# Information Governance Policy

| | |
|---|---|
| **Author** | **Cheryl Lincoln; Head of Compliance and DPO** |
| **Approved by** | **Information Governance Steering Group** |
| **Approval date** | **May 2026** |
| **Review date** | **May 2029** |

Havant
BOROUGH COUNCIL

# Information Governance Policy

## 1. Purpose

This policy establishes the key high-level principles of information governance and data protection in the council. It provides an overarching direction that ensures all staff are aware of their duties and obligations as set out by the Data protection Legislation and ensures all staff are fully supported through a framework of Information Governance Standards, Procedures and Guidance that are embedded into working practices and data processing activities.

Information is one of the core assets of the council and is vital for the delivery of quality services and the efficient management of resources. Information Governance consists of policies, procedures, roles and controls put in place to govern and control all information created, received, managed, shared and disposed of by the council.

This policy outlines the strategic framework of individual responsibilities, accountable roles and governance groups, and cooperation between information-related professionals, to build a culture that values information as an asset.

Information governance applies to all personal and non-personal information, regardless of its format, function or location. Managing information as an asset is not about IT systems but about taking ownership of the information content within and between systems to ensure it is of value, and not a liability, to the council.

## 2. Scope

All employees, casual and agency workers, councillors, volunteers, contractors, partners, consultants and service providers are responsible for appropriately managing and storing the information they create and receive as part of council business.

### 2.1 All employees, casual and agency workers, volunteers

- all users of council information must understand and comply with this policy and associated policies
- employees are bound by the Code of Conduct for Officers to properly protect confidential data and not use it for unauthorised purposes
- failure to comply with this policy or associated policies may result in disciplinary action

### 2.2 Agency, contractors, third party suppliers

- must comply with this policy and associated policies in line with their contract or agreement

- failure to comply with this policy or associated policies may result in the termination of contracts or agreements

### 2.3 All managers

- must implement this policy and associated policies in their teams, including identifying and raising information risks with the relevant Information Asset Owner

### 2.4 Councillors

- should comply with this policy and associated policies in line with the Members' Code of Conduct

Certain roles within the information governance framework are specified, with duties as set out below in section 5.

# 3. Introduction

Public authorities rely on the collection of an ever-increasing amount of information to inform their strategies and plans to provide community and regulatory services. This policy sets out the framework within which the council will promote a culture of good practice around the processing of information and the use of information systems and details the agreed approach for achieving this.

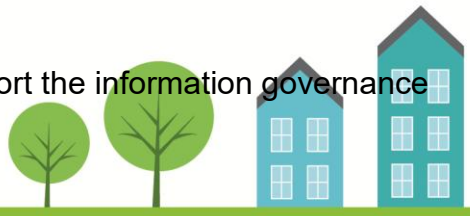
Information is a valued corporate and public asset, and a key resource required to deliver the council's business objectives and to meet the expectations of our customers. Moreover, the council needs to be open in the way it does its business; in how it delivers its services to its customers and in how it makes decisions.

The council applies a risk-based approach to Information Governance which principally focuses on customer safety, business transparency and legislative compliance.

# 4. Policy details:

### 4.1 Information principles

Our information principles guide the future direction of work to support the information governance framework.



These are a common set of principles used across the public sector. For more information see Information principles - The National Archives:

- information is a valued asset – information is an asset which is fundamental to the efficient and effective delivery of public services
- information is managed – information is stored, managed, protected and utilised in a manner that reflects its value
- information is fit for purpose – information must be accurate, valid, timely, relevant and complete to ensure that it meets the purposes for which it is intended
- information is standardised and linkable – the opportunities for using information greatly increase when it is made available in standardised and linkable formats
- information is reused – the value of information can be multiplied by re-use, and therefore opportunities to reuse should be looked for proactively
- information is published – public information should be published, unless there are overriding reasons not to
- citizens and businesses can access information about themselves – citizens and businesses should be able to access information about themselves, along with an explanation of how this information is used

## 4.2 Information Security

The council has, available on its intranet pages, policies, procedures, guidance and training to ensure the effective and secure management of its information assets and resources. The council also maintain business continuity procedures.

The council has incident reporting procedures in place and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

This policy should be read in conjunction with the ICT Security Policy which sets out the overarching approach to Information and Communication Technology (ICT) policies in the council and are available on the council's intranet.

Non-compliance with this Policy and the associated Information Governance standards, procedures or guidance could potentially expose the council and/or its customers to significant levels of risk. The potential impact of such risks through the damage, unauthorised disclosure or loss of information includes but is not limited to:

- disruption to services,
- the risk of harm or distress to citizens,
- damage to the organisational reputation,
- legal action,
- monetary penalties,
- personal distress,

- loss of confidence,
- or media coverage

and may take considerable time and cost to recover from.

# 5. Roles and responsibilities

## 5.1 Chief Executive

The Chief Executive has overall accountability for information governance.

## 5.2 Strategic Leadership Team:

The Strategic Leadership Team (SLT) have oversight of information governance and are responsible for supporting initiatives within their service areas.

## 5.3 Governance Committee

The Governance Committee is responsible for providing independent assurance on the adequacy of the council's risk management framework including internal control, financial reporting and information governance.

## 5.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is an SLT member responsible for managing information risk at the highest level. The Council's SIRO is the Corporate Director: Legal and Governance. The SIRO chairs the Information Governance Steering Group and has overall responsibility for ensuring the council's Information Asset Owners are carrying out their roles effectively. Key responsibilities are to:

- oversee the development of information governance policies and information risk management strategy
- ensure that the council's approach to information risk is effective, in terms of resource, commitment and delivery
- ensure that all staff are aware of the necessity for information governance and the risks affecting the council's information
- provide a focal point for managing information risks and learning from incidents
- prepare an annual information risk assessment for the Chief Executive to be included in the Annual Governance Statement

## 5.5 Data Protection Officer (DPO)

The DPO is an individual designated for the purposes of the UK GDPR, responsible for helping the council fulfil its data protection obligations. Key responsibilities are to:

- maintain expertise in data protection to provide advice on compliance with the UK GDPR and other data protection laws
- monitor compliance with the UK GDPR and other data protection laws, and with the council's data protection polices
- raise awareness of data protection issues, train staff and conduct internal audits
- advise on and monitor data protection impact assessments
- act as the first point of contact for the regulator and for individuals whose personal data is held by the council

The SIRO and the DPO will provide quarterly update reports to the council's Operational Management Team (OMT) which will include a diverse range of Information Governance issues. Any matters which require reporting to the regulator or areas of significant risk shall be reported to SLT.

## 5.6 Monitoring Officer (MO)

As the statutory officer in relation to the 'Access to Information[1]' rules, the MO determines whether reports, or parts of reports are 'exempt' or not for the purposes of Public Meetings run by the Democratic Services Team. The MO is responsible for advising on a councillor's entitlement to information.

The MO is also the "qualified person" for the purposes of determining, under FOIA, whether the exemption at Section 36 (exemption from disclosure of information which might prevent the free and frank provision of advice or exchange of views; or otherwise prejudice the effective conduct of public affairs) can be relied on.

## 5.7 Information Asset Owners (IAOs):

**Information Asset Owners (SLT)**
are accountable and responsible for managing risks to the identified information assets in their service areas. Information assets are any grouping of information, in any format, that has value in supporting your service's work. For more information, see Section 7 below.

**Information Asset Managers (Heads of Service/Managers/Team Leaders)**
are responsible for the day-to-day management of information and the risks of information used in their areas. Information Asset Managers are responsible for ensuring all information is retained or

[1] Part VA of the Local Government Act 1972, as amended in part by the Local Government (Access to Information) Act 1985.

deleted in line with the Retention Schedule, likewise, ensuring it is up to date. Information Asset Managers are responsible for notifying the Data Protection Officer of any changes in processes that deal with personal data.

IAOs may delegate tasks to information managers but retain overall accountability for their information assets:

IAO responsibilities are to:

- lead and foster a culture that values, protects and uses information for the public good
- know what information their assets hold, what enters and leaves them and why
- know who has access to their assets and why, and ensure use of their assets are monitored
- understand and address risks to the asset, and provide assurance to the SIRO
- ensure the asset is fully used for the public good, including responding to information requests

IAOs must assess whether information assets are still required. If not, they are responsible for fully decommissioning them and disposing of information once it has passed its retention period defined in the council retention schedule. Disposal of information is either by complete destruction or transfer to Hampshire County Council Archivist for permanent preservation.

IAOs must maintain entries for their information assets in the Information Asset Register and provide assurance to the SIRO about the management of their assets at least once a year, or sooner if there are changes, IAOs must formally review their information assets, assess the risks to their information and update the central Information Asset Register

## 5.8 Information Professionals

The council recognises that some colleagues are information professionals who are experts in one or more information disciplines that make up information governance, including data protection, IT and cyber security and business intelligence.

Information professionals advise on their areas of expertise in relation to corporate information risks and risks to individual information assets. These professionals sit on the Information Governance Steering Group to provide support and guidance. They will also support information governance at an operational level through their various working groups.

## 5.9 The Information Governance (IG)Team

Is responsible for ensuring the council remains compliant with the legislation referred to in this Policy, managing security incidents and ensuring that training and awareness programmes are in place so that staff are aware of and understand their obligations.

# 6. Governance groups

## 6.1 The Information Governance Steering Group (IGSG)

The IGSG provides overall direction, influence, and leadership for information governance arrangements.

The IGSG is chaired by the council's Senior Information Risk Owner (SIRO) and will:

- monitor compliance with Information Governance Policies and Strategies
- consider potential Information Governance risks
- support to the SIRO and DPO in performing their functions
- review data incidents
- monitor relevant IG performance measures and service areas compliance
- agree Information Governance work plans on a risk-based approach
- agree any significant Information Governance/Management issues to be reported to SLT
- approve an information management training and awareness programme that will meet the needs of the council.

Full details of the responsibilities of the IGSG are defined in the terms of reference and published on the intranet.

## 6.2 The Technical Design and Innovation Authority (TD&IA)

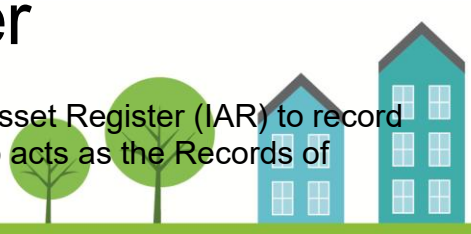
The TD&IA is a specialist group that:

- Supports the Council's Digital and Corporate Strategies;
- Aligns with existing or planned Digital projects and infrastructure;
- Promotes and enables innovation in a secure, safe and sustainable manner;
- Contributes to the Council's Enterprise Architecture.

The Technical Design and Innovation Authority acts to improve control over the way systems are tested, procured and implemented.

# 7. Information Asset Register

The Council will maintain an up-to-date and complete Information Asset Register (IAR) to record data about all information of value held by the council. The IAR also acts as the Records of



Processing Activities (ROPA) to meet Article 30 obligations of the UK General Data Protection Regulation (UK GDPR).

The IAR provides the basis for Information Asset Owners to assess how each asset is meeting its business need and for managing risks to this information.

Information assets are any grouping of information, physical or digital, that has value in supporting services' work.

Information assets have value to the organisation, are not easily replaceable without cost, time, or skill, and impact services if they cannot be accessed.

> *"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles."*
>
> *(The National Archives – Information Asset factsheet)*

Information assets should be defined at a granular enough level that they group together the work that supports a particular business activity:

- if information is used by more than one service, it should be described in one primary asset that has a single Information Asset Owner and referenced in other related assets
- assets can contain other assets. For example, the retention schedule defines some information assets at a broad level, and these are owned by SLT. The Information Asset Register should precisely define information assets according to their service and its locality

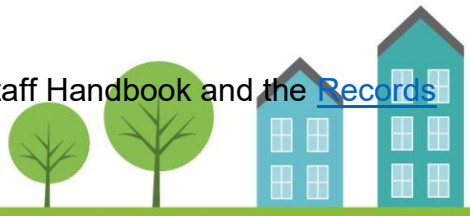
The IAR will be owned by the Head of Compliance

To ensure the Information Asset Register remains complete, the IG Team will work with services to undertake an annual review.

## 7.1 Records Management

Records management comprises processes and practices that ensure council records are systematically controlled and maintained, covering the creation, storage, management, access, and disposal of records, in compliance with best practice, legal obligations and policy requirements.

More information on records management can be found in the IG Staff Handbook and the Records Retention and Disposal Policy.



# 8. Information risk management

Information risks will be handled in a similar manner to other major risks, such as financial, legal and reputational risks.

Risks to information will be identified, assessed and managed in accordance with the Corporate Governance & Risk Policy and Risk Management Framework.

# 9. Training

All employees must complete mandatory information governance training, as part of their induction and on an annual basis, as described in the supporting policies.

Information professionals, IAOs and IAMs should receive specialist training relevant to their role. Additionally, SIRO and deputy SIRO should receive suitable training.

Awareness sessions will be provided to teams on request and regular reminders on information governance topics will be published through corporate communication channels.

# 10. Compliance regime

The council will ensure compliance with relevant legislation, codes of practice and government standards.

The council complies with:

- **Data Protection Legislation** (UK GDPR, DPA2018 and DUAA) which relates to personal identifiable information. (See Data Protection Policy for more information)
- **Environmental Information Regulations 2004** which relates to requests about the environment (air, soil, water, environment e.g. Planning etc.). (see Access to Information Policy for more information)
- **Freedom of Information Act 2000** relates to requests not covered by the above (see Access to Information Policy for more information)
- **Common law of confidentiality**. (See staff IG Handbook for more information)
- **Local Government (Records) Act 1962 / Local Government Act 1972 and Lord Chancellor's Code of Practice for Records Management** relates to the local authority having records management policy and procedures in place

# 11. Organisational and technological change, service design and delivery

Information governance principles will be integrated into all relevant organisational processes e.g. change and project management, IT configuration and procurement.

Information governance responsibilities will be integrated into organisational structures and job roles

The council will use data and insights to drive improvement of our services. This is being delivered through the Data Use and Analytics Strategy.

# 12. Monitoring compliance

This policy will be supported by policies and strategies that will have their own monitoring and governance routes.

The Information Governance Steering Group (IGSG) will monitor and report on overall progress of information governance.

The SIRO will produce an annual report on information governance activity for SLT and Governance Committee.

# 13. Policy approval and review

This policy will be reviewed every three years by the Information Governance Steering Group or following any changes in legislation, regulations, or business practice.

Version control record

| Version number | Date | Author / reviewer | Comments / changes |
|---|---|---|---|
| V0.1 | 08/07/23 | Cheryl Lincoln | Moved to new template, split policy from strategy & framework and reviewed/updated content |
| V1.0 | 06/05/26 | Cheryl Lincoln | Approved by IG Steering Group and SIRO |