employee confidence and accuracy when handling or processing data.
- Maintain a robust set of policies that provide guidance on how to handle and process information assets.
- Ensure all systems holding information assets must be easily searchable to efficiently satisfy FOI and SAR requests.
- Provide an easy way to classify information assets.

Project Actions

1. **Simplify** data input when populating tools such as the Information Asset Database or Records of Processing Activities.
2. Implement a UK GDPR **compliance** programme and maintain the existing **policy** framework to ensure **good practices**.
3. Maintain training and communication plans to ensure staff awareness campaigns remain **engaging** and **informative**.
4. Utilise UK GDPR tools for existing systems to **automate** retention and **simplify** information gathering for FOI and SAR.
5. Create a suite of **flexible** sensitivity labels that **automate** or manually classify information assets.

Protecting Information Assets

Overview

An Information Management strategy must consider Information Security, especially when cyber-attacks are one of the highest risks to information assets. Information assets are business-critical, which ensure the function of the Council, and the delivery of services to our community. It goes without saying that principles such as ‘Data Protection by Design and by Default’ or ‘Privacy by Design’ must be applied by the Council to ensure good practices are being followed when storing, handling, and processing information assets.

Deliverables

- Continue to apply Data Protection by Design and by Default principles to safeguard our resident’s data and privacy.
- Ensure accuracy of all information assets.
- Continue to follow these three principles: Confidentiality, Integrity, Availability (CIA Triad).
- Be accountable, and ensure that all Information Risks are identified, assessed, and mitigated straight away.

Project Actions

1. Adopt Role-based Authentication Controls (RBAC) across all systems to provide **greater security**.
2. Integrate **data protection** into every aspect of project and processing activities.
3. Consider privacy and data protection issues at the design phase of any system, service, product, or process, and throughout the lifecycle.
4. Deploy **Immutability** and **Endpoint Detection and Response** (EDR) systems to protect, log and monitor all information assets.

Responsibilities

The Council embraces a culture of responsibility, and information assets should be no exception to the rule. An information management structure exists across all service areas, assigning responsibility for their information assets. The following structure makes it clear who is responsible.

- **Accountable Officer (AO)** is the Chief Executive and has overall responsibility for ensuring information risks are assessed and mitigated to an acceptable level.
  Information risks should be handled in a similar manner to other major risks such as financial, legal, and reputational risks.
- **Senior Information Risk Officer (SIRO)** is a senior manager familiar with information risks and leads on the Council's response.
- **Data Protection Officer (DPO)** is an essential component of a data privacy accountability framework, playing a crucial role in enabling organisations to ensure, and to demonstrate data protection compliance. Under UK GDPR, the Council is required to have a DPO role because of its status as a Public Authority. As such, the DPO becomes a statutory responsibility.
- **Information Asset Owner (IAO)** are lead specialists involved in running their corresponding department. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they can understand and address risks to the information and ensure that information is fully used within the law for the public good and provide written input to the SIRO annually on the security and use of their asset.

Governance

Policy Framework

The information ‘Management Security Policy’ centre contains all policies needed to help the Council maintain the security of its information assets. It is important that all employees are aware of their individual responsibilities to ensure that information assets remain secure, and safeguards are followed to protect our resident’s rights, freedoms, and privacy.

Corporate Information Governance Group (CIGG)

This group meets every six months and provides appropriate governance and challenge required to oversee and ensure the Council policies and good practices are followed to comply with UK General Data Protection Regulation (UK GDPR) & Data Protection Act 2018. All information assets and personal data processing activities are identified, and any known Information Risks are mitigated, aligned with the Council’s Risk Management strategy. Any related security and information management policies are monitored to ensure the Council remains up to date with current or new legislation changes.
Members of this group ensure coverage across all services:

- Chief Information Officer (SIRO & DPO) (As Chair)
- Director of Finance and Corporate Services (As Sponsor)
- Senior Solicitor (Monitoring Officer)
- Human Resources Manager
- Service Manager representative from each Service Area.

Annual SIRO Audit and report to EMT

This is the Annual Assessment of Information Risk Performance Report for Rushcliffe Borough Council collated by the Senior Information Risk Officer (SIRO). It is a summary of the Information Management Annual Assurance Assessments provided by each Senior Manager in their role as an Information Asset Owner (IAO).

It provides an annual assurance statement that the risks to Information Assets in each service area are under control, including actions to mitigate any identified risks or issues.

Action Plan

The table below sets out a pre-determined timeline when all project actions from this Information Management Strategy will be delivered.

No	Taking back control of Unstructured Data	People	Process	Technology	Content	Delivered By
1	Set default retention policy for all unstructured data	✓	✓			Dec 2022
2	Automatic retention policies assigned to unstructured data	✓		✓		Mar 2023
3	Set reasonable and appropriate storage limits			✓	✓	Dec 2023
4	Migrate unstructured data to cloud platforms	✓	✓	✓	✓	Mar 2025

No	Compliance made easier					Delivered By
1	Simplify the Information Asset Database & Records of Processing Activities tools	✓		✓	✓	Apr 2022
2	Implement a UK GDPR compliance Programme	✓	✓		✓	Mar 2023
3	Staff Awareness Campaigns	✓				Rolling
4	UK GDPR Complaint systems for easier retention, and information gathering	✓	✓	✓		Mar 2024
5	Create flexible sensitivity labels that automate, or manually classify information assets	✓		✓		Sep 2022

No	Protecting Information Assets					Delivered By
1	Adopt Role-based Authentication Controls (RBAC) across all systems	✓	✓	✓		Mar 2024
2	Integrate data protection into every aspect of project and processing activities	✓	✓	✓	✓	Rolling
3	Consider privacy and data protection issues at the design phase	✓	✓	✓	✓	Rolling
4	Deploy Immutability and Endpoint Detection and Response (EDR) systems		✓	✓	✓	May 2023