Information Management Policy

Corporate Services
CORP_32

COUNCIL POLICY			
Date Adopted by Council	23 March 2022	**Council Resolution**	2022/03/23.3
Effective Date	23 March 2022	**Next Review Date**	23 March 2025
Responsible Officer(s)	Information Management & GIS Coordinator	**Revokes**	LSP_CORP_38

Purpose

The purpose of this policy is to aid efficient organisational processes through structured records and information governance practises, while complying with legislative requirements.

Reliable, structured data and recordkeeping practices support council to:

- be transparent and efficient in business transactions with clients.
- make informed decisions based on all available evidence.
- meet legislative responsibilities; and
- protect the interests of elected members, staff, and clients.

Scope

This Policy is applicable to all council employees, contractors, volunteers, temporary, casual workers, and councillors.

A public record is any form of recorded information, either received or created, that provides evidence of the decisions and actions of a public authority in carrying out legislative, administrative, or other public responsibilities. Records can take the form of paper or electronic, such as documents, email, audio recordings, video recordings, CCTV footage, social media posts, websites, text messages, business applications, photos, diaries, publications, file notes, drawings, and plans.

This policy covers public records created, commissioned, received by Whitsunday Regional Council or which council has a legislative responsibility.

This policy provides the overarching framework for any other corporate recordkeeping plans, practices, or procedures.

Applicable Legislation

All public records, including electronic records, are subject to legislation and to legal processes such as discovery and subpoenas. This Policy is in reference to the *Public Records Act 2002* and the Queensland Information Governance Policy released in 2018.

Other key pieces of legislation and standards relating to information and recordkeeping are:

Acts	Standards
• Local Government Act 2009 • Right to Information Act 2009 • Information Privacy Act 2009 • Copyright Act 1968 • Electronic Transactions (Qld) Act 2001 • Evidence Act 1977 • Judicial Review Act 1991 • Public Service Act 2008 • Intellectual Property Laws Amendment Act 2015	• Information Standard 18: Information Security (IS18) • Information Standard 44: Custodianship (IS44) • Australian Standard AS ISO 15489, Records Management • Australian Standard AS ISO 16175, Principles, and functional requirements for records in electronic office environments • Australian Standard AS/NZS 5478:2015, Recordkeeping metadata property reference set • ISO 15076, Image technology colour management - Architecture, profile format and data structure • ISO 19005, Document Management – Electronic Document File Format for Long-Term Preservation • Payment Card Industry Data Security Standard (PCI DSS)
There are other Acts which explicitly state specific recordkeeping requirements. They include: • Business Names Registration Act 2011 • Land Act 1994	

Policy Statement

Records are a corporate asset and this policy outlines and directs the practices of council in relation to the management of information and records.

Records of council are created and received because of interactions with residents, other agencies, government departments and businesses. Reliable, accurate data is critical for council to be able to make informed decisions, take appropriate actions and interact with stakeholders in a transparent, consistent, efficient, and professional manner. To meet these requirements the following principles must be followed:

- Compliance with the Public Records Act 2002 and associated framework.
- Compliance with Information Privacy Act 2009 & Right to Information Act 2009.
- Processes are in place to systematically and effectively manage complete and reliable records.
- Council employees, contractors elected members and volunteers are aware of their recordkeeping obligations.
- Recorded Information can be retrieved efficiently, in a cost-effective manner when required.
- Full and accurate records must be created and maintained for as long as required for legislative, business and accountability purposes.
- Records must be captured in council's electronic document and records management system.
- Records must only be disposed of with authorisation from the CEO or nominated delegate (Director of Corporate Services).
- Physical archived records prior to the document management system are to be stored in a secure location with environmental controls in place to preserve the records for the required time, with long term, high value and high-risk documents progressively digitised over time; and
- Assigned key roles and education in relation to record creation and recordkeeping.

Whitsunday Regional Council will implement and maintain appropriate strategies, processes, applications, and tools to ensure records of business activities are made and kept meeting operational business needs and recordkeeping obligations.

Ensure that records management is integrated into core and operational functions and will develop performance metrics that align with the intent and objective of this policy with the strategic objectives of the Council.

Ensure that records are retained and disposed of in a planned and authorised way in consultation with the Queensland State Archives, bearing in mind that the CEO is ultimately accountable for the creation, management, appraisal, and retention of Council's public records.

1. Responsibilities and Accountabilities

The creation, capture, integrity, access, and retention of Whitsunday Regional Council's records under the *Public Records Act 2002* and the *Local Government Act 2009*.

Key roles and services are integral to support Councils' record management objectives and transform Councils' information management maturity for efficient utilisation and verification of information to serve our community. Broadly these include:

CEO • Council complies with responsibilities under the *Public Records Act 2002*. • Delegates authority for various authorisations related to records management.	**Technology & Innovation Manager** • Ensure information systems are maintained for the required length of time and audited for compliance.	**Information Management Team** (Enable the business to be effective by): • Ensuring compliant recordkeeping processes are in place across the business. • Auditing and educating the business in sound records creation and records management practices.

2. Record Creation, Capture, and Integrity

2.1 Creation and Capture of Records

Full accurate records must be created and saved in a format, media and location that is readable and accessible for the life of the record. Records created by council must comply with the provisions of the *Copyright Act 1968* and the intellectual property rights will remain Council's property, except where a Council has a contract with a supplier stating otherwise.

For records to be authentic, complete, and accurate they need to identify and capture the following metadata standards into council's record management system:

- what took place, where and when something was done, or why a decision was made. Also, who was involved and under what authority.
- author.
- date the record was created and received.
- document type (e.g., inward, outward, and internal).
- security classification (who can view the document).
- version number.

- subject (to determine information retention).

Final records must be captured that contain signatures and attachments for records to be considered complete. When scanning either historical or current records the digitisation and disposal of records process must be followed.

2.2 Identifying Public Records

This table is adapted from *What records do I need to keep?* Queensland State Archives

What is a public record? *Note: This list is not exhaustive*	**What is not a public record or does not need to be stored?** *Note: This list is not exhaustive*
• Any data within a database or document that records business processes or actions (e.g., rates payments, license applications and approvals, salary payments) of council • Information published on a webpage or website that relates to the business functions of council • All agendas, minutes and papers that were presented at meetings within council • Financial statements, corporate and operational plans • Audit reports, analysis reports, business cases, proposals • Legal agreements, contracts and leases • Records required for legal proceedings or right to information requests • Draft documents containing significant annotations or submitted for comment or approval by others • Handwritten notes documenting a decision or action • Recruitment and selection documentation • New and updated policies and procedures • Work diaries / Appointment Books / Outlook calendars related to local government executive, statutory or administrative function • Visitor books • Letter or emails from customers requesting information or action and the response/s sent back • Records generated from a project, including plans, estimates and costing, re-sourcing requirements, background research material	• Drafts of reports, correspondence and / or routine calculations that were not circulated internally or externally or finalised • An external database that was used for reference purposes only • Drafts of information prepared for a webpage or website that were never circulated for comment or approved as a final version or published • Information downloaded from the internet • Agendas and minute from a staff social club meeting • An external publication • Advertising or training brochures from an external provider • Informational material that includes lists of suppliers, catalogues, directories, address and contact lists • Unsolicited letters or emails advertising products or services • An email about an afternoon tea for a work colleague who is leaving • Election materials created or received by a Councillor in regard to electioneering are private records of the Councillor • Credit cards and associated card data must not be stored or must be rendered unreadable (redacted) if contained within a document that needs to be registered

• A work-related email that documents an action or decision (e.g., an email that approves the purchase of new signage) • Workplace health and safety risk assessments, incident reports, take 5s, etc • Correspondence or petitions relating to lobbying matters such as improving road conditions • Surveys and evaluations (e.g. Customer service, training, procurement, tenders) • Building information modelling (BIM) records • Preparation of elections such as nominations, etc	

2.3 Information Security Classification

a. Identifying information holdings.

The department or individual (originator) must determine whether information being generated is official information (intended for use as an official record) and whether that information is sensitive or security classified.

b. Assessing sensitive and security classified information.

To decide which security classification to apply, the originator must:

I. assess the value, importance, or sensitivity of official information by considering the potential damage to Council, organisations, or individuals, that would arise if the information's confidentiality was compromised (refer to the following classification table), and
II. set the security classification at the lowest reasonable level.

If the originator does apply classification the document, it will be deemed classified as ALLSTAF.

ALLSTAF (INTERAL ACCESS ONLY)	Most documents and information is classified as viewable by all staff. As an employee you are obligated by confidentially in the Code of Conduct handbook to keep information you view and create to within WRC unless it carries a higher security classification which restricts who else in the organisation you can discuss certain matters with.
PRIVATE	Personal information must not be used for a purpose other than the particular purpose for which it was obtained and must not be disclosed to a third party, except for: • an individual has agreed to the use / disclosure. • reducing or preventing a serious threat to the life, health, safety, or welfare of an individual or the public. • a requirement or authorisation under law or necessary for law enforcement. • research or statistical purposes. When records containing personal information is going to be used, we must only use those parts that are directly relevant to fulfilling the particular purpose.
CONFIDENTIAL	Information marked as confidential to the CEO and some support staff, often relating to high level investigations, such as Crime and Misconduct Commission.
HR (Personnel Files)	Information relating to employment of individual staff including personnel plans, training, recruitment and employment lifecycle, payroll paperwork, etc are only visible to the People and Culture team and CEO.
ICT	Information containing passwords or sensitive information in Information Technology are only visible to Information Technology team.
LEGAL	Information containing sensitive legal matters are only visible to the Legal and Governance team and CEO.
PROCUREMENT CONFIDENTIAL	Information containing high value or sensitive procurement matters are only visible to the Procurement team and CEO.
PUBLIC	Documents or information that is available in the public domain. This information may be published on external sites / website.
WORK COVER	Information relating to work cover claims are only visible to the Workplace Health and Safety team.
YOUTH CASE MANAGEMENT	Information relating to case management involving young people. These documents are only viewable by the Legal team.

c. Declassification.

The originator remains responsible for controlling the sanitisation, reclassification, or declassification of the information.

d. Marking information.

The originator must use Council records management process and tools (digital or manual) to set the classification.

e. Using metadata to mark information.

Originator must apply Council's endorsed metadata standard to protectively mark information, using the 'Security Classification' property.

f. Storage.

Originator must ensure sensitive, and security classified information is stored securely in an appropriate secure container for the approved zone in accordance with the minimum protection requirements defined in Council's Information Management Procedures.

g. Transfer.

Originator or Information Management must ensure sensitive, and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements define in Council's Information Management Procedures.

h. Disposal.
Originator or Information Management must ensure sensitive, and security classified information is disposed of securely in accordance with the minimum protection requirements define in Council's Information Management Procedures.

2.4 Electronic File Formats

Information on preferred and acceptable file formats for long-term storage and accessibility is available on the National Archives of Australia website at https://www.naa.gov.au/information-management/storing-and-preserving-information/preserving-information/preserving-digital-information/long-term-file-formats

2.5 Auditing

Auditing is an important final step in the record creation process to ensure records are complete, accurate and can be discovered easily in the future. Auditing encompasses security and system changes, individual document auditing, and system utilisation.

The officer creating / registering the records into the EDRMS system is responsible for ensuring the final records are complete, preserved in a readable format for future use, and the correct metadata and indexes applied for easy retrieval.

Records specialists will complete checks on registered documents to ensure quality standards are maintained. Annual audits on a portion of electronic records will be analysed to ensure records are able to be opened in current systems.

2.6 Information Asset Custodianship

A custodian of an information asset is responsible for ensuring corporate information is collected and maintained according to specifications and priorities determined by consultation with stakeholders and made available to the wider organisation and public as appropriate and in a format that conforms with Council's standards and policies. Custodianship is assigned to a directorate or cross-directorate work units using the following criteria:

- Have sole statutory responsibility for the capture and maintenance of the information.
- Have the greatest operational need for the information.
- Are the first to record changes to the information.
- Are the most competent to capture and / or maintain the information.
- Are in the best economic position to justify collection of the source information.
- Requires the highest integrity of the information.

Information asset custodianship is documented in the Information Assets register. The Queensland Government has published *Information Standard: Custodianship (IS44).*

3. Access and Security

3.1 Availability

All records shall be available to staff to efficiently perform their role with the exception of investigations, personnel and payroll files, protective custody, confidential meetings, and commercial in confidence documents.

Access to council records will be governed by the Right to Information Act, Public Records Act, Information Privacy Act and the Protocols for dealing with RTI and IP applications AG_2/20_CS, with a view to provide openness and transparency of public documents by displaying these on Council's website or at customer service centres.

3.2 Information Security

Council officers must take all reasonable steps to ensure that information is adequately safeguarded in accordance with the ICT Facility Users Policy and Information Security Policy.

Council officers must not intentionally access files, registers or any other document that contains personal information unless it is necessary for their duties. Where access is necessary for work purposes, council officers must not disclose personal information to an unauthorised person.

Electronic devices and physical documents containing personal information must be kept secure from unauthorised access. The Information Technology department enforces security of council devices through technology policies, such as passwords, automatic screen locks when inactive, and permissions based on an officer's role to corporate systems. Corporate systems also provide auditing and control mechanisms to ensure the integrity of information.

Solutions hosted on servers and infrastructure outside of Australia do not need to comply with Australia's Information Privacy laws, therefore personal information must not be entered into these systems.

4. Archiving and Disposal

4.1 Retention

Records retention is the term applied to the safeguarding of important records that document decisions, evidence, financial activities, and internal controls. Retention of record types is determined based on the value of those records to council, the state of Queensland, the community, and/or Australia as a whole.

All Local Governments agencies in Queensland utilise the authorised retention and disposal schedules issued by Queensland State Archives. This schedule must be applied to the records of council when determining how long records should be retained or destroyed. The schedules identify the retention periods for records based on an appraisal of the records' value including their cultural, historical, fiscal, business, social and legal value.

Vital records are identified using a risk-based approach and are considered to be those that are:

- Permanent archival records based on the retention schedules (such as Council meeting minutes and various registers relating to properties, burials, applications, etc).
- Processes and information required to operate during a disaster.
- Council data not available from external sources that is essential for the ongoing business operations and that Council council could not function without.
- Council policies and procedures.
- Council owned properties and buildings.
- Projects, decisions, or events that caused major public controversy or had legal implications.

Such records may be considered vital only in the short term or may retain this status indefinitely.

4.2 Sentencing

Sentencing is the process of appraising records based on Queensland State Archives authorised retention and disposal schedules. The Information Management staff appraise council's records using a combination of the General Retention and Disposal Schedule (GRDS) and the Local Government Sector Retention and Disposal Schedule (QDAN 480).

4.3 Disposal of Records

No business records are to be destroyed, deleted, sold, donated, abandoned, damaged or the original amended without approval of the CEO or Director of Corporate Services. Records must only be disposed of in accordance with authorised disposal schedules as prescribed by the *Public Records Act 2002*, with the exception of a disposal freeze when certain types of records must not be destroyed until the disposal freeze is lifted. Disposal freezes are issued when it is necessary to temporarily stop the destruction of records (e.g., when records are required for legal proceedings or commissions of inquiry). They are issued for a set period of time, although they may be open ended if an end date can't be determined.

Prior to the destruction of temporary value records, (where the retention period has elapsed), approval must be given by the State Archivist, which is the correct use of the current retention schedules and signed endorsement by the CEO or authorised delegate. All documentation relating to the disposal process, must be maintained to validate the legal disposal of records. This validation may be required for an application under the *Right to Information Act 2009* or for legal discovery.

Before records can be destroyed, the following checks must be completed.

- The records are no longer needed for ongoing business.
- The records are not required for any right to information requests.
- Ensure records are not required as evidence for any current or pending legal action.

- No disposal freezes have been issued for the records.
- Consider other potential reasons to retain records, e.g., high-profile issue such as asbestos.

Permanent (archive value) records cannot be destroyed, even if the original physical records have been successfully digitised. Original records with a permanent retention period must be provided to the Information Management team for transfer to Queensland State Archives following digitisation.

4.4 Destruction Methods

Expired or digitised temporary records (following authorisation), or copies of records that contain confidential, personal, or sensitive information must be shredded or placed in the locked commercial shredding bins provided. Records to be destroyed are transported off-site in a secure manner and disposed of by either pulping or shredding.

5. Secure Storage

5.1 Storage - Electronic

Electronic records must be stored within Council's EDRMS system for compliance, discovery, integrity, and correct retention. Other information must be maintained in an approved Council corporate database or system for compliance, integrity, and security, and to ensure backups are kept for the retention period of the information.

The EDRMS system ensures Council's records are preserved, versions remain unaltered, history regarding tasking and notes are attached to documents, standard metadata is applied for ease of retrieval, and duplicates are controlled. Documents attached in other corporate systems must be added into the EDRMS system for preservation.

Whitsunday Regional Council non-public domain information must be stored on-shore within an Australian located data centre to minimise the risk of personal and confidential information breaches, as Council is subject to the *Information Privacy Act 2009* and the Australian Privacy Principles as an Australian Government agency. Overseas suppliers and contractors may be subject to different legislative rules regarding privacy and security.

5.2 Storage - Physical Records

All Council records shall be stored in conditions appropriate to their format and use in accordance with the Australian Standards on Records Storage, to minimise their deterioration.

5.3 Non-recordkeeping Systems

The following systems or tools do not provide adequate recordkeeping functionality and must not be used to store Council (public) records:

- Personal drawers, folders and filing cabinets.
- Email (Outlook).
- Local computer drives (e.g., My documents or Desktop).
- Portable devices and storage devices (e.g., Mobile phones, tablets, USB sticks, hard drives).
- Shared (network) drives.

5.4 Strategy and Implementation

5.5 Strategic Recordkeeping Implementation Plan (SRIP)

Council maintains and works to a strategic recordkeeping plan that provides long term direction and governance with the plan and goals being reviewed every four years. The plan is designed to provide tangible projects and outcomes to improve and maintain recordkeeping maturity across Council in all aspects of records management functions.

5.6 Compliance

Information Governance is the umbrella recordkeeping policy for State and Local Government in Queensland. It is technology-neutral and provides policy requirements for recordkeeping regardless of the administrative environment in which public records are created, managed or disposed. The policy sets out the foundational principles of recordkeeping for public authorities to meet minimum recordkeeping requirements now and into the future.

There are six policy requirements:

1. Agencies must ensure records management is supported at all levels of the business.
2. Agencies must systematically manage records using governance practices that are integrated and consistent with broader agency frameworks.
3. Agencies must create complete and reliable records.
4. Agencies must actively manage permanent, high-value and high-risk records and information as a priority.
5. Agencies must make records discoverable and accessible for use and re-use.
6. Agencies must dispose of records in a planned and authorised way.

5.7 Communication and Training

The communication plan provides a strategy for ensuring council staff are kept abreast of initiatives, policies, procedures, changes, and responsibilities for compliant recordkeeping practises.

5.8 Disaster Recovery

The disaster recovery plan covers disaster prevention, preparation, response, and recovery operations for Council's record holdings. The purpose of the plan is to assess the risks associated with council records, provide instruction on actions to take place at various stages, identify vital records, set roles and responsibilities, and document the full recovery process back to normal operations.

Definitions

CEO refers to the Chief Executive Officer of the Whitsunday Regional Council appointed in accordance with the *Local Government Act 2009*.

Council refers to the Whitsunday Regional Council

Council Business includes the provision of services, delivery of programs, development of policies, making of decisions, performance of Council functions and other similar types of transactions.

Councillor - refers to an elected member of Council

Current Retention and Disposal Schedule is one that has been approved by the State Archives and has not been superseded by another Retention and Disposal Schedule. At the time of disposal, public records must be sentenced under a current Retention and Disposal Schedule.

Data exchange is the process of sharing data from Council with another agency or contractor or vice versa.

Data migration is ensuring information from a legacy system is converted into the new system or exported in a readable format and saved into Council's EDRMS system for the required retention period.

Data sharing agreement is a signed agreement authorising the exchange of data for only the purpose and time specified, after which the data must be destroyed securely.

Digitisation is the creation of digital images from paper documents by such means as scanning or digital photography.

Digitised Records are digital images, created through the digitisation of physical records, which are then managed and used as official records of business activity in accordance with Information Standard 40: Recordkeeping.

Disposal refers to the final stage of record management. Under the Archives Act 1983, this means either, the destruction, the transfer of custody or ownership, damage or alteration of records. Public records cannot be disposed of without authorisation and must not be destroyed if a disposal freeze is in place. Disposal of records must be documented.

Disposal Freeze is an authority that temporarily freezes the disposal of public records relating to a specific topic or event, including records that have a temporary disposal status under an approved Retention and Disposal Schedule. Generally, these freezes relate to a particular issue that has created significant or substantial public interest. Original paper records to which a disposal freeze applies must not be destroyed while the freeze is in place.

Early Disposal refers to the practice of destroying original paper records after digitisation and before the authorised retention period for that class of record has expired. The digitised copy of the record must be retained for the same length of time that the paper original would have needed to be kept.

EDRMS refers to Council's Electronic Document and Records Management System.

ELT is the abbreviation for the Executive Leadership Team at Whitsunday Regional Council.

Employee refers to all council employees, contractors, volunteers, temporary, and casual workers.

Environmental controls are controls used in a records storage environment that assist in the long-term preservation of records, such as air conditioning, fireproof / fire control equipment and vermin control.

Ephemeral material is information relating to personal activities, drafts, reference material, duplicates etc, which have no value to the business and do not add value to another record (working document).

File formats encode information into a form which is intended for processing and use by specific combinations of hardware and software.

Full and accurate records are those records that provide reliable, complete and authentic evidence of business activities and decisions.

Official record is a record made or received by Council in the conduct of its business. This includes records made or received by a Council member in the conduct of the business of their office (i.e., Mayor or Councillor) but does not include records that are merely transitory or ephemeral in nature or that are personal or private in nature.

Personal information means "information or an opinion, whether true or not true, (including information or an opinion forming part of a database) relating to a natural person or the affairs of a natural person, whose identity is apparent, or can reasonably be ascertained, from the information or opinion including a photograph or other pictorial representation."

Originator - refers to the receiver of the information to be classified.

Outsourcing is the process of contracting a portion of a Council's activities to third-party providers.

QSA refers to Queensland State Archives as the regulatory body for Queensland record-keeping standards.

Record means recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the business or affairs and includes:

(a) anything on which there is writing; or

(b) anything on which there are marks, figures, symbols or perforations having meaning for persons, including persons qualified to interpret them; or

(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or

(d) a map, plan, drawing or photograph.

Redaction is the process of censoring or obscuring of part of a text for legal or security purposes, usually in the form of blacking out portions of a document that contain personal information.

Retention of a record is the period determined by the National Archives of Australia and the Queensland State Archives for document groups that each record must be kept, based on the information's archival value.

Secure Location is a place to securely store records in a controlled access environment to prevent unauthorised access to certain records and ensure records do not go missing.

Sentencing is the process of appraising records based on Queensland State Archives authorised retention and disposal schedules.

Standing endorsement arrangement is where the CEO or authorised delegate authorises a specific set or group of records over a certain time to be destroyed efficiently without seeking approval each time.

USB storage device is a peripheral device that plugs into a computer via the USB port and has the capability of storing large files for easy transportation.

Relating Documents

Code of Conduct
Elected Members Records & Information Management Policy
Digitisation and Disposal of Records Process
Electronic Signatures Policy
Information Security Policy
IT Facilities User Policy
Risk Management Policy

Human Rights Compatibility Statement

This policy has been assessed as compatible with the Human Rights protected under the *Human Rights Act 2019.*