RECORDS AND INFORMATION MANAGEMENT

POLICY

JUSTICE AND COMMUNITY SAFETY DIRECTORATE

DOCUMENT INFORMATION

Date approved/effective:	28 August 2025
Date last reviewed:	28 August 2025
Endorsed by:	Richard Glenn, Director-General
Policy Custodian:	Executive Branch Manager, Governance and Business Improvement
Review date:	Three years from date of effect/last review

UNCONTROLLED IF PRINTED

CONTENTS

1. DEFINITION OF TERMS 3
2. PURPOSE 3
3. SCOPE 3
4. POLICY STATEMENT 3
5. ROLES AND RESPONSIBILITIES 4
6. RECORDS AND INFORMATION MANAGEMENT PRINCIPLES 6
7. RECORDS AND INFORMATION FRAMEWORK 7
8. ENDORSED LOCATIONS 9
9. PROCEDURES FOR RECORDS AND INFORMATION MANAGEMENT 11
10. ENQUIRIES 11

© Australian Capital Territory 2025



This work, the JACS Records and Information Management Policy is licensed under a Creative Commons Attribution 4.0 licence.
You are free to re-use the work under that licence, on the condition that you credit the Australian Capital Territory Government as author.

The licence does not apply to the ACT Government logo.

1. DEFINITION OF TERMS

Term	Definition
Officer	For the purpose of this document, the term 'officer' includes all staff, volunteers, consultants, contractors and outsourced providers acting on behalf of the Directorate.
Records and Information	Information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation, or in the course of conducting business.
Records and Information Management	Records and information management covers, but is not limited to, the creation, keeping, protection, preservation, storage and disposal of, and access to records of the Directorate.

2. PURPOSE

2.1 The Justice and Community Safety (JACS) Directorate is responsible for creating and maintaining records to inform and support decisions made within the Directorate. It is important that these records are readily available to the Directorate and the community, now and in the future.

2.2 This policy forms part of the records and information governance framework for the creation, capture and management of records and information in the Directorate.

3. SCOPE

3.1 This policy applies to all full time and part time staff, volunteers, consultants, contractors and outsourced providers as per the *Territory Records Act 2002* (the TR Act). This includes staff employed by a Statutory Office Holder where the relevant Principal Officer has adopted the JACS Records Management Program.

3.2 This policy applies to all aspects of Directorate operations including all records and information created during business transactions, and all business applications used to create or store records and information including email, cloud-based solutions, business systems, databases and websites.

4. POLICY STATEMENT

4.1 Information and records are vital government and public assets and their management is the responsibility of all who work directly and indirectly for the Directorate.

4.2 The Directorate is committed to the proper management of records and information as mandated by the TR Act and will ensure records and information is retained for as long as required in a readily accessible form.

4.3 This policy provides the basis for how the Directorate, and all individuals acting on behalf of the Directorate, adhere to legislative and better practice requirements for records and information, including what is outlined in the:

- *Territory Records Act 2002*
- JACS Directorate's Records and Information Management Program
- Territory Records Office's Standard for Records and Information Governance
- Territory Records Office's guidelines to implement the Standard for Records and Information Governance
- International and Australian standards.

4.4 The policy is complemented by the ACT Government Data Governance and Management Policy Framework, which sets out the essential data governance and management practices required to ensure data is captured, protected, used and shared to effectively support decision making for the ACT community.

4.5 All individuals acting on behalf of the Directorate **must** make, keep and manage full and accurate records in a timely manner to support business needs, government accountability, legal and regulatory obligations, community expectations and for historical purposes.

4.6 All records, information and data received or generated by staff, volunteers, consultants, contractors and outsourced providers as part of their duties are Territory records and belong to the ACT Government and not to individuals, agencies or companies.

4.7 This policy will be referenced in Directorate policies and procedures wherever possible to ensure its application is widespread and consistent.

5. ROLES AND RESPONSIBILITIES

Role	Responsibilities
All Staff	All staff are responsible for the creation and management of records and information about the work they perform on behalf of the JACS Directorate.
Principal Officer	The Principal Officer is ultimately responsible for the management of records and information for the administrative unit, and: • promoting compliance with this policy • delegating responsibility for overseeing records and information to an appropriate executive

Role	Responsibilities
	• ensuring the Records and Information Management Program is adequately resourced. • For JACS, the Principal Officer is the Director-General. For Statutory Offices and any entity declared or identified as an agency under the TR Act, the Principal Officer is the person prescribed by regulation to be the Principal Officer of that agency.
Executive Branch Manager, Governance and Business Improvement	The Executive Branch Manager, Governance and Business Improvement is responsible for the active support of, and adherence to, this policy by promoting a culture of compliance with records and information governance and overseeing the development and currency of strategic information management documents.
Records Management staff	Records management staff are responsible for implementing and monitoring legislative and better practice requirements for records and information. An important aspect includes the identification of records and information management requirements, and the development, implementation and support of records and information management procedures. Records management staff are also responsible for: • encouraging and maintaining compliance with the Records and Information Management Standard Operating Procedure • ensuring effective communication of the JACS Directorate's Records and Information Management Program • being a source of recordkeeping knowledge and advice • contributing to the design, development and maintenance of recordkeeping systems • contributing to the procurement and design of new business systems to promote the principle of 'records by design' • preparing and reviewing policies, procedures and work instructions for efficient record management operation • contributing to the development and review of the Whole of Government Records Disposal Schedules that are utilised across the ACT Government.

Role	Responsibilities
ICT Staff	ICT staff, including Digital Canberra staff, are responsible for maintaining the technology for business systems including appropriate system accessibility, security and back-ups. ICT staff should ensure that any actions such as removing data from systems or folders, are undertaken in accordance with this policy, particularly in terms of the retain principle (outlined below).
Agency Security Advisor	The Agency Security Advisor provides advice on security policies and guidelines associated with the management of records and information.
Managers and Supervisors	All managers and supervisors are responsible for ensuring their staff, consultants, contractors and outsourced providers are aware of, and follow their responsibilities for records and information management. This includes addressing records and information management during performance review discussions and when establishing job descriptions. Managers and supervisors **must** also consult with JACS Records Management staff of any changes in the business environment that may affect the creation and management of records and information, such as the planned de-commission and procurement of business systems.
Volunteers, Contractors, Consultants and Service Providers	Volunteers, contract staff, consultants and services providers acting on behalf of the Directorate are responsible for the creation and management of records and information about the work they perform on behalf of the Directorate.

6. RECORDS AND INFORMATION MANAGEMENT PRINCIPLES

6.1 The Directorate's records and information will be managed according to the principles outlined in the Standard for Records and Information Governance released by the Director of Territory Records. This includes:

5.1 Principle 1 - Strategy: The Directorate strategically manages its records and information by applying the Records and Information Management Program and this policy.

5.2 Principle 2 - Capability: The Directorate has established and continues to grow its capability to effectively manage records and information. We review our capability on a regular basis and implement plans to build our records and information management maturity.

5.3 Principle 3 - Assess: The Directorate assesses its records and information management requirements to ensure appropriate evidence of our business activities is captured and maintained.

5.4 Principle 4 - Describe: The Directorate maintains control over its records and information by ensuring it has systems in place to maintain authenticity, usability and reliability.

5.5 Principle 5 - Protect: The Directorate ensures there are appropriate storage and preservation mechanisms in place to protect our records and information.

5.6 Principle 6 - Retain: The Directorate assesses its records and information to determine appropriate retention periods.

5.7 Principle 7 - Access: The Directorate ensures records are managed so they can be found, accessed, used and re-used wherever appropriate.

7. RECORDS AND INFORMATION FRAMEWORK

7.1 LEGISLATION

7.1.1 The Directorate **must** comply with a range of laws related to the creation and capture of records and information.

7.1.2 In general, all business units **must** comply with the:

- *Territory Records Act 2002*
- *Freedom of Information Act 2016*
- *Evidence Act 2011*
- *Information Privacy Act 2014*
- *Health Records (Privacy and Access) Act 1997*
- *Human Rights Act 2004*
- *Electronic Transactions Act 2001*
- *Public Sector Management Act 1994*
- *Financial Management Act 1996*
- *Work Health and Safety Act 2011*
- *Working with Vulnerable People (Background Checking) Act 2011*

7.1.3 Business units may also have to comply with legislative recordkeeping requirements from time to time specific to their functions. The specific legislation applicable to Directorate functions can be found in the Administrative Arrangements available on the ACT Legislation Register.

7.2 STANDARDS AND REGULATIONS

7.2.1 Standards and regulations also help guide the Directorate in performing its functions. The Directorate operates in line with numerous standards, regulations, schemes, notifications, directions, delegations, and memorandums that relate to the functions prescribed under the Administrative Arrangements. The Directorate applies the following records management standards:

- ASO ISO: 15489 - Records Management
- SA/SNZ TR ISO: 26122 - Work Process Analysis for Recordkeeping
- AS: 5044 - AGLS Metadata Standard
- AS/NZS 5478: 2015 – Recordkeeping Metadata Property Reference Set
- ISO: 16175 - Principles and Functional Requirements for Records in Electronic Office Environments

7.3 ASSOCIATED POLICIES AND PROCEDURES

7.3.1 The Directorate has also adopted a range of policies relevant to the management of records and information that **must** be applied alongside this Policy, including, but not limited to:

- ACT Public Service Code of Conduct
- ACT Public Service Code of Ethics
- ACT Government Data Governance and Management Policy Framework & Guide
- ACTPS Data Sharing Policy
- ACTPS Protective Security Framework
- ACTPS Social Media Guidelines for Official Use
- ACTPS Social Media Guidelines for Personal Use
- ACTPS Acceptable Use of ICT Resources Policy
- ACTPS Cyber Security Policy

- JACS Records and Information Management Program
- JACS Records and Information Management Standard Operating Procedure
- JACS Privacy Policy
- JACS Data Breach Standard Operating Procedure
- JACS Protection of Information Standard Operating Procedure
- JACS Freedom of Information Policy
- JACS Open Access Policy

7.3.2 This Policy should also be applied in conjunction with any business unit policy or procedure documents that relate to the creation and management of records and information in the delivery of business functions.

8. ENDORSED LOCATIONS

8.1 Only endorsed locations can be used to store records to ensure they are readily accessible, appropriately protected, and retain their integrity as evidence.

8.2 For locations to be endorsed, they **must** be registered with the JACS records management team to help ensure appropriate records management processes can be applied and, where appropriate, supported by the development of information management plans.

8.3 The following are endorsed locations for the storage of Directorate records:

Physical

- Territory Archives, Building 7, 9 Sandford Street, Mitchell ACT
- approved secondary records management storage providers, including Grace and Iron Mountain (for existing stored items only).
- workplaces that accommodate JACS Directorate staff and approved volunteer locations (note, a basement or other non-standard floor space is not an endorsed location until it has been assessed and approved to hold records).

Digital

- Content Manager (CM) (also known as TRIM) where staff are using Electronic Document and Records Management System (EDRMS) record types, including where this has been integrated with business systems
- Objective (Public Trustee and Guardian only)

- approved business applications.

8.4 The following are non-endorsed locations:

Physical

- unoccupied outbuildings
- any location that is not under the direct control of the Directorate, such as a personal residence
- any other location that could reasonably be representing a risk to physical records.

Electronic

- Outlook
- SharePoint (including the JACS intranet)
- Microsoft Teams and Viva Engage
- One Drive
- network drives (such as the G drive)
- staff drives (such as the H drive)
- portable devices (such as flash drives)
- personal IT devices
- unapproved business systems.

8.5 Directorate records and information held in non-endorsed locations, including on personal devices or accounts, remain subject to the access provisions of the *Freedom of Information Act 2016*.

8.6 Records and information captured in a non-endorsed location should be moved to an endorsed location as early as possible to promote accessibility and ensure appropriate management principles are applied.

8.7 Records held on network drives pending migration to an EDRMS should be managed and structured in a way that supports their integrity and accessibility. This includes implementing proper naming conventions and managing the lifecycle of the record in accordance with its approved Record Disposal Schedule.

9. PROCEDURES FOR RECORDS AND INFORMATION MANAGEMENT

9.1 This policy is supported by the Records and Information Management Standard Operating Procedures and forms part of the broader records and information management framework.

9.2 The procedures detail the way officers - including staff, volunteers, contractors and consultants – in the Directorate will create, capture, manage, care for, keep and access records and information.

9.3 JACS records management staff are responsible for coordinating the development of procedures for these processes.

9.4 Adherence to the requirements of the procedures is obligatory for all staff, volunteers, consultants and contractors to ensure legislative requirements are met.

10. ENQUIRIES

Enquiries about this policy can be directed to:

Governance, Coordination and Reporting
JACSGCR@act.gov.au

DETAILS

Document Properties	Approval Details
Document Name:	Records and Information Management Policy
Document Number:	0079-1
Custodian:	Executive Branch Manager, Governance and Business Improvement
Advisor:	JACS Senior Records Officer (SRO)
Responsible Branch:	Governance, Coordination and Reporting
Stakeholders:	All JACS staff
Document/Legislation References:	*Territory Records Act 2002* *Freedom of Information Act 2016* *Information Privacy Act 2014* *Public Sector Management Act 1994* *Electronic Transactions Act 2001* Digital Recordkeeping Policy for the ACTPS ACT Government Data Governance and Management Policy Framework and Guide JACS Privacy Policy JACS Data Breach Standard Operating Procedure JACS Freedom of Information Policy

AMENDMENT HISTORY

Version	Issue Date	Amendment Details	Author	Approved by
1.0	27 June 2018	New version of Records Management Policy	JACS Records Manager	Director-General
1.1	January 2021	Reviewed	JACS SRO	Director-General
1.2	December 2021	Transfer to the new SOP template	JACS SRO	EBM, GBI
1.3	September 2022	Minor Update.	JACS SRO	Director-General
1.4	August 2025	Administrative update.	JACS SRO	EBM, GBI