



## Paroo Shire Council

Council Policy	
<b>Policy Name:</b>	<b>Recordkeeping, Reporting and Data Breach</b>
<b>Policy Number:</b>	GP-66
<b>Version:</b>	1.0
<b>Commencement and Review:</b>	This policy will commence from 15/10/2024 and will be reviewed 2 years from the commencement date.
<b>Document Owner:</b>	Director Corporate, Governance and Risk
<b>Approval Date:</b>	15/10/2024
<b>Meeting Resolution:</b>	M24/282

### 1 Statement of Intent

The intent of the Paroo Shire Council (Council) Recordkeeping, Reporting and Data Breach Policy is to provide an overarching framework for the creation, securing and management of Council Records, irrespective of technology, device or access method, and then to facilitate the use these Records for accurate Reporting.

### 2 Commencement and Review of Policy

This Policy will commence from 15<sup>th</sup> October 2024. It replaces all other Recordkeeping and/or Reporting Policies (Whether written or not).

This Policy will be reviewed two (2) years from the commencement date or earlier if deemed necessary through changes to legislation or business practice. Minor amendments that do not impact upon the intent of the Policy may be made in consultation with and approved by the Chief Executive Officer (CEO).

### 3 Application of Policy

#### 3.1 Purpose

This Recordkeeping and Reporting Policy, and all associated standards, guide, reference, practices, and procedures, form part of an ongoing commitment to Records management governance and Reporting.

The purpose of this Policy to establish a framework for Council to fulfil its Operational Plan, obligations, functions and statutory responsibilities, as it relates to Recordkeeping, Reporting, and data breaches, including:

- under the *Public Records Act 2002*, the Records Governance Policy issued under s.25 (1)(f) of the *Public Records Act 2002*, the Local Government Sector Retention and Disposal Schedule and Records Governance Policy (and any successors arising from the equivalent and transitional provisions in upon the enactment of *Public Records Act 2023* from 5 December 2024) and the *Queensland recordkeeping metadata standard*

*and guideline.*

- procedures to support all who deal with Records in discharging their obligations in relation to the creation, maintenance, storage, accessing, amending, disclosing and disposing of Council Records, in a manner that is compliant with the standards set out by Queensland State Archives and this Policy;
- supporting operational procedures and governance, including the mandatory use of standardised Record naming conventions, folder structures, workflows, automations, tasking agents, completion percentages, expiry dates, based on relevant Records that are created, modified, received or otherwise used in Council discharging its functions;
- supporting whole-of-Council, departmental, group and individual Reporting and dashboards both in real time and historically;
- supporting the transition to the *Public Records Act 2023* from 5 December 2024; and
- To prepare for the *Mandatory Notification of Data Breach (MNDB) Scheme* including *Data Breach Registers and Policies* taking effect from 1 July 2026.

### **3.2 Policy Statement**

Council's Records are its corporate memory and as such are a vital asset that support ongoing operations and provide valuable evidence of business activities over time. Council is committed to implementing best practice Recordkeeping systems to ensure the creation, maintenance and protection of accurate and reliable Records.

Council recognises its regulatory requirements as a public authority under the *Public Records Act 2002* and *Public Records Act 2023* from 5 December 2024. It is committed to the principles and practices set out in the QGCDG (Queensland State Archives) Records Governance Policy, the Local Government Sector Retention and Disposal Schedule (QDAN 480v.4), any successors and other relevant Queensland State Archivist standards and guidelines.

Council recognises an overarching commitment to open and accessible information for officers to ensure Access supports quality decision making that is fully informed, while ensure Access Control to Records to qualified, certified or otherwise needs basis, where appropriate to ensure excellence in governance.

Council recognises that Records are the principal way Council be made aware it is legally obliged to act, or to achieve the Corporate Plan, the Operational Plan and to discharge any obligations, functions and statutory responsibilities, including as it relates to limitation and expiry dates, as prescribed by law, by outer limit terms, by fixed time terms or sound governance practices.

Council recognises its performance, and functions can only be accurately reported on if Recordkeeping is undertaken with best practice.

Council recognises it holds significant amounts of personal information within its online resources and that this information must have Access Control, appropriately secured from unauthorised access or the subject of an unauthorised disclosure, whether internally or by external authorised Access, or malicious or criminal actors attempting to subvert Access Control.

### **3.3 Scope**

This Policy and the Recordkeeping, Reporting and Data Breach Procedure applies to Paroo Shire Council Councillors, employees, contractors and volunteers who create, maintain, store and/or access Records, business systems, database applications and business applications on behalf of Council.

To the extent this Policy is inconsistent with Council Policy PCOM030 – Body Worn Cameras, PCOM030, legislation first, then the CEO second, should there still be inconsistency, will

determine which prevails, and the CEO can decide this on a case-by-case basis.

### **3.4 Recordkeeping, Reporting and Data Breach Procedure**

All Recordkeeping practices of Council must be in accordance with this Policy and its supporting procedures and to achieve the Policy Statement.

The CEO is responsible to adopt and maintain a Recordkeeping, Reporting and Data Breach Procedure, which is to be read in conjunction with this Policy and applies in the same manner as identified in the Scope.

The CEO must ensure that the Recordkeeping, Reporting and Data Breach Procedure is updated to be consistent with legislation, included related instruments referred to in Related Links, and the State Archivist's requirements and supports the achievement of Council's Operational Plan.

The hierarchy of requirements relating to Council Records, including what they are and how they are kept, is:

1. Firstly, the *Public Records Act* 2002 and from 5 December 2024 the *Public Records Act* 2023, then
2. the Queensland Archivist's Record Keeping Procedure and the Local Government Sector Retention and Disposal Schedule (and any successors); then
3. Council's Recordkeeping, Reporting and Data Breach Procedure; then
4. finally, any other policies or procedures of Council that deal with Records.

### **3.5 Retention and Disposal of Records**

In general, it is an offence to destroy any public Record without authorisation from the State Archivist. Unless otherwise authorised, all Records must be retained and disposed of in accordance with the Local Government Sector Retention and Disposal Schedule. This Schedule is used in conjunction with the General Retention and Disposal Schedule and the Recordkeeping, Reporting and Data Breach Procedure.

A deliberate approach to not comply with the *Public Records Act* with Council Records may amount to corrupt conduct.

### **3.6 Retention of Records**

Records must be appraised for possible continuing archival value. That is, Records with legal, historical, or cultural significance to Council and the community must be retained permanently in Council's Records Collections or State Archives.

Any Records subject to legal processes such as discovery and subpoena or required for internal or external review or investigation or relevant to an application made under the *Right to Information Act 2009* must be protected and not destroyed even if the retention period has passed.

### **3.7 Disposal of Records without Reference to a Retention and Disposal Schedule**

Only Excluded Records, as defined in this Policy and expanded upon in the Recordkeeping, Reporting and Data Breach Procedure, which is a very narrow subset of Records can be disposed of at any time. The Records Officer should be consulted if there is any doubt as to what they are.

Where the official version of a Record is verified as being already maintained in Council's Recordkeeping system a copy may be destroyed/disposed of, in the appropriate manner, at any time without reference to the Retention and Disposal Schedules.

All other Records must be retained in Council's Internal Recordkeeping System and disposed

of in accordance with this Policy. Amendment of a Record is taken to be Disposal of a Record.

### **3.8 Mandatory Self-Reporting and Other Reporting on non-Compliance with this Policy**

- 3.8.1 Recordkeeping of Council Records is one of the most complex governance requirements of any local government.
- 3.8.2 Where any person identifies any breach of this Policy, whether by action or omission, use of an Application, Recordkeeping of any Record (other than an Excluded Record) including Record Capture, Access, Access Control, Disclosure, Retention, Disposal, irrespective of Device or Storage Device, it is mandatory that this must be immediately reported in writing to the reporting person's relevant supervisor and the Records Officer in accordance with the Recordkeeping, Reporting and Data Breach Procedure.
- 3.8.3 The Policy facilitates a non-punitive, educative and supportive approach to any person who self-reports unintentional, or incapacity based, non-compliance with this Policy, that can be reasonably explained, in accordance with the Recordkeeping, Reporting and Data Breach Procedure.

## **4 Internal Recordkeeping System and Enterprise Management System**

### **4.1 Internal Recordkeeping System**

- 4.1.1 Council's Internal Recordkeeping System (the Internal Recordkeeping System) is defined in the Recordkeeping, Reporting and Data Breach Procedure, where it is mandatory all Records are captured and stored.
- 4.1.2 Access to the Internal Recordkeeping System must be Access Controlled and secured by appropriate means, which as a minimum must include two factor authentication (2FA), where the Application provides for this.
- 4.1.3 Council's Internal Recordkeeping System (IRS) is dedicated to creating and maintaining authentic, reliable and useable Records which meet the needs of internal and external stakeholders.
- 4.1.4 Records are maintained for as long as they are required to by law and longer if they effectively and efficiently support Council's business functions and activities.
- 4.1.5 Paper-based Records received by Council must be captured within the Internal Record Keeping system through digital imaging.
- 4.1.6 The Internal Recordkeeping System is the sole source of truth for Records and reference to the Record in the Enterprise Management System should be referenced to the Internal Recordkeeping System in accordance with the Recordkeeping, Reporting and Data Breach Procedure.
- 4.1.7 Alternative electronic storage facilities do not contain Recordkeeping functionality to ensure Records are captured and managed in accordance with sound Recordkeeping principles.
- 4.1.8 Council's Internal Recordkeeping Systems manage the following processes and associated Reporting:
  - Creation and Capture of Records, including Excluded Records;
  - Storage of Records;
  - Protection of Record integrity and authenticity;
  - Security of Records;
  - Access to Records including with Access Control;
  - Disposal of Records in accordance with retention and disposal

schedules;

- Recordkeeping Reporting;
- Governance Reporting;
- Performance of Council's statutory functions and achievement of the Corporate Plan; and
- Real time dashboards and other historical Reporting.

## **4.2 Enterprise Management System**

- 4.2.1 The Internal Recordkeeping system is distinct from other software used by Council, including the Enterprise Management System (EMS).
- 4.2.2 Records may be required to be kept in the Internal Recordkeeping System and the Enterprise Management System or other specific software used by Council.
- 4.2.3 Where Records are required to be kept in the IRS and the EMS, the Recordkeeping, Reporting and Data Breach Procedure must identify the methodology.
- 4.2.4 All of Council's Records must be maintained within the Internal Recordkeeping System and where appropriate identified or referred to in the Enterprise Management System in a manner to avoid duplication.

## **4.3 Mandatory Requirement to Transfer Record to Internal Recordkeeping System**

- 4.3.1 If Council has provided or made available, it is mandatory each:
  - 4.3.1.1 each Device provided must be used as the sole device used for its purpose and not used for an unintended purpose;
  - 4.3.1.2 any Application, or Access methodology related to any Record, including with any Access Control restrictions, each must be used as the sole way to be used for its intended purpose and not to used for an unintended purpose; and
  - 4.3.1.3 any Application or Access methodology that is not the Internal Recordkeeping System must be transferred to the IRS, and where appropriate the Enterprise Management System (EMS), contemporaneously, and in accordance with the Recordkeeping, Reporting and Data Breach Procedure.
- 4.3.2 If a person covered by this Policy uses any Non-Council provided Application, Device, Storage Device, or other thing, connected to Council Records, Recordkeeping, including Access, Access Control, it is mandatory:
  - 4.3.2.1 each must be approved in accordance with the Recordkeeping, Reporting and Data Breach Procedure; then
  - 4.3.2.2 any Record must be transferred as soon as practicable to the IRS, in accordance with the Recordkeeping, Reporting and Data Breach Procedure which may also require this to be recorded in the EMS.
- 4.3.3 If the person or persons involved in any Recordkeeping of a Council Record is in anyway unable to strictly comply with this Policy, it is mandatory that they must immediately disclose this to their Supervisor and the Records Officer and for this disclosure to be in writing and in accordance with the Recordkeeping, Reporting and Data Breach Procedure.

## **4.4 Request to Access Records to support Aboriginal people and Torres Strait Islander**

## **communities**

- 4.4.1 Subject to some exceptions, it will be unlawful for Council to make a decision or take an action that is not compatible with human rights, or to make a decision and fail to give proper consideration to relevant human rights.
- 4.4.2 Council will ensure the proper handling and accessibility of Public Records to support Aboriginal people and Torres Strait Islander communities and recognise, the rights of Indigenous peoples in Australia and will support culturally sensitive making, managing and accessing of Public Records.
- 4.4.3 The Recordkeeping, Reporting and Data Breach Procedure is to be updated to incorporate the First Nations Advisory Group perspectives, as provided by Public Records Review Committee from time to time, empowered by the *Public Records Act 2023*.

## **4.5 Restricted Records and Prevention of Unauthorised Authorised Access**

- 4.5.1 Council must take reasonable steps to ensure Records that must or should be restricted are suitably secure and have Access Control, to only those with a specific requirement, having regard for their role, qualification, delegation or statutory power.
- 4.5.2 Council must implement both covert and overt monitoring of access, including logging user Access, including to Access Controlled Records, to reduce the risk of unauthorised Access and unauthorised Disclosure of Records.

## **4.6 Prohibited Recordkeeping**

- 4.6.1 Each of the following are prohibited:
  - 4.6.1.1 Disposing of Council Records;
  - 4.6.1.2 the use of undisclosed listening devices, irrespective as to whether the user is a party to the conversation or not;
  - 4.6.1.3 creating, using, accessing or keeping a Record for a reason other than the stated purpose, unless this is authorised or required under a law, but only then if this in accordance with the Recordkeeping, Reporting and Data Breach Procedure;
  - 4.6.1.4 the use of alternatives to the Internal Recordkeeping System and the Enterprise Management System as a method of Recordkeeping;
  - 4.6.1.5 Records stored are accessed in network drives (for example S drive) or other storage devices, Microsoft 365, SharePoint or file services such as Dropbox, without the written authority of the CEO who is only authorised to permit a duplicate Record of one contained in the Internal Recordkeeping System;
  - 4.6.1.6 The use of any device, Application, virtual private network, personal email, messaging application (including with timed auto-delete functionality), other communication method that creates or stores Records, technology the prevents or limits any Record from being kept in accordance with this Policy, or that could subvert the true identity, location or detection of the person dealing with a Record, including Record Access, with or without Access Control.
- 4.6.2 The Chief Executive Officer must ensure the Recordkeeping, Reporting and Data Breach Procedure strictly enforces the prohibitions and including serious sanctions for even a single breach of this prohibition.

## **5 Data Breach**

### **5.1 What is a Data Breach?**

A 'data breach' of an agency means either of the following in relation to information held by Council:

- 5.1.1 unauthorised access to, or unauthorised disclosure of, the information.
- 5.1.2 the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

The above definition encompasses any information held by an agency. Under section 47, for a data breach to be an 'eligible data breach' triggering notification and obligations under the Mandatory Notification of Data Breach (MNDB) Scheme, which Queensland is a signatory to, from 1 July 2026, both of the following must apply:

- 5.1.3 there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or
- 5.1.4 unauthorised disclosure of the information is likely to occur, and
- 5.1.5 the unauthorised access or disclosure of the information is likely to result in serious harm to an individual

### **5.2 Council to Prepare for the Mandatory Notification of Data Breach (of Personal Information) Scheme – Data Breach Registers and Policies**

Personal Information means: "information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether the information or opinion is true or Recorded in a material form."

The Recordkeeping of Council, including with the Internal Recordkeeping System, must be designed to protect Personal Information from:

- 5.2.1 unauthorised access and unauthorised disclosure; and
- 5.2.2 the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

Any person covered by the Scope of this Policy must be trained so they comprehend the meaning of:

- 5.2.3 "unauthorised access" and "unauthorised disclosure" of personal information, and how to report and respond to any potential or actual unauthorised access or unauthorised disclosure event.
- 5.2.4 the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur and how to report and respond to any potential or actual loss event

## **6 Recordkeeping and Reporting Responsibility**

### **6.1 CEO**

The CEO is responsible for ensuring Council's compliance with the *Public Records Act 2002* and the principles and standards established by Queensland State Archives, and include:

- 6.1.1 Accounting for Recordkeeping and Recordkeeping systems within Council to Ministers, Parliament and others as required;
- 6.1.2 Creating and maintaining a Recordkeeping, Reporting and Data Breach Procedure

- 6.1.3 Assigning Recordkeeping responsibilities within Council;
- 6.1.4 Providing appropriate resources to maintain Recordkeeping systems and processes;
- 6.1.5 Ensuring Recordkeeping systems are in place and produce complete and reliable Records;
- 6.1.6 Ensuring Recordkeeping requirements are included in all business undertaken by Council;
- 6.1.7 Taking all reasonable steps to implement recommendations made by the State Archivist;
- 6.1.8 Publishing a Recordkeeping, Reporting and Data Breach Procedure to achieve this Policy's purpose;
- 6.1.9 Actively promoting and supporting a positive Recordkeeping culture throughout Council;
- 6.1.10 Ensuring employees, contractors and volunteers are aware of their Recordkeeping responsibilities; and
- 6.1.11 Ensuring Council's Reporting on Records and performance is accurately reported and aligned with the Operational Plan including Council, departmental and work area real time, historical and live dashboard Reporting.
- 6.1.12 These responsibilities are delegated to relevant positions in accordance with the provisions set out below or as otherwise delegated by the CEO in accordance with the Delegations Policy or as they see fit.

## **6.2 Director Corporate, Governance and Risk**

The Director Corporate, Governance and Risk shall:

- 6.2.1 Approve and implement 2 Factor Authentication (2FA), the Record folder structure and Council wide file and folder naming conventions, workflows, tasking, expiry dates, for the Internal Recordkeeping System to achieve the Policy Statement objectives, and the Corporate Plan, including Record access, retention, disposal, standard and ad hoc Reporting and real time dashboards.
- 6.2.2 Approve and implement a suite of reports and dashboards to comply with this Policy, to support the Corporate Plan, monitor Record access, governance, workflow and fact finding and as otherwise requested by the CEO;
- 6.2.3 Source and retain expert advice on information technology for Recordkeeping strategies in an electronic environment;
- 6.2.4 Source and retain the technical infrastructure required for Recordkeeping and Reporting;
- 6.2.5 Supply technical support for the Recordkeeping systems;
- 6.2.6 In partnership with the Records Officer; develop, manage and monitor the technical aspects of:
  - Disaster preparedness and recovery strategies and procedures;
  - Records and systems migration strategies and procedures;
  - Regular backups for Records and Recordkeeping systems and business systems that create and store Records; and
  - Manage the security mechanism for the protection from unauthorised access to information in electronic form, including real time access alerts for Records



described in the Recordkeeping and Reporting Policy.

### **6.3 Records Officer**

The Records Officer Shall:

- 6.3.1 Implement Recordkeeping processes consistent with this Policy and the Recordkeeping, Reporting and Data Breach Procedures;
- 6.3.2 Identify Recordkeeping requirements in consultation with other organisational units;
- 6.3.3 Consult with Queensland State Archives in relation to policy and Information Standards development;
- 6.3.4 Make, keep and preserve complete and reliable Records that document business transactions within compliant and accountable Recordkeeping systems;
- 6.3.5 Develop and implement an active Records training and awareness program in relation to Recordkeeping obligations, processes and procedures, including inductions for new employees;
- 6.3.6 Promoting and facilitating Records management compliance including with naming conventions, expiry dates, correct folder usage, workflow usage tasking, and associated Reporting;
- 6.3.7 Ensure strategies and procedures exist to identify and locate Records;
- 6.3.8 Develop and maintain Recordkeeping administration for Council's Internal Recordkeeping System;
- 6.3.9 Monitor compliance with this Policy and Recordkeeping, Reporting and Data Breach Procedure, system and procedures and makes recommendations to the CEO/Directors/Managers and Supervisors for improvement or modifications of practices;
- 6.3.10 Develop and implement an internal Recordkeeping framework, including policies, standards, procedures and tools;
- 6.3.11 Identify and manage vital corporate Records regarding the relevant storage parameters and accessibility standards; and
- 6.3.12 Develop, manage, test and review disaster preparedness and recovery strategies and procedures for all Records, including electronic Records.

### **6.4 Managers and Supervisors**

Managers and Supervisors shall

- 6.4.1 Ensure complete and reliable Records are made and captured into the relevant Record and business systems that create and maintain Records, and at all times using and ensuring their team use the correct Recordkeeping workflow trigger, including in the IRS;
- 6.4.2 Ensure Recordkeeping systems underpin and support business processes and report any deficiencies to the CEO, Records Officer and Director Corporate, Governance and Risk; and
- 6.4.3 Train, coach, support and monitor employee, contractor and volunteer achieve best practice compliance with this Policy, Recordkeeping, Reporting and Data Breach Procedure, and associated processes and practices.

### **6.5 Councillors, employees, contractors and volunteers**

Councillors, employees, contractors and volunteers shall:

- 6.5.1 Each Councillor, employee, contractor and volunteer is responsible for creating and

registering Records that are evidence of business activity (inclusive of emails and mobile phone data);

6.5.2 All Councillors, employees, contractors and volunteers have the following obligations regarding Recordkeeping:

- 6.5.2.1 All are required to protect and maintain the privacy of personal and confidential information contained in council Records;
- 6.5.2.2 Create, capture, describe and store Records to support the conduct of Council activities in conjunction with approved metadata;
- 6.5.2.3 Create complete and reliable Records of Council business in accordance with the *Public Records Act 2002*;
- 6.5.2.4 Comply with all policy documents introduced to foster Recordkeeping best practice throughout Council in compliance with the State Archivist Records Governance Policy;
- 6.5.2.5 Council staff have a legal obligation to always ensure that high standards of data quality, data protection, integrity, confidentiality and Recordkeeping are met in compliance with the relevant legislation. It is responsibility of all employees to familiarise themselves with the Recordkeeping and Reporting and adhere to the principles...
- 6.5.2.6 Capture Council's Records into the relevant Recordkeeping system at the time of creation or receipt, and at all times using the correct Recordkeeping workflow trigger, or other method;
- 6.5.2.7 Keep Records for as long as they are required for business, legislative, accountability and cultural purposes;
- 6.5.2.8 Ensure that Records in any format, including electronic documents and messages are captured into the Internal Record Keeping System in accordance with Council's Recordkeeping, Reporting and Data Breach Procedures and protocols;
- 6.5.2.9 Adhere to confidentiality and privacy principles when dealing with Records;
- 6.5.2.10 Request assistance if unable to achieve these responsibilities; and
- 6.5.2.11 Immediately Mandatorily report non-Compliance with this Policy at each instance non-compliance is observed.

## 7 Breach of Policy

Inadequate management of Public Records can constitute corruption. It can also result in disciplinary action which may lead to dismissal and/or civil legal action against the individual and organisation involved.

## 8 Definitions

Access	Includes to log-in, read, edit or otherwise consume, whether in person, digitally, through or arising from any Virtual Private Network, Application programming interface (Api), or other exporting/importing methodology
Access Control	The process of Council granting or denying requests for access to systems, Applications and Records, including the process of granting or denying requests for access to facilities, through any digital item, or Access methodology, Application, software or software as a service, virtual private network, email,


	communication tool, or any other platform capable of Recordkeeping, Application programming interface (Api), or other exporting/importing methodology
Application	Means a software program, Software as a Service, or group of software programs designed for end users. Examples of an application include any EMS, IRS, word processor, a spreadsheet, an accounting application, a web browser, an email client, a media player, a file viewer, a video and/or audio Recorder, messenger or communication tool, an aeronautical flight simulator, a console game, or a photo editor, with or without Artificial Intelligence (AI) capability. The collective noun application software refers to all applications collectively. This contrasts with system software, which is mainly involved with running the computer.
Capture	A deliberate action which results in the registration of a Record into the IRS and EMS
Council	Means Paroo Shire Council
Device	Means any physical item, including any computer, tablet, smartphone, mobile phone, any other device, equipment (such as CCTV, CC Audio, Body Worn Camera and Microphone, other camera or audio device) or other physical technology or any other thing related to Recordkeeping
Disclosure	Means the same as s 23(2) of the <i>Information Privacy Act 2009</i> : An entity (the first entity) discloses personal information to another entity (the second entity) if—  (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and  (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and  (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.
Disposal	"Dispose" has a broad meaning and includes to delete the Record or alter or damage the Record. The alteration or damage to the Record must change how accurately an action or decision is shown in the Record or otherwise affects the integrity of the Record
Enterprise Management System (EMS)	Means Practical Plus including any associated accounting or invoicing subscriptions
Excluded Record	Ephemeral Records (that is items of short-term temporary informational value that are not required to be kept as Records)

		may be destroyed at any time without reference to a retention and disposal schedule. These Records which may include announcements of social events, duplicate copies or extracts of documents kept only for reference, copies of circulars, forms, etc, can be disposed of as part of normal office administrative practice
Internal Keeping (IRS)	Record System	Means Magiq Documents Module, which is designed to facilitate the creation management, use, storage, retention, access, disclosure and disposal of a range of physical (including location pre-being digitised) and digital Records used by Council (also known as InfoXpert or eDRMS)
Metadata		Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time
Record		<p>Any form of recorded information, both received and created, that provides evidence of any of Councils activities, decisions and actions, while undertaking its functions other than an Excluded Record.</p> <p>Public Records can take many forms, they can include (but are not limited to): Video including CCTV, audio recordings – with or without CCTV, body worn camera footage, text messages, emails, mobile phone data, Applications, including social media interactions, data held in the IRS, the EMS, other business systems, data in messaging Applications, including WhatsApp, Facebook Messenger, Signal, Snapchat and all associated metadata and contextual information.</p> <p>Means any recorded information created or received by a Council in the transaction of its functions or the conduct of affairs including:</p> <ul style="list-style-type: none"> <li>a) Anything on which there is writing; or</li> <li>b) Anything on which there are marks, figures, symbols or perforation having a meaning for persons, including persons qualified to interpret them; or</li> <li>c) Anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or</li> <li>d) A map, plan, drawing or photograph. Source <i>Public Records Act 2002</i> definitions; and</li> <li>e) Must include any contextual information, including metadata.</li> </ul>
Recordkeeping		Making and maintaining of complete, accurate and reliable evidence of Council functions, decisions and actions, including contextual material, in the form of Recorded information in accordance with the <i>Public Records Act</i> (as amended) and requirements of the State Archivist (as amended) and as described in this Policy.
Records/Public Records		Records and Public Records mean more than one Record and have the same meaning, and are used interchangeable, meaning any Record that is not an Excluded Record.

Reporting	Includes any reporting to achieve: best practice Recordkeeping; the Corporate Plan; the Operational Plan; and any other Council function, in real time and/or historical all-of-Council, Department, Work Unit, officer, contractor and third-party reporting, relating to: performance; conduct; investigation and fact finding; compliance; enforcement; monitoring; governance - whether pending, in progress or completed, or as otherwise requested by the CEO.
Retention and Disposal Schedule	A legal document issued by the Queensland State Archivist to authorise the disposal of Public Records under the <i>Public Records Act 2002</i> and <i>Public Records Act 2023</i> .
Retention Period	The minimum period that Records need to be kept before their final disposal as specified in unauthorised retention and disposal schedule.
Storage Device	Includes any place where any Record is stored. It could be disk storage, a flash drive, a backup disk drive, an online backup service, an indexing internet page, mobile phone, tablet, virtual private network, including through Application programming interface (Api), or other exporting/importing methodology

## 9 Relevant Links

- *Crime and Corruption Act 2001*
- *Electronic Transactions Act 2001*
- *Evidence Act 1977*
- *Human Rights Act 2019 (Qld)*
- *Industrial Relations Act 2016 (Qld)*
- *Information Privacy Act 2009 including the Information Privacy Principles (Schedule 3)*
- *Information Privacy and Other Legislation Amendment Act 2023*
- *Invasion of Privacy Act 1971 (Qld)*
- *Local Government Act 2009*
- *Public Records Act 2002*
- *Right to Information Act 2009*
- *Uniform Civil Procedure Rules 1999*
- *Industrial Relations (Tribunal Rules) 2011*
- PCOM030 - Body Worn Camera
- Local Government Sector Retention and Disposal Schedule
- Queensland State Archives Records Governance Policy
- Queensland recordkeeping metadata standard and guideline 2012 (and successors)
- Applying the legislation – *Information Privacy Act 2009* GUIDELINE Information Privacy Act 2009 - Mandatory Notification of Data Breach scheme

<b>Endorsed</b>		<b>Date:</b> 15/10/2024
<b>Name:</b>	Neil Polglase	
<b>Title:</b>	Interim Chief Executive Officer, Paroo Shire Council	
<b>Signature:</b>		

#### Version Control

Date	Version	Meeting Resolution	Amendments / Comments
15/10/2024	1.0	M24/282	