Bayside Council
Serving Our Community

Information Management Policy

25 March 2026

Information Management Policy
File: F22/192 Document: 25/272899
Policy Register: F16/951 Policy No.: PP26/13
Class of document: Council Policy / Administrative Policy

Enquiries: Manager Customer Experience

Telephone Interpreter Services - 131 450 Τηλεφωνικές Υπηρεσίες Διερμηνέων بخدمة الترجمة الهاتفية 電話傳譯服務處 Служба за преведување по телефон

Contents

1 Introduction

1.1 Background

The Information Management Policy establishes a governance framework for the creation, capture, control, use, maintenance, and disposal of records and information. It ensures compliance with relevant legislation, such as the State Records Act 1998, and other regulatory requirements. This policy defines the roles and responsibilities of all users of information including employees, contractors and third parties.

1.2 Definitions

Capture
Saving or registering a record into Councils approved corporate information systems whether hardcopy or digital. This may mean registering the record into Council's information system and assigning metadata to describe it and allow for the appropriate management of the record over its lifecycle.

Data
Data is typically comprised of numbers, words or images. Data is a representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means.

Information
Collection of data in any form, which may be transmitted, manipulated, and stored, and to which a meaning has been attributed. Information may include, but is not limited to: a written document, an electronic document, a webpage, an email, a spreadsheet, a photograph, a database, a drawing, a plan, a video, an audio recording, a label or anything whatsoever on which is marked any words, figures, letters or symbols which are capable of carrying a definite meaning to anyone.

Information and Data Governance
Information and Data Governance sets and guides the policies, structures, responsibilities and standards required for managing Council's information effectively, securely and in compliance with legislative requirements. It helps ensure that data is accurate, available and accessible. Information and data governance includes information and data architecture, modelling, integration and master data management.

Information Management
Information Management refers to all processes, tools and services that form the end-to-end solutions to plan, acquire, create, circulate, distribute, use, manage, retain or dispose of information according to legislative drivers and business relevance. The management of the various types of information may require different approaches and standards. Information Management includes information governance.

Information Systems
Information Systems are an integrated set of components (typically include hardware, software, databases, networks, people and procedures) for collecting, storing, and processing data, providing information, providing tracking data for a workflow process, providing knowledge, or storage and retrieval of digital products.

Record
Recorded information created, received, used or maintained by Council in the transaction of business which provides evidence of Council activities. Records contain information that reflects what was communicated or decided or what action was taken and therefore constitutes the evidence of activities.

System of Record
Designated information system as the authoritative and approved data source for storing and managing the specific type of information.

1.3 Policy statement

The policy outlines Bayside Council's responsibilities and strategies for information management, guiding the creation and management of information assets by all users and clarifying roles and responsibilities. It sets out the requirements to meet the State Records Act 1998 key compliance obligations for public offices. It aims to meet business needs, accountability requirements, and stakeholder expectations by ensuring information is well-described, stored in endorsed locations, accessible when needed by authorised persons, and protected from unauthorised access and disclosure.

1.4 Scope of policy

This policy applies to all users of information and all information assets (records, information and data) in any format, created or received, to support Bayside Council activities.

It covers all applications used to create, manage and store information assets, including dedicated information management systems, business information systems, databases, email, voice and instant messaging, websites, and social media applications. This policy covers information created and managed in-house and off-site, on all platforms.

This policy applies to:

- The Mayor, Councillors,, staff and all other users (including contractors, work experience students, apprentices, volunteers and consultants), vendors, and external service providers who are granted access to Council information assets and supporting technology or who manage and create Council's public records.
- All types of data, information and public records, regardless of format, medium and source which relate to the business and administration of Council.
- All data and information management activities including the way in which Council plans, identifies, creates, receives, collects, organises, secures, uses, controls, disseminates, shares, maintains, preserves and disposes of information under its control.
- All Council controlled or commissioned information systems and services which manage information and public records.

All practices and processes related to information systems and services associated with creating and managing information and public records.

Council's information management capabilities are delivered via:

- people (leadership, trained, shared knowledge, with assigned responsibilities and accountabilities, leadership and training),
- information (trustworthy, secured, discoverable, accessible, used and reused with confidence and insights),

- processes (planned, documented information systems and service design appropriate to customer and business needs and legislative requirements), and
- technology (enabling capture, storage, protection, discovery, access, and leveraging of information).

2 Information Management

2.1 Why is information management important?

We rely on information to develop policy and deliver services that are valuable to our community.

Good information management:

- Ensures the right information is readily available to the right people at the right time.
- Enables information to be handled securely, with appropriate protections for privacy and confidentiality.
- Allows Council to demonstrate that information is being created, used, maintained and disposed of with integrity so that we act in the interest of our community through the decisions we make and the actions we take.

2.2 Why is an Information Management Policy needed?

An Information Management Policy provides a structured approach to managing information effectively. It ensures consistency, security, and efficiency by establishing clear guidelines, processes and tools for handling data throughout its lifecycle.

2.3 What does success look like?

The outcomes of good information management are apparent to our community when Council can:

- Make well informed, transparent, and timely decisions.
- Deliver customer-centric services efficiently – making the most of every resource available and every interaction between Council and the community.
- Drive innovation by making information available for use by the business, in a legally, ethically and culturally appropriate manner.
- Be accountable through a secure and discoverable record of government that is valued by our community and used to by future generations.

In supporting these outcomes, the Information Management Policy:

- Defines a common set of principles for information management that support the development of strategies and plans at an agency level.
- Enables all users of Council information to understand the requirements for good information management.

While the focus of the Policy is information management, the technology used to achieve this is recognised as a critical enabler of information management.

3 Principles

3.1 Information Management principles

Bayside Council information management principles provide a quality benchmark for the management of information within our organisation. The principles outlined below must be implemented in practice at all levels of the organisation to ensure an appropriate level of information management maturity is reached.

a. Business-enabling, aligned to business needs and customer outcomes.

   Council only collects, creates, and manages information that directly supports organisational strategy, business functions and operations, services and delivery, and the needs of our customers. The use of Council systems to create, store, use and share information ensures the information we rely on for making insightful business decisions is readily available to those that need it. Information held in appropriate business systems is effectively managed, protected and made accessible as appropriate.

b. Secure, valued and managed as an asset.

   Council recognises that its information is a core component of our services and operations, so it needs to be supported and maintained as a secure business asset. This entails identifying corporate information assets, registering and tracking assets and assigning appropriate governance and management responsibilities to those assets throughout their lifecycle. Council provides an information governance structure, outlining clear information management roles and responsibilities

c. Trustworthy and used with confidence.

   Well-managed information is critical to the effective and efficient operation of our organisation by ensuring all users have access to the right information at the right time.

   Council shares information appropriately, ensuring the correct controls are in place to manage access, security, and privacy of the information held.

d. Managed across the full lifecycle, protected from unauthorised use and inappropriate deletion.

   The use of Council approved business systems, services, and repositories to create, store, use and share information, ensures the information is appropriately managed, maintained, protected, and secured. (see Appendix 1)

   All users must be aware of their responsibilities regarding making and keeping appropriate business records, and the retention and disposal of those records.

   Appropriate retention policies are applied to all information stored in enterprise information management systems.

e. Available and open to the community and Government in line with related policies such as the Government Information (Public Access) Act 2009 (GIPA Act).

f. Considered, planned and designed to inform business operations and support systems design, architecture, and maintenance programs.

Information management should be consciously planned and integrated into business operations, system design, and maintenance. Information must meet business and governance requirements, with specifications for its security and use. Information management principles must be incorporated into system design and change management to meet policy and legal obligations.

3.2 Legislative requirements for information governance

There is a body of legislation and policy that governs public information and records management. The key legislation governing information management in the NSW public sector includes:

- Data Sharing (Government Sector) Act 2015: Facilitates data sharing across government agencies to improve service delivery and policy-making.
- Government Information (Public Access) Act 2009 (GIPA Act): Promotes transparency by providing the public with access to government information.
- Health Records and Information Privacy Act 2002 (HRIP Act): Protects the privacy of individuals' health information.
- Privacy and Personal Information Protection Act 1998 (PPIP Act): Safeguards personal information held by public sector agencies.
- State Records Act 1998: Ensures proper management and preservation of government records.

3.3 Digital Records Management

Council has a legal obligation to manage its records and must be able to account for its actions and expenditure of resources appropriated by Council on behalf of the community. Information is a key Council asset and needs to be managed well to realise its value.

Digital management of records enables Council to make the best use of new technologies and innovative ways of doing business. It ensures that Council information is not lost in storage, is able to be searched for and therefore accessed and utilised by Council staff when needed.

It enables Council to implement information reforms more efficiently and effectively.

3.4 Creation and Capture

Records are created every time someone in Council writes an email, drafts a brief, writes a report or records minutes, adds data to a spread sheet or takes a photo.

This information is created as part of a specific business process and needs to be managed so that it can be searched, shared, reused and repurposed, and increasing its value to Council. Records need to contain specific information to make them complete, accurate and reliable.

The information needs to reflect:

- What happened, the order of events
- What was decided or recommended
- What advice or instruction was given
- When it happened and who was involved.

3.5 Access to Council Records

Bayside Council requires open access to information and records unless the record itself requires protection. Protecting our information and records are governed by:

- Council's Access to Information Policy
- Access to Information Guidelines for Local Government
- Privacy and Personal Information Protection Act 1998
- Health Records and Information Privacy Act 2002
- Government Information (Public Access) Act (GIPA) 2009

All Council records are public documents and must be managed to provide easy access by our community.

3.6 Records Security

Records should be stored within approved recordkeeping systems to prevent unauthorised destruction, alteration or removal. Council's approved recordkeeping systems have a full audit log, security and are managed and monitored.

- Council records must be stored only in Council's official recordkeeping systems – for example EDRMS, Finance System and Customer Request Management System

3.7 Disposal and Destruction of Records

General staff cannot destroy or dispose of Council records. Only authorised staff may destroy or dispose of Council records following strict procedures and with the final approval of the Coordinator Data & Information Management.

Records can only be destroyed in accordance with:

- The General Disposal Authorities
- NAP (Normal Administrative Practice)
- Council specific Disposal Authorities – FA450
- Transferred to State Archives for permanent retention.

Council records must be protected, maintained and accessible for their total retention period and must be disposed of in accordance with the State Records Act 1998 and Council's disposal procedures.

Information and records which staff deem as ephemeral, may be destroyed using a procedure called 'Normal administrative practice (NAP)'. This practice usually occurs because the records are duplicated, unimportant or for short-term use only.

3.8 Value of Records as a corporate asset

The records of Bayside Council are an essential resource for information as they:

- Are a vital asset which Council can use to make future decisions
- Are the major component of the Council's corporate memory and provide evidence of business transactions and decisions
- Exist for a variety of administrative, functional, historical and legal reasons
- Support policy formulation and consistent and equitable decision making.

3.9 Privacy Impact Assessments (PIA)

Privacy Impact Assessments will be developed for new initiatives, projects and procurement processes, including those undertaken by contractors and third parties. They will be used to manage, minimise or eliminate potential impacts and ensure compliance with appropriate legislation. This will be an important component of the 'privacy by design' process, ensuring that privacy considerations are built into projects from their conception through to implementation. This will be done in consultation with Manager Governance & Risk and will be aligned with Council's Privacy Management Plan.

4 Policy implementation

4.1 Policy responsibilities

Council Officials

It is the responsibility of all Council Officials to adhere to this Policy.

Relevant training is available to Council Officials through the Councillor Portal.

General Manager

Provides strategic direction and resources for effective information management and governance.

Directors

1. Ensures information assets are managed based on value and risk and stored in approved systems.

2. Ensures staff are trained in using information systems.

3. Ensures directorates follow proper governance and processes to comply with the Information Management Policy.

4. Endorses information management policies and procedures.

5. Promotes a positive information management culture in the directorate.

6. Reports risks and addresses policy breaches.

Managers

1. Leads compliance with the Information Management Policy, relevant policies, and legislation for managing information systems and assets.

2. Ensures data responsibilities are met for specified information systems.

3. Ensures staff are trained in using information systems.

4. Ensures information management is included in agreements with anyone accessing Council-managed information.

5. Reports risks and addresses policy breaches.

6. Ensures endorsed information systems support business needs.

Coordinator Data & Information Management

1. Leads the development and communication of the organisation's information management governance.

2. Leads the delivery of information management services.

3. Aligns information management investment with Council's strategic goals.

4. Ensures information systems produce and store accurate records.

5. Integrates information management into all Council business.

Data & Information Management Team

1. Manages Council's public records and implements record governance standards, providing advice on recordkeeping processes and compliance.

2. Identifies recordkeeping needs and supports business units with strategies to locate records.

3. Ensures staff understand recordkeeping responsibilities and provides training on obligations and procedures.

4. Supports business areas with managing public records, including scanning, registration, and handling incoming and outgoing correspondence.

Information Technology team

1. Provides technical support for information systems.

2. Advises on IT and services for information management strategies.

3. Manages vendors, contracts, software assets, and service integration for information systems.

4. Collaborates with business areas to define functional requirements for information systems.

5. Manages security to protect information from unauthorized access.

6. Advises on information and cybersecurity risks.

7. Guides information asset owners on security classifications and controls.

All users

1. Follows information management principles, standards, and best practices in daily tasks.

2. Creates and maintains accurate records of business activities for accountability and decision evidence.

3. Ensures records are captured in approved Council systems.

4. Stays aware of policies and legislation affecting Council's information management and complies with them.

5. Relevant training is available to staff via Council's Learning Bay and via the Annual Refresher Training.

4.2 Procedures

Procedures that support this policy, may be approved by the Director City Performance or Manager Customer Experience

- Records Destruction Procedure (using NAP)
- Records Retention and Disposal Procedure
- Records Archiving Procedure (NEW DOC)

5 Classifications

The purpose of document classification is to organise and categorise documents systematically to enhance accessibility, security, and efficiency. By assigning specific labels or categories to documents based on their content, sensitivity or purpose, organisations can ensure that information is easily retrievable when needed. Document classification also helps protect sensitive or confidential data by applying appropriate access controls and security measures. Additionally, it supports compliance with legal and regulatory requirements by ensuring that records are managed in line with established policies.

5.1 Public

Information that can be made available in the Public Domain and which would not cause damage or harm if released.

5.2 Internal

Information generally available to users within Council and which contains business value to the organisation, or which requires protection due to personal data. Access is restricted to users within the organisation in connection with their employment.

5.3 Confidential

Information whose unauthorised disclosure (even within the organisation) could cause serious damage in terms of financial loss, legal action, loss of reputation,

damage to individuals.

5.4 Highly Confidential

Information that, if lost, compromised, or damaged, would cause significant harm with ramifications external to the organisation, including significant damage to stakeholders, breaches of legislation, sustained negative media reporting and significant loss of trust or confidence in the organisation.

6 Access Controls

Specify who has access to different types of classified information and under what conditions. This helps in ensuring that sensitive information is only accessible to authorised personnel.

Classification	Restrictions	Example
Public	None	**Council meeting minutes and agendas:** Records of discussions and decisions made during council meetings. **Planning applications and decisions:** Documents related to land use and development proposals. **Annual financial reports:** Summaries of the local government's financial activities and status. **Public notices:** Announcements about upcoming meetings, public hearings, or changes in local regulations.
Internal	Access is restricted to users within the organisation in connection with their employment.	**Internal memos and emails:** Communications between staff members. **Operational reports:** Documents detailing the day-to-day activities of various departments. **Staff schedules and rosters:** Information about employee work hours and assignments. **Policy and procedure manuals:** Guidelines for how different tasks and responsibilities should be handled.
Confidential	Access is restricted to users with specific roles and clearance.	**Personal information:** Details about employees or residents, such as tax file numbers or medical records. **Legal documents:** Information related to ongoing legal cases or confidential legal advice. **Commercial negotiations:** Details of contracts or negotiations with private companies.
Highly Confidential	Access is highly restricted and must be explicitly authorised by the respective	**Personally, Identifiable Information (PII) regarding vulnerable population:** information, which by itself or combined with other information, could be used to identify, contact, or locate a person (e.g. name, email, phone number, birth date, passport number, Driver's License Numbers,

	Information Owner and the CIO.	Medicare or Centrelink numbers, criminal record, etc.) **Vulnerable populations other sensitive information** such as health information, vulnerability information, political affiliations and child protection incidents (e. g. images of children and case information) **Sensitive disciplinary matters** as determined by the Human Resources department **Fraud/ corruption investigation information** **Highly confidential audit reports** **Sensitive legal matters** as determined by the Legal department **Highly sensitive political, humanitarian or security information** **Whistle-blower information**

7 Document control

7.1 Review

This policy will be reviewed every two (2) years or as required by best practice or legislation changes.

The General Manager and Director City Performance may approve non-significant and/or minor editorial amendments to this document that do not change the policy substance.

7.2 Related documents

- Cyber Security Policy
- Data Breach Policy
- Access to Information Policy
- Legal Documents – Process & Operational Procedure
- Content Manager Business Rules & Procedures
- Privacy Management Plan
- Code of Conduct
- Information Classification and Handling Standard (NEW DOC)
- System of Record Register (NEW DOC)
- File Sharing Guidelines (NEW DOC)
- Privacy Impact Assessment template (NEW DOC)

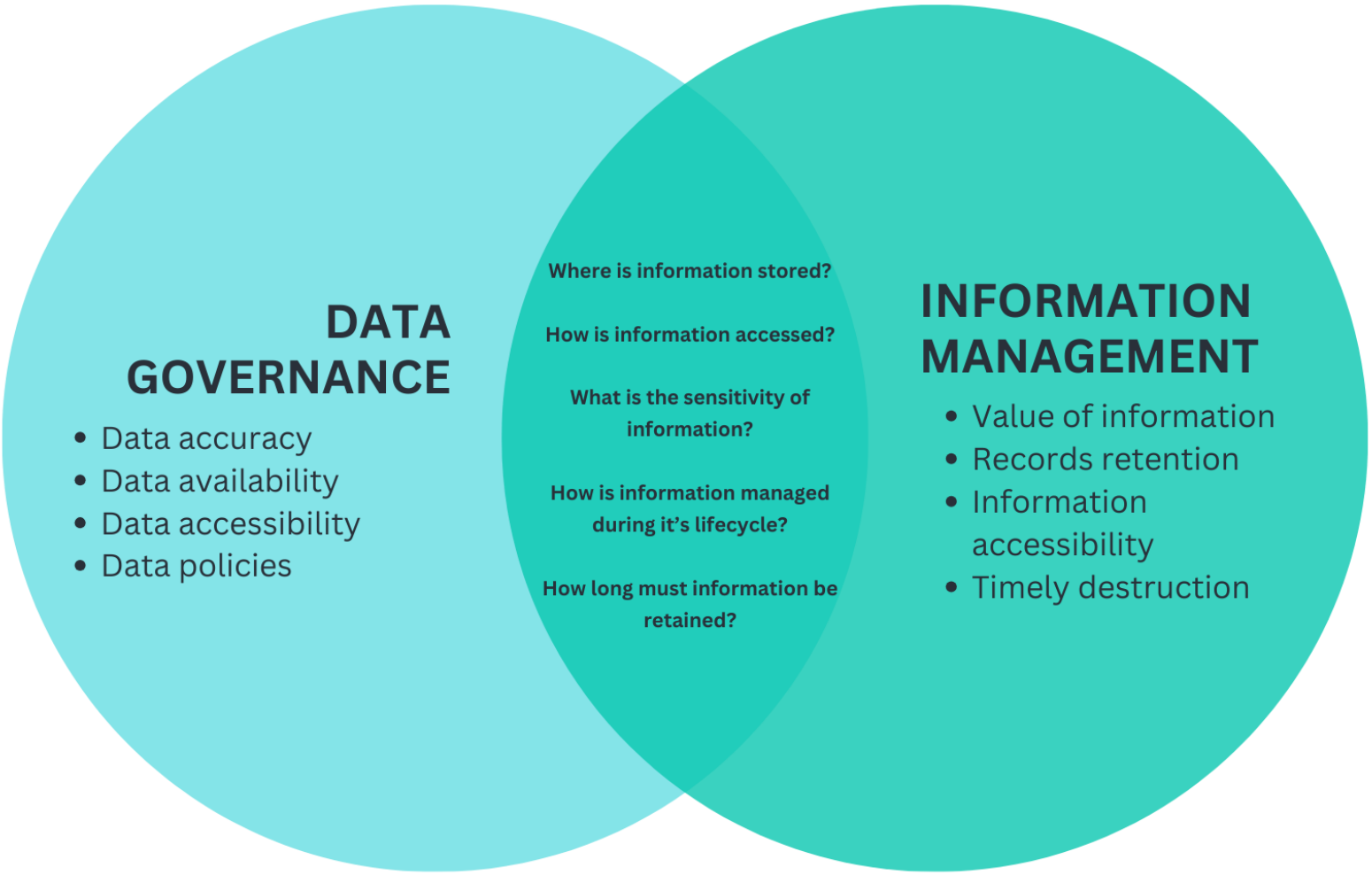
7.3 Version History

Version	Release Date	Author	Reason for Change
1.0	11/03/2026 (CP Com) 25/03/2026 (Council)	Information & Records Lead	New document

8 APPENDIX

8.1 APPENDIX 1 – DATA GOVERNANCE AND INFORMATION MANAGEMENT

Data Governance and Information Management share the joint interests of preservation, retrievability/accessibility, integrity, security and quality of data and records respectively.



8.2 APPENDIX 2 – WHERE TO SAVE BUSINESS INFORMATION

Where to save different kinds of business information

The purpose of this diagram is to help determine where different Council records need to be stored according to Information Management requirements.

Content Manager Pathway TechOne Other Council Applications	Teams One Drive	Sharepoint	Do not save in Council systems
Any official information used by Council to inform decision making such as; • Council reports • Financial records • Council applications (including Development GIPA, Licensing, Permits etc) • Customer requests (CRMs) • Policies and procedures • Official emails • Legal documents • Property information • Name and Address Register • Rating information	Any collaboration information for projects and information shared internally such as; • Meeting notes/recordings • Business unit (BU) specific processing guides/templates • Real-time collaborative documents (including spreadsheets, word documents, presentations etc.) • BU communication • One on one meeting notes • BU project files/documents	Any internal facing communication and documentation such as; • Corporate announcements/news • Corporate dashboards • Corporate templates/forms/style guides • Internal policies, procedures and documents • IT Strategy and IP&R Documentation • BU profiles and information • IT service desk • Learning and development materials and training • Customer Knowledge Base • Work Health and Safety materials • Procurement and fleet materials	Personal information used by individuals and not related to Council business.