

Records Management Policy

Purpose

The purpose of this policy is to establish the requirements for records management at the City of Sydney (City) and the accountabilities for record creation, management, retention, and destruction. Adherence to this policy will ensure the City maintains its records as a valuable resource that will support business operations, meet legislative requirements and community expectations for transparency and accountability, and contribute to Australia's archival heritage.

The records of the City are important assets. The City relies on records to:

- support business efficiency and better service delivery
- provide evidence of accountable decision making and administration
- protect the City's reputation, business and stakeholders, and reduce risk
- sustain corporate memory and provide a valuable cultural resource for the community.

To be able to achieve these benefits, records need to be:

- authentic, trustworthy and accurate
- managed accountably
- readily accessible, understandable, and useable
- valued as critical to business operations
- governed by appropriate risk management approaches
- maintained to meet business, government, and community purposes.

This policy should be read in conjunction with the City's Code of Conduct and the other policies and related procedures referred to in this document.

Scope

This policy applies to:

- business conducted by and on behalf of the City
- records in all formats (physical and digital) across all operating environments, including all City systems (public-facing, front-line, line of business, and corporate)
- City Employees and Workers
- agency staff, third party contractors, and consultants using or managing information on the City's behalf
- Councillors when conducting business in the course of their public duties as Councillors.

This policy does not apply to Councillors' election, party political or Councillors' personal records as these are not City records.

Background – legislative requirements the City must meet

State Records Act 1998 (NSW)

The *State Records Act 1998* (NSW) governs records management obligations at the City. The *State Records Act 1998* (NSW) requires the City to:

- make and keep full and accurate records

- ensure the safe custody and proper preservation of records under the City's control
- establish and maintain a records management program
- monitor and report on its records management
- maintain accessibility to technology dependent records
- retain records for as long as they need to be kept
- manage State archives and provide public access to records where required
- comply with mandatory standards released under section 13(1) of the Act.

The key standard is the Standard on Records Management, which establishes the requirements for effective holistic records and information management. This standard supports good practices in complex business and information environments and promotes the sound management of digital records.

The other standard issued under the *State Records Act 1998* (NSW) is the Standard on the Physical Storage of State records, which sets minimum compliance requirements to ensure physical records are stored appropriately. These include paper files and documents, volumes, maps and plans, photographic, magnetic and optical media.

General retention and disposal authorities are legal instruments issued by State Records NSW under the *State Records Act 1998* (NSW) which mandate how long records must be kept.

Other key legislation

The management of records and information is also affected by other information legislation such as the *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act'), the *Health Records and Information Privacy Act 2002* (NSW), and the *Government Information (Public Access) Act 2009* (NSW) ('GIPA Act'). The *Copyright Act 1968* (Cth) can also influence the accessibility and use of certain records.

Specific legislation, including the *Local Government Act 1993* (NSW), and other legislation can also contain recordkeeping requirements that must be met.

Definitions

Term	Meaning
Archive (Archival record)	A record that has been identified as having permanent value for retention as part of the City Archives. It has a permanent value if it is required under a retention and disposal authority issued by State Records NSW or meets criteria for acquisition under the <u>Archives Collection Management Policy</u> .
Archives management	A component of <u>records management</u> . It involves ensuring that the small percentage of records of permanent value are identified, managed, and able to be kept as part of the City Archives for the ongoing benefit of the City and community.
Business system	A computer system that creates, manages and/or stores information about business activities. Most business systems are systems of record designed for a specific set of business transactions.

Term	Meaning
By design	<p>Record and archives management is conducted 'by design', which involves:</p> <ul style="list-style-type: none">• proactive planning to ensure the right records are created in the right systems able to meet protection and security requirements and mitigate risk• proactive management so that records are kept for as long as required to meet identified business needs, accountability requirements and community expectations• planned destruction of time-expired records so that risks and storage costs are reduced, and resources can be focused on the robust management of high value information.
Corporate records management system	<p>A <u>Business System</u> with a primary function to manage the capture, maintenance, retention, and destruction of records and to provide access to records over time.</p> <p>TRIM Content Manager (TRIM CM) is the City's corporate records management system.</p>
Digital record	<p>Digital information and data that the City might rely on and use as evidence or information about its business, operations, and services. Digital records include:</p> <ul style="list-style-type: none">• 'born digital' records such as MS Office documents, emails, web pages, digital photographs, digital audio files, text messages etc.• geospatial information files• business system data• digitised paper records.
Employees	<p>All City of Sydney employees including permanent (whether full-time or part-time), temporary, casual employees and apprentices.</p>
General retention and disposal authority	<p>A legal document that identifies categories of records and how long they need to be kept. Some records can be destroyed after legal retention periods are met, while some are required to be kept as part of the archival resources of the State.</p>
High risk/value records	<p>High risk records are critical to the performance of core business. Accidental loss or destruction of such records could result in the City being unable to deliver services, meet legal or regulatory requirements, or result in financial loss or loss of reputation.</p> <p>High value records have continuing business value to the City or archival value.</p>
Key records	<p>Records of business processes capture the critical elements of the decision or transaction.</p>
Recordkeeping compliant system	<p>A business system that the Data and Information Management Services Unit (DIMSU) has assessed and found to meet records</p>

Term	Meaning
	management functionality requirements of City policy and relevant legislation.
Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. See section 4(1) of the Privacy and Personal Information Protection Act for the full definition.
Record	<p>Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business. (AS ISO 15489-2017 Records Management Part 1: General).</p> <p>Any document or other source of information compiled, recorded, or stored in written form or on film, or by electronic process, or in any other manner or by any other means. (State Records Act 1998)</p> <p>Note: A record can be in any format, including data and metadata in business and online systems, electronic messages, audio and video files, scanned documents, and paper records.</p>
Records management	<p>The management of records throughout their existence. This includes identifying, classifying, storing, securing, retrieving, tracking, and destroying or permanently preserving records.</p> <p>Records management must be sound and built into systems, processes and daily operations so that records are:</p> <ul style="list-style-type: none">• trustworthy• reliable• efficient• useable• compliant• accountable.
Sensitive information	<p>Sensitive information is that which would result in damage to an individual, organisation or government if compromised through loss, misuse, interference, or unauthorised access, modification or disclosure.</p> <p>See Briefing Note - Executive - Sensitive and Security Classified Information Schema for more information.</p>
Workers	All Employees, agency contractors (labour hire), work experience students and volunteers.

Policy Statement

The City takes responsibility for records management

The City has established a Records Management Program and other key strategies to govern records and information management and City archives in accordance with requirements of the

State Records Act 1998 (NSW). Key employees have the appropriate skills to implement the program.

Employees at all levels, contractors and Councillors have responsibilities for recordkeeping. They must be aware of their obligations under this policy and take reasonable measures to ensure their ongoing compliance. See section on [Responsibilities](#).

The City prioritises high risk and high value records and information

Not all records have equal value. Where resources are constrained, the City will prioritise securing and managing records of higher risk and value.

The City promotes digital first and 'by design' principles

Digital first

The City mandates the creation and management of records in digital format (digital records), as digital records are easier to access and reuse.

By design

The management of digital records requires proactive planning, particularly in new systems and service environments, including some external to the City. The City has a '[by design](#)' approach where requirements for records are considered at systems design, acquisition or migration or when entering into working relationships with external parties. By design strategies can produce systems that consider issues such as authenticity, information integrity, preservation, metadata, security and access, accountability and audit controls as well as planning for migration, disposal and future information accessibility. See section on [Responsibilities](#).

The City's records are made and kept in systems that support business and recordkeeping

The City identifies records and information that it requires to meet short and long term business needs, accountability, and community expectations. Records and information required to support high risk and value areas of business must be documented in procedures and business rules and form a designed component of system and service environments.

[Medium to high risk records and information](#) need to be retained in systems that are designed to support them and mitigate risks. The City's corporate records management system, TRIM Content Manager (TRIM CM), provides compliant management of digital records and legacy hardcopy records and their metadata. Certain records may not need to be saved to City business systems. See the [Retaining and destroying records](#) procedure for more information.

If business systems cannot be designed to meet the City's recordkeeping requirements, records should be transferred to TRIM CM for management. Network and personal drives, portable storage media or unofficial physical records are not adequate for the ongoing storage of medium to high risk or valuable records. These should be saved into TRIM CM where they can be protected, managed and accessible to all authorised users. Similar considerations should be made for records stored in Microsoft 365 environments where automated integration is not in place to address these requirements.

The City is accountable for records created and held by external parties on behalf of the City. If records are created outside of City business systems, e.g. if employees are using an externally hosted system or if a contractor uses their own system, they should be protected, maintained, and accessible within that system for as long as the records are required.

If this cannot be guaranteed, and the risks and/or the value of the information are high, key records should be exported and transferred to City recordkeeping compliant systems so the City can retain the information it needs. Contractual arrangements may be necessary to ensure records can be migrated or transitioned between systems if required. Contracts must clearly state that ownership of records must reside with the City.

Cloud solutions must be subject to a Cloud Due Diligence Process. Where a cloud solution does not meet recordkeeping functionality requirements, the business owner must implement appropriate strategies to manage the shortfall. Generally, this will include either integration with TRIM Content Manager and/or manual processes.

Key responsibilities of all individuals:

- Follow established procedures or business rules (where they exist) that define what records and information should be made and the systems that should be used to support processes and information security requirements.
- Where there are no established procedures, consider the risks and value when deciding what records and information to make, where to keep them and what security protections are required.
- Create and manage records and information in digital format. Scan any physical format documents received and manage the digital version as the official record.
- Document business commitments, advice, and decisions including those made in meetings or telephone calls.
- Create and keep personal information only in accordance with the requirements of the Privacy and Personal Information Protection Act. See the City's [Privacy Management Plan](#).
- Use TRIM CM, the City's corporate records management system, to capture key records if there is no designated business system to support your processes.
- Move medium to high risk records in Office 365 environments, network or personal drives, on portable storage media, or unofficial physical files to TRIM CM.
- If an outsourced provider, create, keep and manage records and information for the City in accordance with the responsibilities for creation, management, access and return of records outlined in your contract.

The City only makes and keeps records needed for City business

The City is committed to the principle of data minimisation. The City assesses the level of personal or sensitive information that is appropriate to be collected on a case-by-case basis with a view to minimising the amount of personal and health information it collects and manages.

Where practicable, the City sights identity documents instead of collecting and maintaining copies of them. The City only asks for personal or sensitive information that is required to support a genuine business need.

The City's records are trusted and usable

The City must make complete and accurate records of an acceptable quality to be fit for purpose, trusted, and usable.

Key responsibilities of all individuals:

- Include enough detail in records to ensure they are fit for purpose and have the context to be understood and usable by others.
- Apply adequate metadata to records and information to ensure they can be found and used.
- Follow relevant data procedures or system rules.
- Ensure records and information are accurate, reliable, and trustworthy.
- Create or save records and information in relation to business activities as soon as possible after the action, advice, or decision into a business system used to support them.

The City's records are shared

Records must be available to all authorised employees in order to conduct business efficiently. Making accurate and usable records and keeping them in the right systems promotes accessibility and reuse.

The public has a right to request access to City information, in any format or system, under the GIPA Act. Where possible, the City is also committed to making information available to the public proactively through its websites or other means.

The City's approach to information access is guided by the Information Access Team and is based on principles of open and transparent government, consideration of the public interest and respect for the privacy of individuals.

Key responsibilities of all individuals:

- Ensure records and information are available to colleagues who require it for the purposes of conducting their official duties.
- Only restrict employee access to records when there is a legitimate need, e.g. personal, commercial in confidence or other sensitive information.
- When making and keeping records and information, understand that the public has a right to request access to Government information under the GIPA Act.
- Consider the potential for the proactive release of City records and information to the public for business and community benefit.
- Collect, use, disclose, and manage records and information in accordance with the Privacy and Personal Information Protection Act and the City's [Privacy Management Plan](#).
- Copy records and information only if there is a legitimate reason, in accordance with legal requirements.
- Share records and information with approved users by authorised and appropriate methods. If security requirements apply, the recipient must be informed and must manage and share the records information in accordance with these requirements.

The City's records are protected and secured

The City must ensure records are protected and handled securely to prevent unauthorised access, destruction, alteration, deletion or loss. Protection is 'by design' where possible. Risks to information are identified and managed or mitigated.

The City maintains records of the Office of the Lord Mayor and of each Councillor as separate and discrete from City records. They are not accessible to City employees, unless explicit access is granted by the Office of the Lord Mayor or the specific Councillor. City records are not available to Councillors unless the records are authorised for sharing and required for the performance of their civic office functions. These arrangements do not remove individual rights of access to records and information under the GIPA Act.

Personal information is managed under the relevant provisions of the PPIP Act, the GIPA Act, and the *State Records Act 1998* (NSW). See the City's [Privacy Management Plan](#) for guidance on the City's privacy policy.

Key responsibilities of all individuals:

- Understand processes you are responsible for. These may require specific protections and indicators to safeguard personal, commercial in confidence or other sensitive information, or the intellectual property of others.
- Understand when and how to apply these specific protections and indicators and ensure they are applied consistently.
- Use the right business systems and controls within them designed to provide security and protection.
- Protect and handle records in line with City procedures in all ways information can be used, including records on mobile devices.
- Manage low risk and value records in line with the City's [Retaining and destroying records](#) procedure. They do not always need to be created or saved to City business systems.
- Do not use data backups for records storage.

The City's records are managed and monitored

The management of records is affected by factors such as changes to staff, the organisation, systems and contracts, processes, and changing security or community requirements. The City actively manages, protects, and preserves its records to ensure they continue to be created and kept in accordance with legislation, business needs, and community expectations. Any changes in systems or services over time must include the assessment of impacts of those changes on records creation, quality, management, use, sharing, security, protection, and retention.

Routine, annual, and ad-hoc monitoring and reporting is undertaken to ensure that records management is effective, accountable, and meets business needs and that the City is complying with its legislative requirements and records management standards. Monitoring of technology dependent records is performed to ensure records remain accessible and usable. See below for individual responsibilities and section on [Responsibilities](#) for specific positions or levels.

Key responsibilities of all individuals:

- Transfer high risk or value records from inadequate systems into the right business systems for ongoing management.
- Ensure any records access or security incidents or issues are reported so that strategies can be developed to rectify and manage them.

The City's records are retained and disposed of appropriately

The City is committed to retaining records and information for as long as required to meet business, legal requirements, accountability needs, and community expectations, and no longer. The City Archivist has the delegated authority to approve records disposal.

Some records of minor value, such as drafts, working papers and duplicates may be destroyed when no longer required (without formal authorisation) in accordance with the Retaining and destroying records procedure. Records must not be destroyed if they are subject to current or pending legal action or disposal freezes.

Records which have been successfully scanned are authorised for destruction under General Retention and Disposal Authority: Original or source records that have been copied (GA45) providing relevant requirements are met.

No other records should be destroyed without authorisation from the City Archivist. The City Archivist must also provide formal approval prior to the decommissioning of systems or migration of content of archival value. Retention and destruction decisions are based on approved general retention and disposal authorities, business and accountability requirements, and the City's Archives Collection Management Policy.

Records identified as having potential permanent or long term value are identified as soon as possible and planned for. Planning can include recommended storage environments, handling requirements, system documentation, and migration strategies to ensure records remain trustworthy, accessible, and usable. Permanent records must be transferred to Archives in accordance with established procedures and managed as part of the City's archival collection.

Key responsibilities of all individuals:

- Destroy records of minor value such as some drafts, working papers, and duplicates in accordance with the City's Retaining and destroying records procedure when no longer required.
- Do not destroy other records without authority.
- Ensure any transfers to Archives are managed in accordance with procedures.

Responsibilities

The responsibilities defined in this policy are supported by records and information tools, guidance, advice and assurance services that are delivered by Data and Information Management Services Unit (DIMSU).

All individuals will:

- follow established procedures or business rules (where they exist) that define what records and information should be made and the systems that should be used to support processes and information security requirements
- where there are no established procedures, consider the risks and value when deciding what records and information to make, where to keep them and what security protections are required
- create and manage records and information in digital format. Scan any physical format documents received and manage the digital version as the official record
- document business commitments, advice, and decisions including those made in meetings or telephone calls
- create and keep personal information only in accordance with the requirements of the Privacy and Personal Information Protection Act and the City's [Privacy Management Plan](#)
- use TRIM CM, the City's corporate records management system, to capture key records if there is no designated business system to support your processes
- move medium to high risk records in Office 365 environments, network or personal drives, on portable storage media, or unofficial physical files to TRIM CM
- if an outsourced provider, create, keep and manage records and information for the City in accordance with the responsibilities for creation, management, access and return of records outlined in your contract
- include enough detail in records to ensure they are fit for purpose and have the context to be understood and usable by others
- apply adequate metadata to records and information to ensure they can be found and used
- follow relevant data procedures or system rules
- ensure records and information are accurate, reliable, and trustworthy
- create or save records and information in relation to business activities as soon as possible after the action, advice, or decision into a business system used to support them
- ensure records and information are available to colleagues who require it for the purposes of conducting their official duties
- only restrict employee access to records when there is a legitimate need
- when making and keeping records and information, understand that the public has a right to request access to Government information under the GIPA Act
- consider the potential for the proactive release of City records and information to the public for business and community benefit
- collect, use, disclose, and manage records and information in accordance with the Privacy and Personal Information Protection Act and the City's [Privacy Management Plan](#)
- copy records and information only if there is a legitimate reason, in accordance with legal requirements
- share records and information with approved users by authorised and appropriate methods. If security requirements apply, the recipient must be informed and must manage and share the records information in accordance with these requirements
- understand processes you are responsible for. These may require specific protections and indicators to safeguard personal, commercial in confidence or sensitive information, or the intellectual property of others
- understand when and how to apply these specific protections and indicators and ensure they are applied consistently

- use the right business systems and controls within them designed to provide security and protection
- protect and handle records in line with City procedures in all ways information can be used, including records on mobile devices
- manage low risk and value records in line with the City's Retaining and destroying records procedure. They do not always need to be created or saved to City business systems
- not use data backups for records storage
- transfer high risk or value records from inadequate systems into the right business systems for ongoing management
- ensure any records access or security incidents or issues are reported so that strategies can be developed to rectify and manage them
- destroy records of minor value such as some drafts, working papers, and duplicates in accordance with the City's Retaining and destroying records procedure when no longer required
- not destroy other records without authority
- ensure any transfers to Archives are managed in accordance with procedures.

Managers and Team Leaders will:

- be specifically responsible for the effective control of the records in their area.
- ensure records management is integrated into work processes, systems, and services
- foster a culture of good records management practice
- monitor and address the security and quality of records management practice in their sections and teams
- ensure employees receive appropriate training in their processes, business systems, and records management responsibilities so they can comply with this policy
- cooperate with reviews, compliance audits, assessments and report on records management
- complete cloud due diligence assessments for any cloud services used in their area
- ensure any disposal of records or transfers to Archives are managed in accordance with City procedures and delegations.

When appropriate to their management level and the risks or value of the information, Managers with the support of Information Services section may need to:

- identify high risk, high value processes in the business unit, and develop and implement procedures or business rules that identify and document what records should be made and the systems to use to support these processes, taking into account any legislative requirements and security needs
- ensure their workers, including contractors and volunteers understand their accountabilities and responsibilities for records management prior to the commencement of service
- conduct risk assessments and ensure contractual arrangements with outsourced, cloud, and service providers include records management responsibilities
- as part of requirements gathering for the procurement or design of new systems, processes or services, identify requirements for records creation, quality, management, access, use, sharing, security, protection, and retention. Address these according to risk and value
- ensure when using externally hosted or contractor-owned systems that they make and keep records the City needs, that information is adequately protected and that access can be

assured as long as needed. This may require contractual arrangements for migration or transition between systems

- routinely monitor records management and protection measures in City systems and other system and service environments and respond to risks, staff and organisational change, increasing or decreasing security requirements and community requirements and expectations
- contact the Information Services section for advice regarding bulk scanning, disposal, or retention of existing records
- contact the Information Governance and Archives teams for advice and approval when decommissioning systems or services to ensure legal rules are met
- determine when personal information may require destruction, in accordance with privacy and records legislation
- review and release records for broader corporate or community use when appropriate
- ensure (in liaison with DIMSU) that any changes in system or services over time include assessment of the impact on records creation, quality, management, use, sharing, security, protection and retention
- respond to records destruction notifications from the City Archives.

Business system owners will:

- be specifically responsible for the operational management of a business system that transacts or supports City business.
- ensure the business system can create and manage records appropriately
- ensure records required for permanent retention are appropriately identified, managed, and protected in an accessible and stable format
- ensure requirements for records are considered and addressed when systems are acquired or modified
- monitor compliance with existing City policies and procedures in the system.
- test/audit systems to ensure they are operating routinely and address any issues affecting information integrity, usability or accessibility
- liaise with the Archives Team when planning to migrate or decommission systems or purge data
- ensure records and information are handled securely according to their sensitivity during retention, destruction and decommissioning processes
- conduct risk assessments and ensure contractual arrangements with outsourced, cloud, and service providers include records management responsibilities
- provide full and detailed responses about their systems for records management compliance audits and assessments when asked
- ensure any manual processes identified as required to meet recordkeeping obligations are routinely and effectively carried out.

Directors will:

- be responsible for championing and supporting records management in their division.
- provide stewardship for the City's records, including direction and support
- champion a culture of good recordkeeping in their divisions

Chief Executive Officer will:

- ensure that the City complies with the requirements of the State Records Act and regulations (State Records Act, s10)
- champion a culture of good recordkeeping in the City
- approve exemptions to the City's principle of digital recordkeeping in instances where a requirement for maintenance of records in hardcopy format is demonstrated
- approve and promote compliance with this policy.

Information Services Section

Information Services is a section within the Data and Information Management Services Unit (DIMSU). It encompasses the functions of information governance, document services, information access, and archives management.

Information Services has primary responsibility for supporting managers and individuals with tools, guidance and advice to assist them in integrating the requirements of this policy into their work. It provides records and information assurance services for the City as a whole.

Information Services will:

- implement and regularly monitor the efficacy of the Records Management Program and other strategies for records and information management
- provide efficient and effective records management services, systems, and tools to the City's employees, to agreed standards
- provide training to employees in recordkeeping and records management systems
- provide advice and assurance services on records and information management across the City, including information classification
- collaborate with managers, project managers and business system owners to determine records management needs for systems and services, migration and decommissioning projects
- monitor records management performance and compliance with policy, standards and procedure and liaise with State Records NSW when required
- investigate and provide formal approval for the decommissioning of systems
- manage the disposal of records in any format, including the retention, destruction or transfer of records in accordance with authorised retention and disposal authorities and business rules
- manage the City's semi active records and archival collection and the provision of public access to City records and information, where appropriate
- manage loans or purchases of archival records or donations to the City Archives
- provide the public with access to City records in accordance with the GIPA Act and City policy and procedure.

Manager, Information Services will:

- develop strategies and policy for records and information management across the City
- manage the corporate records management system
- review this policy
- produce, endorse and approve as appropriate procedures for records management.

Chief, Data and Information Management will:

- be the Senior Responsible Officer for managing the Records Management Program and guide compliance with records management standards
- work with other managers of information assets to develop a coherent information landscape across the organisation
- establish a governance framework and strategies to ensure the requirements of this policy are fulfilled
- ensure collaboration across business areas where required for new systems and services, migration, and decommissioning projects
- respond to requests or directions from State Records NSW to complete records management compliance audits and assessments
- respond to notices issued by State Records NSW under s.12(5) of the State Records Act
- approve procedures for records management.

Legal and Governance will:

- identify recordkeeping failures as part of audits, breaches, or legal matters and raise these in reports and with Information Services for action.

Consultation

The Chief Data and Information Management, Manager Information Services, Information Access Manager, City Archivist, Document Services Manager, and Information Systems Team were consulted in the review of this policy.

Legal Services and Governance provided comments and feedback on the updated policy.

References**Laws and Standards**

- Local Government Act 1993
- State Records Act 1998
- State Records Regulation 2015
- Government Information (Public Access) Act 2009
- Government Information (Public Access) Regulation 2018
- Privacy and Personal Information Protection Act 1998
- Electronic Transactions Act 2000
- Environmental Planning and Assessment Act 1979
- Data Sharing (Government Sector) Act 2015
- Copyright Act 1968 (Cth)

Policies and Procedures

- State Records NSW:
 - Standard on Records Management
 - Standard on the Physical Storage of State Records
 - General retention and disposal authorities (various)
- Archives Collection Management Policy

Laws and Standards

- Access to Information Policy
- Information and Technology Strategic Plan
- Records Management Procedures
- Privacy Management Plan
- IT Systems Security Policy
- Access to Information Guideline
- Requirements for Making and Keeping Councillor Records
- Australian and International Standard AS ISO 15489.1-2017, Records Management, Part 1: Concepts and Principles
- International Standard ISO 16175 - Information and documentation - Principles and functional requirements for records in electronic office environments.

Review period

This policy will be reviewed every 3 years.

Approval Status

The Chief Executive Officer approved this policy on 8/11/2023.



Monica Barone, Chief Executive Officer

Approval History

Stage	Date	Comment	TRIM Reference
Original Policy	February 2009	Approved by CEO	2008/092328
Reviewed	5 September 2014	Approved by CEO	2014/411091
Reviewed	18 April 2018	Approved by CEO	2018/224731
Reviewed	6 October 2020	Minor updates to terminology and references.	2018/224731
Reviewed	8 November 2023	Two new sections added: <ul style="list-style-type: none">• Prioritising high risk and high value records and information• Only making and keeping records needed for City business.	2023/560518

Stage	Date	Comment	TRIM Reference
		Minor amendments to references, terminology, style, format, and updates to links and resources.	
Commence Review Date	8 February 2026		
Approval Due Date	8 November 2026		

Ownership and approval

Responsibility	Role
Author	Information Analyst
Owner	Chief Data and Information Management
Endorser	City of Sydney Executive
Approver	Chief Executive Officer