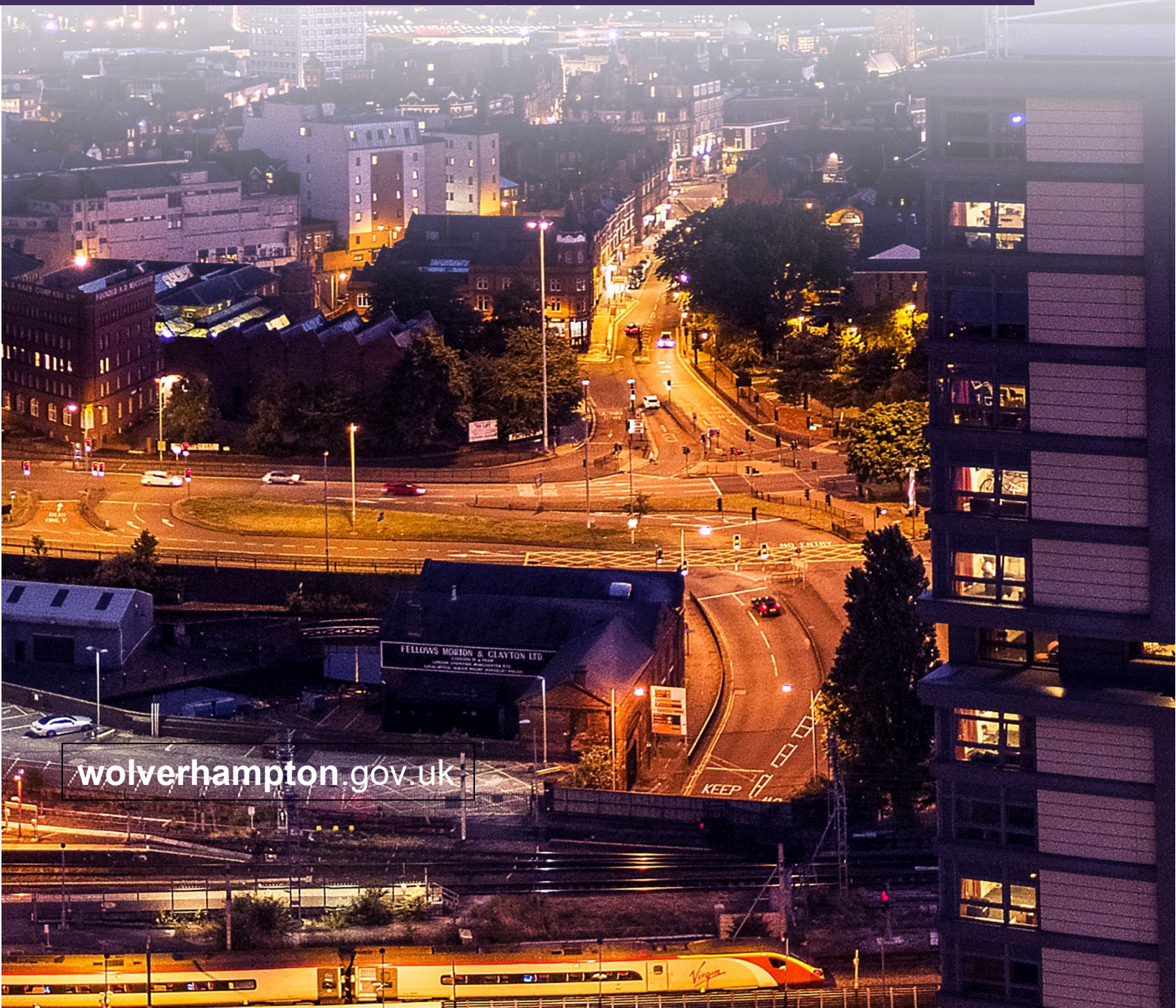


# Information Governance and Data Management Strategy 2024-2026

IG00



[wolverhampton.gov.uk](https://www.wolverhampton.gov.uk)



## Version History

Version	Date	Description	Author/Role
0.1	01/07/2021	Initial Draft. With thanks to Gloucestershire County Council	Kate Collins and Stuart Taylor. Information Governance Technical Specialists
0.2	09/08/2021	Review by wider Information Governance Technical Specialists and DPO	IG Team
1.0	17/02/2022	Approved by members of IG Board and SEB	IG Team
2.0	05/12/2023	Scheduled review	Information Governance Team

## Table of Contents

Version History .....	1
Executive Summary .....	2
Overview .....	2
Benefits .....	4
Citizens .....	4
Staff .....	4
The Council .....	4
Legal and Regulatory Requirements.....	5
Compliance and Accreditation .....	5
Information Assets .....	6
Records Management.....	6
Transparency/Reuse of Public Data .....	7
Information and Cyber Security.....	7
Information and Data Sharing .....	8
Privacy by design.....	9
Data Quality .....	9
Training and Awareness .....	10
Measuring Success.....	10
Costs, increasing financial constraints, resources, .....	11
Monitoring and Review .....	11
Further Information and Related Documents .....	11

## Executive Summary

Information and data are critical to every part of the Council's business. Managing and using it correctly, protecting it appropriately and making it available to both stakeholders and the public enables the Council to fulfil its objectives, deliver improved services and increase our standing with the public.

Key themes in the strategy are to

- Continually improve the Council's information management framework to achieve greater value from our data to aid in informing decisions and achieving better outcomes for our communities.
- Sustain our focus on the important themes within information management so that the public and partners can maintain trust and confidence in the way we operate.
- To be open and transparent in the way the Council operates, providing easy access to data and information.

But, increasing demands for the right to government information and data means the relationship between the citizen and the public sector is changing. We are also entering a new digital era which will transform the way that public services are used and delivered. In responding to these challenges, the Council is embracing a move towards greater openness and maximising the value of information to help facilitate closer collaboration and digital services.

This information governance and data management strategy sets out our approach to managing our information to achieve the right balance between making information more widely available to the public, whilst ensuring that robust protection is in place.

## Overview

Information comes in many forms such as policy documents, research papers, minutes, statistics, operational data, case files, personal data. It is held in a variety of printed and electronic formats across the Council. We use this information in our daily working lives as we work to achieve our objectives, whether it be delivering services, formulating policy, managing projects, holding meetings or managing staff.

Services are often delivered in partnership or are commissioned from third parties. This requires additional safeguards when managing our information: we need to ensure that information ownership is clear, the right people have appropriate access to the right information, and it is handled correctly throughout its lifecycle.

The Council is transforming the way we do business with our customers and increasing provision of digital services. The Council's digital vision is to digitally connect our community, city and Council and put the power in people's hands by being an insight driven organisation. Improved digital options so that more customers

choose to do business with us online, through increased self-service, leading to more end-to-end transactions, more mobile working, automated workflow and virtual contact by staff; good information management is an essential part of this.

Evidence-based decision making requires good quality, relevant and timely information and data interrogation tools to support service delivery and the planning of future services, performance monitoring and nationally required returns. We need flexible and agile teams across the Council; staff need secure access to the information they need, at any time, from anywhere.

To encourage a 'One Council' approach and reduce silo working, records must be regarded as a Council asset rather than individual/service assets. This means a change of culture from relying on information held by individuals in their personal drives and email stores, as well as manual storage units.

In addition, there is now more external scrutiny of how councils manage their information, through enhanced data protection legislation, and a move towards greater openness and transparency around the information that we hold.

To maximise the potential benefit from our information, we need to manage it effectively, re-use it where we have a legal basis to do so, share it appropriately and ensure that it is robustly protected. Past experience has shown us that this does not always happen – information that is not managed properly may be lost, shared with the wrong people or not found at all.

Poor data quality and failure to manage information appropriately can lead to:

- Less value for money in terms of service delivery
- Additional costs of recreating or recovering lost information, and storing or digitising information we don't need.
- Poor outcomes for customers, poor decision making, difficulty, delays or additional costs in providing on-going services.
- Poor external inspection outcomes
- Loss of access to information (e.g., security incidents or systems unavailable) impacting rights and freedoms
- Penalties and fines.

This strategy sets out the City of Wolverhampton Council's approach to improving the way the Council creates, uses, manages, shares and protects information to achieve the Council's objectives and effective partnership working.

## Benefits

When information and data is well managed it brings a number of benefits both to citizens, staff and the Council:



### Citizens

- Your information is accurate, reliable and accessible.
- You will know what information we hold, how we use it and whom it is shared with.
- You will be confident that your information is protected and handled appropriately.
- Decisions that affect you are more transparent.
- You can engage and collaborate with us in achieving our aims.
- You can hold us to account

### Staff

- Your information is accurate, reliable and accessible.
- You will know what information we hold, how we use it and whom it is shared with.
- You will be confident that your information is protected and handled appropriately.
- Decisions that affect you are more transparent.
- You can engage and collaborate with us in achieving our aims.
- You can hold us to account

### The Council

- We can keep information protected and secure.
- We build trust in the quality of our information both for staff and the public.
- We can provide more effective services and help control costs.
- We can be more transparent.
- Our decisions and policies are better informed
- We can comply with legislation.

## Legal and Regulatory Requirements

There is a complex legal framework under which we must manage the information we are responsible for. This includes, but is not limited to, the following:

- Data Protection Act 2018
- UK General Data Protection Regulations (UK GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2005
- Re-use of Public Sector Information Regulations 2015
- Public Records Acts 1958 and 1967
- Local Government Acts 1972, 1985, 1988 and 1992

In addition, there are many information requirements specified in legislation governing the provision of services to children, adults, and other Council services.

Further regulatory requirements include, but are not limited to.

- Records Management Standard BSI008
- Caldicott principles
- Local Government Transparency Code of Practice
- Lord Chancellors Code - Section 46 Code of Practice under the Freedom of Information Act
- ICO Data sharing: a code of practice

## Compliance and Accreditation

Accreditation is the formal recognition that an organisation is competent to perform specific processes, activities, or tasks (which are detailed in a scope of accreditation) in a reliable, credible and accurate manner. These accreditations provide assurance to citizens and partners that we have appropriate measures in place to secure information.

We are committed to maintaining the following relevant accreditations, to ensure we meet minimum standards imposed by legislation and regulation:

- Public Services Network (PSN)
- Data Security and Protection Toolkit (DSPT)
- Cyber Essentials Plus
- Archives Service Accreditation (National Archives)

## Information Assets

Regardless of the format e.g., paper, electronic, or microfilm. It will often be a collection of business information, for example information held in the social care system and any supporting files and documents would collectively be an information asset.

Managing information assets involves understanding what information is held and any legal reasons why. What is added and removed, how information is stored and shared, and who has access and why. It is important that our information assets are properly managed so we can understand and address risks to the information and data and ensure that information is only used within the law for the public good.

We will:

- Ensure that information asset ownership and responsibilities are clear.
- Maintain a register of our information assets, owners and types of processing.
- Provide sufficient information and training to asset owners to ensure data risks are managed effectively.
- Continue to work towards a comprehensive overview of core business data, using tools such as the information asset register, register of processing activity (ROPA) and information flow mapping.

## Records Management

The management of information in systems throughout its whole life; creation, storage, use and retention/disposal.

Many Council staff spend a high proportion of their time creating, gathering or managing information. Information is a valuable asset, and we can create efficiencies by continuing to work innovatively in the way we manage and use it.

We will:

- Maintain a records retention schedule.
- Ensure secure confidential waste facilities are in place.
- Continue to ensure new projects, processes and service reviews store all key information electronically, where feasible.
- Strive to ensure records are captured electronically at creation.
- Keep records securely and accessible to those who need to use them.
- Ensure they are disposed of securely at the end of their retention period.
- Maximise the use of existing technology to help users manage and use information more effectively.

## Transparency/Reuse of Public Data

There are increasing demands for transparency of public sector information. Each year we see a significant growth in the number and/or complexity of requests for information under Data Protection, Freedom of Information and Environmental Information legislation.

We will:

- Manage requests for information.
- Regularly review practices to ensure we are best placed to deal with the ongoing increase in volume and complexity of requests.
- Keep up to date with ICO guidance and decisions, and case law.
- Develop and upskill an internal network of key staff.
- Promote the public's rights of access to information on our website.
- Analyse requests to identify additional information that can be proactively published.
- Publish responses to requests in a disclosure log.
- Publish information in accordance with the mandatory requirements of the local government transparency code.
- Look to open up our data to encourage those with digital skills to develop solutions for the public.
- Continue our programme of proactively publishing information and datasets to support requirements of openness, transparency and accountability.
- Ensure FOI responses provide access to information in a re-usable format.

## Information and Cyber Security

The significance of information and related technologies is increasing in most aspects of business and public life, with the associated information security and cyber threats also increasing.

We therefore have a greater need to mitigate information risk and protect our information and related ICT assets from ever changing threats.

Security is an essential part of managing information. We are expanding our understanding of information risk management to encourage proportionate security measures that reflect a balance of the risks and the benefits. We are developing an all-encompassing approach to protecting information through a combination of ICT technical and nontechnical security measures.

We will maintain and develop appropriate technical measures, including:

- System security standards for new systems.
- Network protection, including firewalls, antivirus software and penetration testing.
- Password standards.
- Data classification standards and tools.



- Secure channels for interacting with customers.
- Monitoring of information security controls used by our data processors.
- Understanding of security weaknesses and incidents, implementing improvements as required.

We will ensure appropriate organisational measures are in place, including:

- A framework of policies, guidance and self-help tools.
- UK GDPR self-assessments with prospective suppliers to ensure compliance.
- Pre-employment checks that meet the Government standards.
- Mandatory training on protecting information and bespoke role-based training for staff who handle more sensitive data.
- Physical security to buildings.
- Secure transfer methods for physical records.
- Accounting for cyber risk.

## Information and Data Sharing

We work with a multitude of partners and suppliers and need to consider how information flows between us. We must ensure any sharing is legal and compliant with the Data Protection Act 2018.

To support this, we need to embed and strengthen information sharing agreements across the Council and its partners.

We will:

- Work with Multi Agencies, sharing information across the city.
- Promote use of the approved specific information sharing agreement template.
- Provide guidance to project managers, commissioners and contract managers to aid partnership working, implement privacy by design, reduce associated risks and ensure the whole information lifecycle is taken into account.
- Where relevant develop tools to enable an improved understanding of Council information and sensitivities before it is shared, e.g., information flow maps.
- Provide a secure means to store, organise, share and access information.
- Consider information implications and, where appropriate, undertake data privacy impact assessments (DPIAs) at the outset of commissioning services, major change projects or new contracts.
- Develop appropriate information governance, procedures and guidance before new technological solutions are implemented where feasible.

## Privacy by design

We deliver a wide variety of services to our city, some require us to collect, store, use, match, and analyse large amounts of personal data our citizens provide to us. We must ensure that any new, large scale or high-risk projects using personal data, have privacy designed into it at the very beginnings. This is to show we are handling people's data in safe and secure ways with the upmost respect for their privacy and comply with our requirements under the UK GDPR and Data Protection Act 2018.

We will do this by conducting Data Privacy Impact Assessments (DPIAs) and escalating any high risks to privacy to the ICO. The process is embedded into project management and procurement processes, and monitored via Leadership Team work.

## Data Quality

We will take the approach that data will be moved from each system to a business analytics platform for transformation and reporting and analytics. This will be managed and maintained by the corporate Data and Analytics Team in a hub and spoke model working with analysts in the wider organisation to a common set of standards.

We will:

- Provide a centralised data management service.
- Make reporting models made available to analysts.
- Ensure analysts have the data and tools they need to enable them to create and publish dynamic visualisations and dashboards.
- Make outputs available to other stakeholders such as team managers, heads of service, directors, members, partners and the wider public to access information on Council performance, as appropriate.
- Ensure data management is governed tightly through principles of access permissions, working within the confines of the DPA and UK GDPR, and any other data and information security standards.

## Training and Awareness

Training and awareness are key to bringing staff onboard to effectively protect the Council's information. Staff are our last line of defence in securing the important information and data that we hold; all staff therefore need to undertake mandatory training and be offered bespoke training according to their role.

We will:

- Ensure there are suitably qualified staff in place to advise the Council.
- Undertake a training needs analysis and provide mandatory training to all relevant staff.
- Provide bespoke training for key groups such as those dealing with personal and sensitive information on a regular basis.
- Ensure our information asset owners understand their responsibilities.
- Develop IG monthly bitesize key messages to communicate to our staff.
- Disseminate policies and key messages to all staff.
- Learn from security incidents, apply and share that learning across the organization via leadership teams.
- Offer targeted training to staff/services where incidents reoccur.

## Measuring Success

In order to know if the strategy is successful, it is important to have in place some performance measures, these include:

- Retaining PSN accreditation.
- Retaining Cyber Essentials Plus.
- Attain DSPT compliance (N3 connection).
- Monitoring of regulatory action taken by the ICO.
- Number of staff undertaken baseline protecting information training.
- Number of staff undertaken additional training.
- Number of serious incidents escalated to ICO or NHS Digital.
- Registers of data privacy impact assessments (DPIAs), information sharing agreements, records retention schedules.
- Percentage of formal requests (FOI, EIR, SAR) responded within legal timescales.
- Percentage of responses to formal requests resulting in an internal review.

## **Costs, increasing financial constraints, resources,**

In view of the large agenda and finite resources, it is necessary to prioritise areas of development activity in accordance with the associated risks. Priority areas for development each year are identified in accordance with Leadership teams and in agreement with our Strategic Executive Board and IG Board.

## **Monitoring and Review**

Ownership of this strategy rests with Information Governance Board members who are responsible for agreeing, monitoring, promoting and reviewing its implementation.

Due to the pace of change, the strategy will be reviewed every 2 years, or sooner if required.

An IG work plan will be developed to support this strategy yearly, the key elements of which will be incorporated into the annual work plans for Information Governance. Progress will be monitored half yearly to the Information Governance Board. Monitoring will also happen via accreditation to external standards, external and internal audit, and by the review of strategic risk registers.

## **Further Information and Related Documents**

This Strategy forms part of the Information Governance Framework, and should be read in conjunction with the other related policies within the framework which can be found here [What is Information Governance? | City Of Wolverhampton Council](#), and are as follows:

- AI00 Access to Council Information
- DP00 Data Protection Policy
- IS00 Information Security Policy
- RM00 Records Management Policy
- Information Governance Definitions, Roles and Responsibilities