RECORDS AND INFORMATION MANAGEMENT

STANDARD OPERATING PROCEDURE

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
Custodian:	Executive Business Manager, Governance and Business Improvement
Review date:	Three years from date of effect/last review

CONTENTS

1. PURPOSE 3
2. SCOPE 3
3. ROLES AND RESPONSIBILITIES 3
4. WHAT IS A RECORD 4
5. WHAT IS THE DIRECTORATE'S OFFICIAL RECORDKEEPING SYSTEM 5
6. RECORD CREATION 6
7. STANDARDS 7
8. FILE TITLING 9
9. HANDLING DIFFERENT TYPES OF RECORDS 11
10. RECORDS MANAGEMENT AND PRESERVATION 12
11. RECORD ACCESS 16
12. RECORD DISPOSAL 17
13. ENQUIRIES 22

© Australian Capital Territory 2025

This work, the JACS Records and Information Management Standard Operating Procedure 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. PURPOSE

1.1 The Justice and Community Safety (JACS) Directorate values records and information as critical assets that support, inform, and provide evidence of business activity and promote government accountability and transparency.

1.2 This Standard Operating Procedure (SOP) supports the JACS Directorate's Records and Information Management Program by outlining procedures for good recordkeeping, record preservation and record disposal.

1.3 The SOP should be read in conjunction with the following policy documents to effectively understand your role and responsibility for creating, managing and maintaining JACS information:

- JACS Records and Information Management Program
- JACS Records and Information Management Policy
- JACS Protection of Information Standard Operating Procedure
- ACTPS Data Governance and Management Policy Framework
- ACTPS Data Governance and Management Guide
- JACS Privacy Policy
- JACS Data Breach Standard Operating Procedure.

1.4 The SOP should also be read in conjunction with any business unit policy or procedure documents that relate to the creation or management of records and information in relation to the delivery of business functions.

2. SCOPE

2.1 This SOP applies to all officers including full time and part time staff, volunteers, consultants, contractors and outsourced providers as per the *Territory Records Act 2002* (the TR Act). The includes staff of a Statutory Office where the relevant Principal Officer has adopted the JACS Records and Information Management Program.

2.2 Some actions discussed in this SOP are solely carried out by dedicated records management staff, while others should be followed by all staff.

3. ROLES AND RESPONSIBILITIES

3.1 The Director-General is ultimately responsible for the management of Directorate records and information and has authorised the Records and Information Management Program and Policy under which these Procedures have been developed.

3.2 The Executive Branch Manager, Governance and Business Improvement is responsible for the active support of, and promoting adherence to, the Records and Information Management Program, Policy and Procedures.

3.3 Records management staff in Governance, Coordination and Reporting (GCR) are responsible for ensuring the Records and Information Management Policy and Procedure for the creation, maintenance and destruction of records is appropriately communicated and implemented.

3.4 This includes ensuring JACS officers:

- understand their recordkeeping obligations and responsibilities that relate to their role in the Directorate.
- have the appropriate knowledge and tools to adhere to ACT Government policies, procedures and standards for keeping records, documenting their activities on behalf of the Directorate and the ACT Government.
- only destroy records under an approved Record Disposal Schedule or in accordance with Normal Administrative Practice (NAP).

3.5 All officers are responsible for the creation and proper management of records and information about work they perform on behalf of the Directorate.

3.6 Further guidance on roles and responsibilities can be found in the Records and Information Management Policy.

4. WHAT IS A RECORD

4.1 ELEMENTS OF A RECORD

4.1.1 A record is any piece of information that is created, received and maintained as evidence and information by an agency or person, in pursuance of legal obligations or in the transaction of business[1].

4.1.2 Records provide proof of what happened, when it happened and who made the decisions. Records are created to support business activity and keep evidence of that activity. Because records provide evidence of business activity, they **must** be created and maintained in a manner that promotes the principles of accountability and open government. This includes preserving records to facilitate public access, both now and in the future.

4.1.3 To be relied upon, records **must** be complete and accurate, classified correctly, trackable, and appropriately stored. Regardless of whether a record is paper-based or digital, it **must** give an account of what was communicated, decided and done.

[1] AS/ISO Standard for Records Management 15489

4.2 RECORD ASSETS

4.2.1 The Directorate is committed to ensuring records in its care are treated as valuable corporate and public assets, critical to the business of the Directorate and the ACT Government.

4.2.2 All records created, received and maintained as part of the duties of staff, volunteers, consultants, contractors and outsourced providers are owned by the Directorate and the ACT Government. Records do not belong to any individual employees or contractors.

4.3 SENSITIVE RECORDS

4.3.1 The Directorate is committed and responsible for ensuring that records containing sensitive information, including those that contain personal information of citizens, provide information that would assist Aboriginal and Torres Strait Islanders to establish links with their heritage, or otherwise contain confidential information, are managed appropriately and preserved securely.

5. WHAT IS THE DIRECTORATE'S OFFICIAL RECORDKEEPING SYSTEM

5.1 The Directorate currently utilises a combination of paper files, approved business systems and the Electronic Document and Records Management System (EDRMS) known as Content Manager (CM) for official recordkeeping purposes. Where it is in place for official recordkeeping, CM **must** be used to store records rather than a paper-based system in support of a 'digital first' approach.

5.2 The Public Trustee and Guardian (PTG) also utilises the EDRMS known as Objective for select records. Staff of the PTG should refer to internal procedures for guidance on the management of records in Objective.

5.3 JACS officers are reminded that the following systems are **not** official recordkeeping systems:

- Network drives such as the G and H drive
- OneDrive
- Microsoft Teams
- Viva Engage and other social media platforms
- SharePoint
- Outlook
- Portable devices such as USB sticks

- Personal ICT devices and accounts.

5.4 Records created and held in any of the above locations **must** be moved to an official recordkeeping system as soon as possible to act as reliable evidence of business activity.

5.5 Records held on network drives pending migration to an EDRMS should be managed and structured in a way that supports their integrity and accessibility as much as possible. This includes implementing proper naming conventions and managing the lifecycle of the record in accordance with its approved Record Disposal Schedule. Only documents that can be legally destroyed under NAP should be deleted from the network drive.

6. RECORD CREATION

6.1 RESPONSIBILITIES

6.1.1 All officers are responsible for the creation of records and for determining what is required to be part of the official file.

6.1.2 The Directorate records management staff are responsible for monitoring how these records are created and liaising with officers to ensure the appropriate handling and naming conventions are used in accordance with this SOP and related information management standards and legislation.

6.2 WHAT NEEDS TO BE A RECORD

6.2.1 In accordance with the *Territory Records Act 2002* (the Act), officers are required to make and keep full and accurate records where it is required to:

- provide evidence of decisions made, advice given or received, or transactions completed
- inform ongoing decision making and business activity
- support the operation of the *Freedom of Information Act 2016* (FOI Act), which provides a general public right to access government information, and
- benefit future generations as a public asset.

6.2.2 It is the responsibility of officers to identify which documents or data needs to be considered a record and managed accordingly.

6.2.3 To determine if a document has value and should be added to an approved recordkeeping system, ask yourself the following questions:

- is it evidence of a decision you have made?
- is it evidence of advice you have given?
- is it evidence of advice you have received?

- is it evidence of a transaction undertaken on behalf of the JACS Directorate?
- does it add context to the matter at hand?

6.2.4 If the answer to any of these questions is 'yes', then it should be retained in an approved recordkeeping system.

6.2.5 In cases where decisions are made as part of a process with established procedures and criteria, the records should clearly show how the established criteria has been applied. Where a decision maker departs from the norm, the reason for doing so should be documented.

6.2.6 Documents that should not be added to an approved recordkeeping system include, but are not limited to:

- personal documents
- unofficial documents and email conversations that do not relate to your work as a public servant
- system messages (i.e. Service Desk emails) unless they are specifically required to provide context to, or evidence of, a business activity (i.e. HR21 notifications may be placed on file with timesheets to provide evidence of approved leave)
- routine or regular meeting acceptances unless there is a business need for evidence of people accepting and attending meetings.

6.3 HANDLING AND MANAGING UNREGISTERED OFFICIAL RECORDS

6.3.1 Any records that fit the description outlined in section 6.2 and are not registered in an approved recordkeeping system used by the Directorate, are still considered to be official JACS records. Unregistered official records need to be treated the same as registered official records. They are still subject to release under the FOI Act and **must** be retained and destroyed in accordance with an appropriate Record Disposal Schedule.

6.3.2 They cannot be disposed of in any way (e.g. shredded, placed in a secure bin, deleted) just because they are not registered in the recordkeeping system. Any unregistered official records identified for destruction, need to go through an official approval process as outlined in section 12 of this procedure.

7. STANDARDS

7.1 The main standards that govern and shape the way JACS creates, manages and handles its records are:

- ISO 16175 – the international standard for records in electronic office environments

- AS: 5044 - AGLS Metadata Standard
- ACT Government Standard for Records and Information Governance
- AS ISO 15489 – Standard on Records Management

7.2 To satisfy these standards, records are created and held according to the following principles:

- Complete
  - No elements of the record are redacted, removed or lacking in critical information.
- Accurate
  - The metadata that forms the record **must** be accurate, without spelling or grammatical errors. i.e. the title, dates, locations, people's names.
- Classified correctly
  - The record **must** be given proper security classifications. Refer to section 10 for guidance on how to apply the appropriate security classification.
- Trackable
  - The record **must** clearly display reference information so that when archived in an EDRMS or paper-based system, the record can be easily located.
- Appropriately stored
  - The record **must** be stored in conditions appropriate to its security classification and retention and preservation requirements.

7.3 SECURITY CLASSIFICATION SYSTEMS

7.3.1 Before a document in any format can become a record, the security classification of the potential record **must** be established. This is to ensure it is appropriately protected, either in the EDRMS or via a paper-based storage system.

7.3.2 To apply the appropriate security classification to a record, refer to the Protection of Information Standard Operating Procedure.

7.3.3 A limited number of areas within the Directorate handle classified material. Refer to section 10 for definitions and examples.

7.4 MANAGING DIGITAL RECORDS

7.4.1 As part of the Directorate's 'Digital First' approach to records management, JACS officers **must** ensure that records are created and/or recorded in an approved EDRMS (CM) or approved business system wherever possible.

7.4.2 Business units **must** also consult with Directorate records management staff when procuring new business systems to integrate a 'records by design' approach in the system design.

7.5 MANAGING PHYSICAL RECORDS

7.5.1 Paper records are to be stored in an endorsed location:

- workplaces that accommodate JACS staff and approved volunteer locations
- Territory Archives Building 7, 9 Sandford Street, Mitchell ACT
- approved secondary storage providers specialising in records, including Iron Mountain (existing consignments only), GRACE and TIMG.

7.5.2 Note that a basement is not an endorsed location until it has been assessed and approved to hold records by a suitably qualified records management professional.

7.5.3 When working from home or in a hybrid setting, records **must** be locked away in a secure cabinet or drawer when not in use. Physical records **must** not be left unattended in personal or work vehicles.

7.5.4 When deciding where to store records, officers should have due regard to both environmental and security considerations. Records held onsite **must** be stored in a container appropriate to their security classification.

7.5.5 As a general rule, physical records should not be held onsite for longer than they are required for operational or business purposes.

7.5.6 Special consideration should be given to the storage of records to be retained as Territory Archives. Such records should be kept on ACT Government premises, including storage with Territory Archives, wherever conditions permit.

8. FILE TITLING

8.1 Taking care to ensure files are titled according to the business functions and activities they represent is important to ensure the records can be easily identified and accessed for as long as they are required to be held.

8.2 Each of the components of a good file title should:

- assist in identifying the records it holds
- act as an access point for users
- distinguish it from other files
- enable searching based on keywords, phrases and numbers.

8.3 THE STRUCTURED TITLE – CLASSIFICATION

8.3.1 Official files **must** be classified using the Whole of Government Business Classification Scheme that is reflected in the Records Disposal Schedules, located on the ACT Legislation Register. The Whole of Government Business Classification Scheme is a controlled vocabulary of terms designed for classifying, titling and indexing records on creation. Proper classification of files at the time of creation helps to ensure that files are easily accessible throughout their existence and can be disposed of in an efficient manner. The classification terms form the structured title.

8.3.2 The Whole of Government Business Classification Scheme constitutes a three-level hierarchy of terms arranged by:

Thesaurus level	Description
Function	Functions are the broadest terms in the classification structure, representing the high-level functions undertaken by the ACT Government in fulfilling its responsibilities to the community. The function title will generally appear in capital letters for example FINANCE & TREASURY MANAGEMENT.
Activity	Activities are used to describe the narrower processes or operations performed by government in undertaking a broad function for example Accounting.
Subject/Free Text	Subjects are non-mandatory terms used to more narrowly define the content of an activity, for example, credit cards.

8.4 FREE TEXT NAMING CONVENTIONS

8.4.1 Free text is the non-controlled element of the file title. Free text should always be meaningful and descriptive, including sufficient information to differentiate it from other records.

8.4.2 When titling a file, staff should:

- consider how other people would search for the topic, both now and in the future
- include date ranges or specific dates to differentiate it from similar files
- avoid using acronyms or abbreviations unless commonly used such as ‘ACT’
- avoid nondescript words such as ‘general’, ‘miscellaneous’, or ‘matters’.

8.4.3 Date ranges are important in file titles to ensure records are not added to a file in perpetuity.

8.4.4 Date ranges can be for a calendar year, financial year or cover multiple calendar or financial years. Their application to a file will tell JACS officers how long the file will be used for until it is deemed to be closed and made inactive.

8.4.5 They will also assist JACS officers with locating information where a timeframe is important and useful to differentiate one record from another.

8.4.6 A full title may therefore be comprised as follows:

Function	Activity	Subject/ Description/ Free text
Finance & Treasury Management	Accounting	Credit Cards - Executive Acquittals – 2025- 2026
Human Resources	Remuneration	Governance Unit Flex Sheets June 2026

9. HANDLING DIFFERENT TYPES OF RECORDS

9.1 EMAIL

9.1.1 If an email provides evidence of a decision, actions taken or advice given, it **must** be treated as an official record and filed appropriately in the recordkeeping system.

9.1.2 In order to maintain their value as evidence, emails cannot be altered or manipulated for as long as they are retained.

9.1.3 Officers **must** manage their work email accounts to ensure information is appropriately stored, noting that Outlook is not an official recordkeeping system. Emails need to be saved to the EDRMS to ensure business continuity, as emails in Outlook may not be accessible to teams or other business areas and cannot be adequately controlled (i.e. with full audit trail and restricted deletion).

9.1.4 As a general rule of internal communication, the initiator of an email is also responsible for capturing it as a record. The recipient should also use their judgement as to whether they will require a copy of the email on their file to maintain the broader context of a particular matter.

9.1.5 Emails received from an external source should be filed immediately by the internal recipient.

9.1.6 Forwards and replies should also be treated as part of the record and will need to be captured on file. Ideally the email chain should be captured on the official file once, reflecting the entirety of the conversation in full. The title of the email should convey what it is about, and any decision or actions taken.

9.2 WORKING PAPERS

9.2.1 The documents created and received in reaching a final position may constitute a record where they explain and justify the decision-making process. This includes

significant drafts of a document that was subsequently finalised, particularly where it demonstrates a change in policy or recommended outcomes. Minor drafts, incorporating grammatical or stylistic changes, may not be as valuable and may not always need to be kept as a record.

9.3 SOCIAL MEDIA

9.3.1 If information being received or communicated via social media provides evidence of a decision, actions taken or advice given, it **must** be captured and managed appropriately. This may include saving a screenshot of the post and reply comments within the social media feed to the official recordkeeping system.

9.4 WEBSITES

9.4.1 Records of website-based activity **must** be kept as evidence, including website content, records of any online transactions and documents reporting the administration of the website.

9.4.2 The documents that comprise a webpage can be captured in their native format. Static websites can be captured by periodic snapshots and should be filed accordingly.

9.4.3 Websites which are updated regularly and need to be part of the official record, should be archived after each update. The website administrator **must** decide whether the record focuses on the individual transactions between clients and servicers or the objects that comprise the content of the website at any given time.

9.4.4 Regardless of the kind of website, website records **must** fulfil the standards of record creation like any other kind of record format.

9.5 NON-WRITTEN COMMUNICATIONS

9.5.1 Much of the work undertaken during the normal course of business will automatically result in the creation of a document that can be used to form the official record. Sometimes however, business activities may not in themselves generate a document, such as a phone conversation, and officers **must** decide whether a record needs to be made for accountability purposes. Verbal decisions, transactions or commitments should be documented to form part of the record (i.e., by way of a file note or email summarising a discussion).

10. RECORDS MANAGEMENT AND PRESERVATION

10.1 RESPONSIBILITY

10.1.1 The management and preservation of records is the responsibility of any JACS officer who is in possession of a physical or digital record.

10.1.2 This covers when the record is:

- filed
- accessed
- being used as a working document; and
- returned for storage (if physical) or checked-in or closed (if digital).

10.1.3 The record should be considered an asset of the Directorate and the ACT Government and as such, should be handled with preservation in mind to allow for continued access and use now and into the future.

10.2 INFORMATION SECURITY

10.2.1 The Directorate's record and information holdings form part of a valuable asset that warrants protection. The ACT Government Protective Security Framework and associated Information Security (INFOSEC) guidelines require staff to implement risk-based security measures to protect information from accidental or unauthorised loss, release or damage. All records and information should be classified and marked on creation in accordance with the INFOSEC guidelines and handled accordingly.

10.2.2 Officers **must** refer to the Protection of Information Standard Operating Procedures to ensure information is held, shared and moved in accordance with applicable security requirements.

10.2.3 Information should be shared with others where there is a 'need to know' and the disclosure complies with any applicable legislation. As an asset, records and information should be used to support business, operational and strategic outcomes where there is a legitimate right and need to access it. Browsing information out of curiosity is strictly prohibited and may be subject to disciplinary action.

10.2.4 Officers should also be conscious of any additional handling provisions that may apply to specific types of information, such as personal information under the JACS Privacy Policy.

10.2.5 Storage of information should be consistent with the guidelines within the Protection of Information Standard Operating Procedure. These standards are:

Protective Marking	Minimum Storage Requirement
Official Official: Sensitive Official: Sensitive - Personal Privacy	• In accordance with the *Territory Records Act 2002*. • Computers/laptops logged off at the end of the day or when left unattended

Protective Marking	Minimum Storage Requirement
Official: Sensitive- Legal Privilege Official: Sensitive - Legislative Secrecy	• Locked desk draw. • Locked in filing cabinets or secured in locked offices.

Cabinet	• In accordance with the ACT Government Cabinet Handbook:
	  ○ Locked in filing cabinets or secured in locked offices.
	  ○ Data storage devices in locked cabinets or secure containers.

Protected	• Class B storage containers in secure Offices. • Data storage devices in Class B storage containers. • Laptops secured in Zone 3 Areas.
Secret	• Class B storage containers in secure Offices. • Data storage devices in Class B storage containers. • Laptops secured in Zone 4 Areas.

10.2.6 In the event of a suspected or known data breach resulting in the unauthorised disclosure or loss of Directorate information, relevant officers **must** immediately enact the JACS Data Breach Standard Operating Procedure to contain, assess and respond to the breach in a timely manner.

10.3 MOVING PHYSICAL RECORDS TO SECONDARY STORAGE

10.3.1 Territory Archives is the primary secondary storage provider for the JACS Directorate. Territory Archives also manage contracts with other third-party storage providers on behalf of the Directorate.

10.3.2 JACS officers are required to identify what physical records need to go to storage and arrange for those records to be collected by Territory Archives. JACS officers will need to separate the physical information into two key piles – registered and unregistered. Territory Archives have forms on their website specifically for registered and unregistered information. These forms assist Territory Archives to effectively manage information and ensure it remains accessible and retrievable when in storage.

10.3.3 Registered files are records that have been registered in the Territory Archives dataset and have an official record number assigned to them. Unregistered information is typically found in the form of notebooks, information stored in D-ring folders or spiral bound books. This information has not been assigned an official record number because it has not been registered with Territory Archives.

10.3.4 Any records identified as being ready for destruction, **must** be set aside and processed in accordance with the instructions at section 12 below.

10.3.5 Business areas **must** send the consignment forms through to the GCR Team for review before submitting a collection request with Territory Archives, to ensure appropriate retention schedules have been assigned to the records.

10.3.6 Records that are moved to secondary storage remain the property of the business unit. Business units can still request the retrieval of the records through Territory Archives, and they can specify how soon they need that information to be delivered by. The business unit also retains responsibility for approving disposal when appropriate.

10.4 CLOSING DIGITAL FILES AND MARKING THEM INACTIVE

10.4.1 Closing a digital file in the EDRMS and making it inactive, is the equivalent of closing a physical file and sending it to storage. Both files are still accessible, however no new information can be added to them.

10.4.2 JACS records management staff conduct regular reviews of digital files that have been inactive[2] for 12 months or longer, and will liaise with business areas to confirm that identified files can be closed and made inactive.

10.4.3 Closing files and making them inactive ensures the records in the file are protected from any intentional or unintentional tampering or changes. It also ensures the file and records move onto the next stage of their lifecycle, as outlined in the Records and Information Management Policy. If the file is identified as temporary, making the file inactive will initiate the count-down to its destruction date.

10.4.4 Closed and inactive files will remain in the EDRMS and be available for JACS officers to search for and view. When the temporary records have reached their minimum retention period, JACS records management staff will commence the destruction process as outlined in Section 12 of this SOP.

10.5 RECORD PRESERVATION STRATEGY

PHYSICAL RECORDS

10.5.1 Records **must** be preserved to ensure they can be accessed for as long as they are required for business use and by law. To preserve paper records of enduring or permanent value, officers **must**:

- treat the record with care
- implement adequate storage standards and handling practices (see section 10)

[2] A file is considered to be inactive when no new records have been saved to the file or the existing information has not been edited.

- use archival quality material at creation.

DIGITAL RECORDS

10.5.2 Preservation of electronic records requires strategies to migrate records to new systems in a way that maintains its reliability and authenticity as evidence.

10.5.3 Records that have deteriorated over time or suffered damage may require specific conservation treatment by experts. Advice on suitable treatments and the availability of experts is available through JACS records management staff.

10.6 BUSINESS CONTINUITY AND DISASTER RECOVERY

10.6.1 Business continuity and disaster recovery planning **must** include strategies for the protection and recovery of records. In particular, business units **must** ensure all necessary measures are in place to protect vital information. Vital information assets are any records or information that would be considered essential to re-establishing critical business operations in the event of a major disruption. Vital information assets should be identified during the business continuity planning processes, with strategies to minimise the risk of their loss. This may include:

- duplication and dispersal
- use of secure, fireproof, waterproof and vermin proof storage facilities
- remote storage and back up.

11. RECORD ACCESS

11.1 The Access Principle of the ACT Government Records and Information Governance Standard means that the JACS Directorate **must** support principles of open government and begin from a position of openness in relation to access to ACT Government records and information.

11.2 JACS officers **must** manage their records and information in a way that supports openness, ensuring they remain accessible for as long as they are required to meet accountability, legislative and business requirements and community expectations.

11.3 LOCATING PHYSICAL RECORDS

11.3.1 Officers can contact JACSGCR@act.gov.au or Territory Archives to locate or ascertain the existence of any official physical files for the purposes of providing access.

11.4 PUBLIC ACCESS

11.4.1 The Directorate is committed to facilitating the public's right to access government information under the *Freedom of Information Act 2016* and the *Territory Records Act 2002*.

11.4.2 The TR Act provides the public a statutory right to access Territory records that are more than 20 years old, with Cabinet records generally being available after 10 years. ArchivesACT assists the Directorate to process public access requests under the TR Act.

11.5 SECTION 28 REGISTER

11.5.1 The Director of Territory Records may declare a record exempt from public release under the TR Act where disclosure could reasonably be expected to:

- endanger the life or physical safety of a person
- prejudice law enforcement
- unreasonably disclose information about any person (including a deceased person)
- be a contempt of court or the Legislative Assembly, or
- the record is subject to legal professional privilege.

11.5.2 In line with sections 28 and 30 of the TR Act, the Directorate is required to keep a register of its records subject to an approved and in force declaration under section 28 (declaration applying provisions of the FOI Act). To confirm whether a JACS record is covered by a section 28 notice or to seek a new declaration, please contact JACS records management staff via JACSGCR@act.gov.au.

12. RECORD DISPOSAL

12.1 RESPONSIBILITY

12.1.1 All JACS officers are responsible for identifying and classifying their records so that they can be managed across their lifespan, including the eventual disposal of some records.

12.1.2 The classification of records is part of the file creation process. Further details on how to apply classification principles can be found in Section 8 above and the JACS Records Management intranet page.

12.1.3 The responsibility of record disposal is shared between all JACS officers and records management staff. All record disposals **must** be cleared through JACS records management staff and the TRO before disposal occurs.

12.2 RECORD DISPOSAL SCHEDULES

12.2.1 A records disposal schedule is a legal instrument issued by the Director of Territory Records that authorises the disposal of ACT Government records. It provides a systematic listing of classes of records and the minimum length of time they **must** be kept. A list of record disposal schedules relevant to JACS can be found here.

12.2.2 Once a record has reached the minimum retention period listed in the authorised disposal schedule and is no longer required for business or accountability purposes or to meet the expectations of the community, it may be legally disposed after following the processes outlined below. Alternatively, some record classes will be identified as 'retain as Territory records' (RTA), meaning associated records **must** be kept indefinitely. Records that are to be retained as Territory archives generally contain information that:

- Provides concise evidence of the deliberations of the Territory and Territory institutions, relating to key functions and programs, and significant issues faced in governing the Territory such as the development and review of legislation.
- Is considered essential to the protection and future wellbeing of Australians and their environment, including protection of their significant rights and entitlements.
- Have a special capacity to illustrate the impact of government activities on individuals, groups and the environment such as major public works.
- Have substantial capacity to enhance the knowledge and understanding of the Territory's history, society, economy, culture and people.
- Provide evidence of the source of authority, foundation and machinery of government and Territory institutions sufficient to document the administrative and legal context of other Territory archives.

12.2.3 Physical records that are to be retained as Territory archives may be transferred to Territory Archives for storage if there is no business need to access it on a regular basis. See section 10 for further guidance on this process.

12.3 NORMAL ADMINISTRATIVE PRACTICE (NAP)

12.3.1 NAP is the common practice of the destruction of temporary or duplicate documents which do not hold significant or continuing value and are not part of the official record.

12.3.2 Material that can be destroyed using NAP includes:

- Rough notes, calculations and diagrams that were used for the preparation of a record.
- Copies of documents where the original is safely retained in the official recordkeeping system – ensure this is the case before destroying the copy.
- Minor or inconsequential drafts. Note: Major drafts in which there is a change to the requirements of a policy or recommendations **must** be retained.

- Modifications and updating of data as part of running established electronic software programs, where such processes do not result in the loss of data of continuing value.

- Published material used only as a reference including pamphlets, leaflets and brochures.

- Information from other organisations that is not essential to the Directorate's functions and does not need to be kept as evidence of a JACS business activity.

- Personal documents such as unofficial emails and resumes.

12.4 NAP DISPOSAL PROCEDURE

12.4.1 There is a simple two step check to ensure NAP can be used for the disposal of a document:

1. Does a Record Disposal Schedule class apply to the document?

2. Does the document hold continuing value and is it the original/only copy available to JACS officers?

12.4.2 If the answer to either/both of the above questions is 'yes', the document is an official record and cannot be disposed of using NAP.

12.4.3 If you answered 'no' to the above questions, then the document may be disposed of using NAP.

DESTRUCTION OF PHYSICAL INFORMATION UNDER NAP

12.4.4 Physical documents subject to NAP **must** be destroyed in accordance with their security classification (i.e. via a secure waste bin).

12.4.5 Empty file covers that were ordered from Territory Archives **must** be returned to Territory Archives with a note advising that they were never used – i.e. no additional papers were placed on the file. This will enable Territory Archives to update their systems and dispose of the file covers.

DESTRUCTION OF ELECTRONIC INFORMATION UNDER NAP

12.4.6 To request information stored in the EDRMS be destroyed under NAP, the creator **must** first move the document to the 'delete file' for their business area.

12.4.7 It is the responsibility of the JACS officer to ensure the document is not sitting alternatively within other files, folders and containers. Once the document has been deleted from the delete folder, it is deleted from all other locations.

12.4.8 The record title should be updated to reference the reason why the item is to be destroyed under NAP (i.e. 'created in error').

12.4.9 Directorate records management staff will raise a ticket with the Digital Records Support Team to request the destruction of digital information under NAP. The records management staff member raising the ticket **must** state that all quality checks have been conducted and confirm that the information fits within the scope of NAP.

12.4.10 For information on the disposal of large volumes of softcopy information outside of the EDRMS or ICT equipment, please contact the Directorate Agency Security Advisor.

12.5 RECORDS DISPOSAL PROCEDURE

12.5.1 As stated above, official JACS records may only be destroyed in accordance with an approved Records Disposal Schedule.

12.5.2 Sentencing is the process of identifying and classifying records according to an approved Disposal Schedule and applying the applicable retention period. Sentencing should take into consideration business needs, requirements for agency accountability and community expectations.

12.5.3 JACS files are generally sentenced upon creation through the application of the Whole of Government naming conventions applied in the EDRMS or paper file creation process.

12.5.4 The retention period identified in the Disposal Schedule represents the minimum timeframe records should be retained and can be extended if the business area believes the records remain of value to the ACT Government and community.

12.5.5 Approval from an Executive Branch Manager or above for the disposal of official records **must** be to be sent through to JACSGCR@act.gov.au before any items are destroyed so that disposal decisions can be verified.

12.5.6 JACS records management staff will review the request and, if appropriate, forward it to the TRO for authority to destroy the records.

12.5.7 The business area will be contacted once the authority to destroy the records has been obtained or advised of an extended retention period if this is deemed appropriate.

12.5.8 Physical records **must** be securely destroyed in accordance with their security classification. Physical destruction can also be arranged through Territory Archives.

12.5.9 The Directorate records management staff will arrange the destruction of digital records in the EDRMS.

12.5.10 The Directorate records management staff will conduct regular disposal reviews of physical and digital records created by JACS. Approval will be sought for the destruction of any records that have exceeded their minimum retention period from the relevant Executive Branch Manager. It is the responsibility of the

business unit to respond in a timely manner to these requests and identify reasons why the records should not be destroyed where applicable.

12.6 CLOSING DIGITAL FILES AND DOCUMENTS

12.6.1 The Protect Principle of the JACS Records and Information Management Policy, requires JACS to secure, store and preserve information, records and data to protect the interests of the organisation and the rights of current and future internal and external stakeholders.

12.6.2 Closing and making a file inactive means that JACS is taking the necessary steps to protect our records and information from misuse, interference, loss and unauthorised access, modification and disclosure.

12.6.3 It also enables JACS to effectively manage the legal destruction of digital information that is no longer required to be kept.

12.6.4 JACS EDRMS users are encouraged to finalise documents in active files that are identified as being a final and true version (i.e. the approved document). This ensures the documents are protected from alteration and manipulation. The documents remain available for JACS EDRMS users to access and read.

12.6.5 Records that have been identified as Territory archives, will continue to be managed by JACS in perpetuity.

12.7 PRESERVATION OF RECORDS ESTABLISHING ABORIGINAL AND TORRES STRAIT ISLANDER HERITAGE

12.7.1 In accordance with the TR Act, the JACS Directorate seeks to ensure that there are arrangements in place for preserving records that contain information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

12.7.2 Any records that contain name and family information that could be used by people to establish links with their Aboriginal or Torres Strait Islander heritage **must** be preserved indefinitely in accordance with the *Territory Records (Records Disposal Schedule - For preserving records containing information that may allow people to establish links with their Aboriginal and Torres Strait Islander heritage) Approval 2011 (No 1)*. This requirement should be interpreted broadly based on the significance criteria identified under the Assess principle and may include, for example, records that detail cases of significant government intervention in the lives of Aboriginal and Torres Strait Islander children who were separated from their families.

12.7.3 Business units have implemented arrangements for the protection of relevant records. If there is any doubt as to whether the records could contain useful information, please contact JACS records management staff for advice.

12.8 RECORDS DISPOSAL FREEZES

12.8.1 The Directorate seeks to ensure that there are arrangements in place to protect records that are required for government inquiries. All record disposal requests will be reviewed by JACS records management staff to ensure they comply any relevant freezes as notified by the Director of Territory Records, including:

- *Territory Records (Records Disposal Schedule - Protection of Records Relevant to Cornwell-type Superannuation Claims) Approval 2016 (No 1)*
- *Territory Records (Records Disposal Schedule - Protection of records relevant to the Royal Commission into Institutional Responses to Child Sexual Abuse) Approval 2022 (No 1)*

13. ENQUIRIES

Enquiries regarding this SOP or for further information on records management in the Directorate, contact:

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

DETAILS

Document Properties	Approval Details
Document Name:	Records and Information Management Standard Operating Procedure
Document Number:	0079-2
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* *Evidence Act 2011* *Financial Management Act 1996* *Health Records (Privacy and Access) Act 1997* *Human Rights Act 2004* *Work Health and Safety Act 2011* *Working with Vulnerable People (Background Checking) Act 2011* Digital Recordkeeping Policy for the ACTPS *ACT Government Data Governance and Management Policy Framework and Guide* *JACS Privacy Policy* *JACS Data Beach Standard Operating Procedure* *JACS Freedom of Information Policy* JACS Open Access Policy JACS Protection of Information Standard Operating Procedure

AMENDMENT HISTORY

Version	Issue Date	Amendment Details	Author	Approved by
1.0	27 June 2018	New version of Records Management Standard Operating Procedure	JACS Records Manager	Director-General
1.1	January 2021	Reviewed	JACS SRO	Director-General
1.2	16 December 2021	Transfer to the new SOP template	JACS SRO	EBM, GBI
1.3	23 September 2022	Information reviewed and updated following consultation with stakeholders	JACS SRO	Director-General
1.4	28 August 2025	Administrative Update	JACS SRO	EBM, GBI