ADUR & WORTHING COUNCILS

Adur District Council and Worthing Borough Council
Information Governance Framework
2025-2028

Document Control

Author	Senior Information Governance Officer
Version number	1.0
Date created	1st April 2025
Approval	
Distribution	
Next review date	1st April 2028
Classification	OFFICIAL

Version History

Version	**Version date**	**Summary of changes**
1.0	**1st April 2025**	

ADUR & WORTHING COUNCILS

Introduction

1. Information is a vital asset for the provision of services to the public and for the efficient management of Council services and resources. It plays a key part in governance, service planning and delivery as well as performance management.

2.Information governance is concerned with how information is held, obtained, recorded, used and shared. Information is used here as a collective term to cover things such as data, documents, records and content (electronic and paper).

3.The Council delivers and ensures that it is managing and using data 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.

4. It is essential that the Council has a robust information governance framework, to ensure that information, particularly personal, special category, sensitive and confidential information, is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and appropriate resources. It is essential that we sustain our focus on these important elements of information management so that the public can maintain trust and confidence in the way we operate.

Scope

5. The principles and commitments set out in this Framework and associated documents apply to all members, employees, trainees / apprentices and volunteers of the Council and to contractors, suppliers and partners delivering services on the Council's behalf.

Key policies

6. The key policies in this information governance framework are the:

- Information Security Policy - aimed at all staff (internal only)
- Information Classification and Marking Policy - aimed at all staff and public
- Data Protection Policy - aimed at all staff and public
- Data Sharing and Quality Policy - aimed at all staff and public

ADUR & WORTHING COUNCILS

	Strategy	INFORMATION STRATEGY
Why do we need to do this?	Policies - Identifies issues and scope	Data Protection Policy; Information Classification and Marking Policy; Data Sharing and Quality Policy
What is required?	Standards - establishes steps to take	Mandatory training, classifying and marking data, maintenance of Privacy Notices, Register of Processing Activities and Data Retention and Disposal Schedules, reporting of data breaches etc
How do we achieve this ?	Procedures - establishes good practices	Adhering to policies such as Clear desk policy, appropriate data sharing, ensuring security of data etc

7. These policies are supported by standards, procedures and guidance which are shown in the framework diagram below.

8. Outputs will be produced from use of these standards and procedures, for example Data Protection Impact Assessments, information awareness guides and training material.

Senior Roles

Chief Executive and Corporate Leadership Team

9. The Chief Executive is the Head of Paid Service who leads the Council's staff and advises on policies, staffing, service delivery and the effective use of resources.

The Chief Executive, together with Corporate Directors and Assistant Directors form the Council's Corporate Leadership Team (CLT) ensures the delivery of an effective Council-wide information governance approach. Quarterly reports are produced by the Senior Information Governance Officer (SIGO) / Data Protection

Officer (DPO) to measure progress, compliance performance and highlight any risks and opportunities.

Recommendations may be made to CLT by the DPO as part of a wider risk management agenda.

Member Authority and Review

10. The Worthing Cabinet Member for Resources and the Adur Cabinet Member for Finance and Resources are the Cabinet Members with responsibility for Data Protection, Freedom of Information, and Information Security within their portfolios.

The SIGO shall be responsible for ensuring the regular review of the Framework and shall report to Members on any required changes which are more than minor and inconsequential.

Senior Information Risk Owner (SIRO)

11. The SIRO is a member of the Corporate Leadership Team; is responsible for managing information risk in the Council and chairs the Technology and Information Governance Board.

The SIRO fosters a culture for protecting and using information within the Council and ensures information governance compliance with legislation and Council policies.

The SIRO provides a focal point for managing information risks and incidents, prepares an annual information risk assessment for the Council and gives strategic direction to the work of the DPO

Data Protection Officer (DPO)

12. All public authorities and organisations that collect and use large volumes of personal information must appoint a DPO . A DPO must act independently and is responsible for advising the Council on its data protection obligations; monitoring internal compliance with data protection law; informing and providing advice regarding Data Protection Impact Assessments (DPIAs); investigating data breaches and incidents; and acting as a contact point for individuals with concerns about the

way their data has been handled and the Information Commissioner's Office. (the UK Regulator for Data Protection).

Single Point of Contact (SPOC)

13. Within the Council, the Single Point of Contact is responsible for ensuring that the Council uses open surveillance / CCTV cameras in a way which is compliant with relevant legislation and the Surveillance Camera Commissioner's Surveillance Camera Code.

Information Asset Owners (IAO) / (UK GDPR Leads)

14. Each service has an Information Asset Owner (also known as a UK GDPR Lead) is accountable for identifying, understanding and addressing risks to the information assets within their specific services as well as ensuring good information governance within their business unit. GDPR training is mandatory for all GDPR Leads.

They are the first point of contact for colleagues regarding any UK GDPR-related queries within their service. They are also responsible for signposting their colleagues, being aware of the UK GDPR governance framework procedures, noting any gaps in knowledge or breakdown in procedures.

They ensure that procedures are followed in their service area, especially by maintaining and/or updating their service area's Privacy Notices, Register of Processing Activities and Information Retention and Disposal Schedule.

The IAO supports the SIGO and notifies of any issues/updates and when stepping down from the role, ensures there's a hand over to the new Lead.

They ensure information is held, used and shared appropriately and support the DPO to address risks to the information.

Information Asset Owners must understand what information is held within their service, what is added/removed, how information is moved and who has access and why. *The IAO is not necessarily the creator or primary user of the asset, but they must understand its value to the council and in particular, their own service block.*

ADUR & WORTHING COUNCILS

Technology and Information Board

15. The Board is chaired by the Head of Technology and Design and attended by the Information Security Officer, Platforms Manager, DPO/SIGO and other IT/Digital Management and staff members as necessary.

Officer Resources

Digital and Technology

16. The Ask Digital IT function and Security team are the lead for cyber security management and advice for the Council's IT infrastructure. They are responsible for providing and maintaining the technical architecture, required to enable good data quality across the council; supporting staff to use the tools and assets within this architecture.

Legal Services

17. The role of Adur and Worthing Councils Legal Services is to provide a legal service representing and advising the Councils and supporting and facilitating their functions. This includes providing a service to the Councils' bodies such as the Cabinets, Committees, Working Groups and individual Members/Officers exercising powers under delegated authority.

It is not the role of Legal Services to advise or assist third parties, i.e. members of the public or Members or Officers in their private capacity as individuals.

Information Governance Team

18. The Council has dedicated resources to support the implementation of its Information Governance Framework. The role these teams play in that regard are briefly set out below.

The IG Team provides expert advice, guidance and training to all staff on Information Governance and supports the DPO in their role. The IG Team coordinates the management and reporting of data incidents and breaches; supports the production of DPIA's and Information Sharing Agreements (ISAs) to minimise information risk;

maintains information to evidence compliance with data protection law (e.g. annual reviews of service Privacy Notices, Register of Processing Activities and Retention/Disposal Schedules).

Advice and guidance on data quality and more technical aspects of data minimisation (i.e. anonymisation and pseudonymisation) is also provided.

The IG Team log information rights requests (e.g. Subject Access Requests (SARs); erasure requests etc), Freedom of Information requests and Environmental Information requests and assigns them to services.

Service Information Officers (SIO)

19. Each service has a SIO, who must:-

Monitor the nominated SIO mailbox for requests for information (RFIs) and ensure that allocated colleagues also have access to the nominated email accounts, to cover periods of absence and to arrange this through Ask Digital, if necessary.

Monitor and respond to outstanding RFIs using the Mats RFI SIO Portal - Guidance on how to use this can be found in the Mats RFI System - SIO User Guide. (Internal document).

Provide the information requested to the Information Officer (IO) via the RFI system within the time scales specified, or notify IO as soon as possible if unable to provide the information within the statutory timescales.

Raise any concerns about disclosing the requested information, or if further clarification is required from the requester, with IO.

Liaise with their Head of Service on the response and consult with any third party whose interests may be affected by disclosure.

Complete the mandatory Information Certificate on the Learning Hub; the training is valid for 2 years from the date of completion.

Familiarise themselves with the FOI/EIR Act & exemptions/exemptions and follow the FOI/EIR Publication Procedure.

Complaints and Customer Feedback Team

20. The Corporate Complaints Process (Make a Complaint), has two stages and Managers are asked to try and resolve all problems before they become a formal complaint:

Stage 1 - Service Manager
Stage 2 - Director for the relevant service

The Insight Team acts as a point of contact for all compliments and complaints received and they will log them onto the system and assign them to the relevant Head of Service, who will re-assign it to the appropriate officer for acknowledgement and response as appropriate.

General responsibilities

21. All Council Directors and Managers are responsible for promoting and monitoring the implementation and adherence of this Information Governance Framework and its associated standards, procedures and guidance within their directorates and services.

22. All staff are responsible for ensuring they apply this Information Governance Framework, its associated standards, procedures and guidance to their work and the information they handle.

23. Wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter which could lead to dismissal or the termination of their employment or service contracts.

Training and guidance

24. Information Governance training for all staff is mandatory at induction and periodically thereafter, in line with the corporate training standards for information governance.

ADUR & WORTHING COUNCILS

25. All agency, voluntary and other staff with access to Council systems and data will be required to undertake the training in line with requirements.

26. Bespoke training modules for specific information governance and / or certain business roles are delivered to front line staff. The requirements and standards for these have been developed, agreed and will be kept under review.

27. Training compliance will be monitored by the Senior Information Governance Office/Data Protection Officer and reported regularly to the Technology and Information Board.

28. Awareness sessions may be given to staff as required, at team meetings or other events.

29. Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails and, on occasions, through targeted networking events and workshops.

30. Policies, procedures, standards and advice are available to staff at any time on the Data Protection and Information Governance hub of the Council's intranet.

Monitoring and review

31. This Information Governance Framework will be monitored and reviewed every three years in line with legislation and codes of good practice.

32. The policies, procedures, standards and guidance that form part of the Framework will be reviewed as set out in the individual documents.

33. A detailed review and change log of all documents which comprise this Framework will be maintained by the Information Governance team.

External Legislation

34. External legislation related to this policy includes:

- UK General Data Protection Regulation
- Data Protection Act 2018

ADUR & WORTHING COUNCILS

- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts
- Computer Misuse Act 1990

Further Information

35. Further information, advice or guidance on this document can be obtained from:

The Information Governance Team
By email: data.protection@adur-worthing.gov.uk