ACT Government
Community Services

RECORDS, INFORMATION AND DATA PROCEDURES

Records Management Program

JUNE 2018

ACT GOVERNMENT
GPO BOX 158 Canberra City

CONTENTS

1 OVERVIEW: RECORDS, INFORMATION AND DATA MANAGEMENT PROCEDURES

Title:	Records, Information and Data Management Procedures
Publication date:	2018
Document location:	www.communityservices.act.gov.au

1.1 Purpose

All staff are responsible for the creation and management of records, information and data, and these procedures will assist staff to meet their responsibilities.

These records management procedures form part of the Directorate's records management framework. They are designed to complement the Records, Information and Data Management Policy.

These procedures aim (in conjunction with the Records, Information and Data Management Policy) to promote consistent and coherent processes and practices, and form part of the Directorate's normal administrative practices. These procedures are also strategically linked to ACT Government's Standard for Records, Information and Data and associated Guidelines.

The Records Manager and/or Records Management Unit are responsible for coordinating the development and promulgation of these procedures.

1.2 Scope

The procedures are designed to provide directions for records, information and data management for a range of processes undertaken by all full-time and part-time staff, volunteers, consultants, contractors and outsourced providers as part of their duties.

Some procedures are solely carried out by the Records Manager and/or Records Management Unit while others are carried out by all business areas.

1.3 Responsibilities

The Director-General as Principal Officer, is ultimately responsible for the management of records, information and data, and has authorised the Records Management Program and the Records, Information and Data Management Policy under which these procedures have been developed.

The Chief Information Officer is responsible for the active support of, and adherence to, the Records Management Program, the Records, Information and Data Management Policy, and the Records, Information and Data Management Procedures.

1.4 Implementation

All managers and supervisors have a responsibility to foster an environment that promotes good records, information and data management. Effective implementation requires managers and supervisors to monitor their full-time and part-time staff, volunteers, consultants, contractors and outsourced providers to ensure they understand and apply relevant records, information and data management procedures.

1.5 Review date

These procedures are subject to regular updating by the Records Manager and/or Records Management Unit.

At a minimum, these procedures will be reviewed and updated at least every five years or as required (such as after significant administrative change).

1.6 Further Help

For further information or assistance concerning recordkeeping practices contact the Records Manager / Records Management Unit via email CSDRMU@act.gov.au

1.7 References

Directorate Policies and Standards

- *The Directorate's Recordkeeping Policy*
- *Directorate's Information Management Policy*
- *The Directorate's Data Entry Standards*
- *Directorate's Records Management Unit Operations Manual*
- *Directorate's Record Retention and Disposal Manual*
- *The Directorate's Injury Prevention Health and Safety Policies*
- *Directorate's Record Advice Sheet 3 – Rules in regard to the Destruction of Records*
- *Directorate's Workplace Health and Safety Policy Statement*

Legislation (ACT and Cwlth)

- *Children and Youth People Act 2008*
- *Freedom of Information Act 2016*
- *Information Privacy Act 2014*
- *Health Records (Privacy and Access) Act 1997*
- *Territory Records Act 2002*
- *Aboriginal and Torres Strait Islander Heritage Protection Act 1984 (Cwlth)*
- *Work Health and Safety Act 2011*

Best Practice Standards Policies and Advice

- *Territory Records Office Standard for Records, Information and Data*
- *Records Disposal Schedule for Source Records - NI2011-170*
- *Records Disposal Schedule - Preserving records containing information that may allow people to establish links with their Aboriginal and Torres Strait Islander heritage*
- *Australian Standard: AS5044—AGLS Metadata Standard*
- *Australian Standard AS5478—Recordkeeping Metadata Property Reference Set*
- *International Standard: ISO15489—Records Management part 1*
- *International Standard: ISO15489—Records Management part 2*
- *International Standard: ISO26122—Work Process Analysis for Recordkeeping*
- *International Standard: 13028:2010 (E) Information and documentation – Implementation guidelines for digitising of records*
- *International Standard: ISO16175—Requirements for Records in Electronic Systems*
- *ACT Public Sector Work Safety and Injury Management Policies*
- *ACT Government Metadata for Web-based Resources Policy*
- *Territory Records Office Records Advice No. 03: Email as a record*

- *Territory Records Office's Records Advice Number 32 - Utilising a Records Disposal Schedule.*
- *Territory Records Office Advice Sheet number 42 - Sentencing legacy records.*

2 - STRATEGY PRINCIPLE

2.1: Administrative Change Procedure

2.1.1 Purpose

The purpose of this procedure is to ensure that machinery of government changes are reflected in respective recordkeeping systems and that any records (physical or digital) are also moved to the agency that has acquired the records as a result of administrative change.

2.1.2 Scope

The procedure applies to all records and files.

2.1.3 Responsibilities

The procedure applies to the Records Manager / Records Management staff.

2.1.4 Background

When machinery of government changes occur, records (physical and digital) relevant to that function must be transferred to the organisation now responsible for that function.

From a recordkeeping perspective, recordkeeping systems must be updated to reflect the machinery of government changes. The Administrative Arrangements are updated each time a function is given or taken away from a Directorate, and so a watch must be kept on the Notifiable Instruments on the Legislation Register.

The Administrative Arrangements are found on the ACT Parliamentary Counsel's website.

2.1.5 Operational Instructions

Losing a function: Identify the records to be transferred

All records (physical and digital) relating to the function being transferred should be transferred to the gaining organisation. In the case of physical records, control records (metadata) need to be identified and copies of these records supplied along with the physical records to the gaining agency. In the case of digital records, it will involve a digital copy and metadata being supplied and uploaded to the gaining agency's recordkeeping system.

Once both agencies have an understanding of the scope of the records to be transferred, the Records Manager is to:

- generated a report from the recordkeeping system listing each individual record being transferred;
- Update the metadata in the recordkeeping system to indicate the records are transferred to the gaining agency; and
- Alert the gaining agency to the record disposal schedules on the Territory Records Office website.

Transfer the records

- Make arrangements for the official transfer of the records to the gaining agency. This may also include, in the case of digital records, supplying a copy of digital records as well as metadata in a format suitable to the gaining agency. This may include discussions with Shared Services ICT Digital Recordkeeping team for assistance;
- Line area staff must not forward physical files outside their building without first consulting the Records Manager;
- All classified (sensitive) physical files are to be prepared for transmission in accordance with the *ACT Government Protective Security Policy Framework* and sent through in a safe manner. Staff receiving classified (including sensitive) files must sign and return to the sender an appropriate receipt of received material.

Gaining a function:

The Records Manager is to determine the internal plan for receiving records. This includes

- Plan for the receipt of records (physical and digital), control records (including metadata) and record disposal schedules;
- Arrange for the transfer of immediate use of physical records;
- Ensure the records are clearly labelled. Store active records close to the relevant work area or in the current records repository. Store infrequently used records offsite. If they remain in the same physical location and only ownership changes, ensure any evidence involved in the outsourced arrangement is obtained;
- Digital records will require discussions and assistance from Shared Services ICT Digital Recordkeeping team to upload records.
- Conduct a census of physical records to ensure the process is complete.

Maintain records received in their original form

Wherever possible, so as not to lose contextual information about transferred records, it is vital that the receiving agency ensures the recordkeeping systems differentiate between received and native records. Transferred records should not be:

- Re-titled or re-numbered (also known as “Top-Numbering”), or
- Re-arrange the order of the received records.

Seek information from the transferring agency regarding stored records

It is essential the receiving agency obtains information from the transferring agency concerning physical records in storage that may be relevant to the business of the receiving agency. Negotiate which records are required to complement the current records being received. Access to records in storage needs to be determined, including costs.

Update the control records

Update the control records (metadata) to indicate:

- The records received from the transferring agency;
- The date of the transfer;
- The name and contact details of the transferring agency; and

- Place a copy of the signed acknowledgement of transfer into the recordkeeping system.

This may include updating / uploading digital records and metadata to gaining agency's recordkeeping system and discussion should include Shared Services ICT recordkeeping team.

Conduct a file census

A file census of physical records is to be arranged by Records Manager to ensure the process is complete.

2.2: Work Health & Safety (WH&S) in Records Management Procedure

2.2.1 Purpose

The purpose of this procedure is to ensure a safe working environment for Records Management staff as well as any people physically handling records do so safely.

2.2.2 Scope

This procedure is to highlight and eliminate risks to health and safety, so far as is reasonably practicable.

2.2.3 Responsibilities

This procedure applies to all Records Management staff, contractors and consultants involved with records management activities.

2.2.4 Background

The Directorate is committed to providing a safe and healthy work environment for employees, contractors, consultants and visitors at all Directorate workplaces in accordance with the *Work Health and Safety Act 2011* and other relevant legislation.

2.2.5 Operational Instructions

Storage

Records storage areas are to be kept clean to reduce the dust build up. There is to be no eating or drinking in record storage areas. Proper lighting and ventilation is to be provided that is consistent with work place health and safety standards as well as Territory Records Office Standard and Guidelines regarding the storage of records. All records are to be housed in proper containers and stored on appropriate shelving in secured areas or cabinets. The Records Manager is to liaise with offsite storage providers to ensure pest control programs are regularly undertaken.

Manual handling

Manual handling means more than just lifting or carrying something. The term 'manual handling' is used to describe a range of activities including lifting, lowering, pushing, pulling, carrying, moving, holding or restraining something. Before manually handling items, staff are reminded to ensure that they have identified any potential hazards that may arise.

Staff should always consider:

- What you are handling – size, weight and composition; including not lifting more than 16kg individually at any time;
- Where you are moving the item to – make sure the route is free of hazards, e.g. obstructions;
- The workplace and workstation layout;
- The actions, movements, working posture and position required to move the items;
- Seeking assistance if required – do not lift items that may be too heavy or too awkward; and
- The use of appropriate ladders, lifting and carrying devices.

Rest breaks and general work space set up including:

- A staff member must not work more than 5 hours without a half hour break;
- It is recommended that staff work space be assessed between 3-6 months;
- A foot rest is recommended to increase circulation and prevent cramp; and
- Your knees should be at least one hand width length from the edge of the chair and no more than 2 hand widths to prevent back strain.

Underpinning the ACTPS policies are numerous Directorate directions and procedures which detail specific roles and responsibilities to assist workers in carrying out their duties in a safe manner. The Work Health and Safety Policies include, but are not limited to:

- Accident/Incident reporting;
- First aid in the workplace;
- Work Health and Safety Inspections; and
- Electrical safety management.

Ergonomic Environment and Correct Posture

There are a number of ways staff can stop back and neck pain, these include:

- Get your environment right - Most staff spend many hours in front of a computer on a daily basis. As a result of incorrect positioning the possibility of Musculoskeletal injuries increase.
- Get moving - Any activity that gets you moving can increase your flexibility and strength.
- Get walking - Parking further away from shops and public transport, or taking a walk at lunchtime are quick, easy ways to increase activity in your day.
- Get stronger - Building postural endurance specific to your daily activity demands is a priority.
- Breaking up sitting time - Simply by standing regularly for brief periods, can have significant health benefits. It is thought that standing every 20 minutes for 1-2 minutes is enough to be of benefit.

2.3: Resourcing the Records Management Program Procedure

2.3.1 Purpose

The purpose of this procedure is to outline the appropriate resources for the management of the Directorate's Records Management Program.

2.3.2 Scope

This procedure relates to the provision of resources and outlines responsibilities for the Records Management Program.

2.3.3 Responsibilities

The Director-General, as Principal Officer, has overall responsibility for approving resources, supporting and ensuring a successful Records Management Program. The Records Manager and Records Management staff are responsible for implementing the Program.

2.3.4 Background

The Directorate is committed to providing appropriate resources to achieve a successful Records Management Program, in accordance with the *Territory Records Act 2002* and in line with Directorate's Strategic Plan 2016 / 17 – *connecting to whole of government priorities and initiatives.*

2.3.5 Operational Instructions

Financial resources:

- Expenses for the operation of the Records Management Program will be met from the Directorate normal budgetary arrangements;
- Where appropriate, the Directorate has a Service Level Agreement with Shared Services Record Services for the provision of records management and mail services;
- The Directorate has in place appropriate storage provisions including the storage of records offsite; and
- Salaries are financed by the Directorate's corporate services function.

Human resources

- The Directorate's Records Management Program is appropriately resourced for the effective and efficient management and control of the organisation's records;
- The duty statements and position profiles of staff responsible for records management are reflective of contemporary recordkeeping practices and processes; and
- All staff, including contractors and consultants are made aware of their responsibility for maintaining records and the making and keeping of full and accurate records of the Directorate's activities is mandatory.

A. Principle Officer

The Director-General as the Principal Officer has statutory responsibilities under the Act for ensuring that the Records Management Program is created, approved, implemented and adhered too.

B. Records Manager

The Records Manager has overall day-to-day responsibilities for the Directorate's records management including the responsibility for ensuring compliance with the Directorate's Records Management Program including:

- Strategic planning for records management activities, including resourcing;
- Assigning records management tasks to identified positions;
- Incorporating recordkeeping principles into all business processes;
- Obtaining expert advice where required on records management issues and practices;
- Meeting all reporting requirements;
- Arranging appropriate resources allocation to enable the program to be established and maintained, in accordance with the Director-Generals' commitments; and
- Monitoring that staff charged with specific records management responsibilities are appropriately trained and managed for the task.

C. Records Management staff

The Directorate's Records Manager is responsible for identifying staff with records management responsibilities and ensuring appropriate duties are outlined in positions descriptions. These duties include:

- Designing, developing and maintaining recordkeeping systems including the developing and maintenance of functions-based thesaurus;
- Providing advice regarding applying thesaurus terms from the Whole of Government Thesaurus to records to ensure consistent classification, titling and indexing;
- Maintaining control and consistency with the creation of records (whether paper files or digital records);
- Managing the control; storage and retrieval of records from storage providers;
- Providing training in recordkeeping principles and practices;
- Facilitating public access to records in cooperation with the Directorate's FOI officers;
- Where appropriate, appraising and developing the functional Whole of Government Records Disposal Schedules; and
- Sentencing and disposal of records in accordance with Whole of Government Records Disposal Schedules.

D. All staff

Good recordkeeping is practiced by staff including contractors and consultants as a normal part of everyday business processes. Staff, contractors and consultants can fulfil their recordkeeping responsibilities by adhering to the Directorate's Policy and Procedures for recordkeeping. In particular, staff have a responsibility to:

- Adhere to the Directorate's Records Management Policy and Procedures;
- Make full and accurate records as evidence of their business activities;
- Identify, classify and capture records including electronic records into official recordkeeping system/s;
- Foster and promote good recordkeeping practices; and
- Protect records in their care.

E. Managers and supervisors

Managers and supervisors at all levels are responsible for encouraging staff under their direction to meet all the requirements of the *Territory Records Act 2002*. This is achieved by complying with the Directorate's Policy and Procedures for recordkeeping. It is the responsibility of every business manager to support recordkeeping practices and processes of their staff by:

- Ensuring their staff undertake introductory recordkeeping training;
- Facilitating their staff access to tools, procedures and expertise to help them carry out their recordkeeping responsibilities;
- Encouraging compliance with the Directorate's Records Management Program within their area/s of responsibility;
- Having detailed knowledge of business recordkeeping requirements in areas for which they are responsible;
- Knowing the records management procedures in sufficient detail to be able to meet their responsibility;
- Being familiar with the principles of records management;
- Ensuring that full and accurate records are made as evidence of business activity and are captured into official recordkeeping system/s;
- Providing guidance and on the job training in good records management practices;
- Ensuring that staff have an understanding of best practice recordkeeping standards and guidelines; and
- Monitoring to ensure records management procedures are implemented.

F. Human Resource managers

The Directorate's induction and general training programs include basic records management principles, processes and practices and the need to comply with the Directorate's Recordkeeping Policy and Procedures.

G. Webmaster & Intranet manager

It is essential that web-based records, whether provided in-house or outsourced, are identified and maintained in accordance with the Directorate's Recordkeeping Policy and Procedures. As such, webmasters are responsible for monitoring compliance. The document owners are responsible for version control on the Internet and the Intranet.

H. System administrators

System administrators are responsible for maintaining the Directorate's digital recordkeeping systems including maintaining the integrity and authenticity of digital records and their associated metadata.

2.4: Liaising with Director of Territory Records and Dispute Resolution Procedure

2.4.1 Purpose

The purpose of this procedure is to set out a mechanism to liaise with the Director of Territory Records as well as establish dispute resolution processes concerning the Directorate's compliance with its Records Management Program and the *Territory Records Act 2002*.

2.4.2 Scope

The procedure sets to establish open communication with Director of Territory Records for the purposes of liaising, providing and obtaining advice, auditing, monitoring and reporting on any aspect of the Directorate's Records Management Program. The procedure also establishes mechanisms for resolving any disputes with the Territory Records Office.

2.4.3 Responsibilities

The procedure applies to Records Manager, Records Management and Directorate staff, consultants and contractors.

2.4.4 Background

The Director of Territory Records plays a key role in administering the *Territory Records Act 2002*; publishes and provides advice on issues standards and guidelines; authorises records disposal schedules; and is permitted to audit, monitor and report on any aspect of the Directorate's records, information and data management framework.

The Directorate's Records Manager provides strategic records management advice to the organisation and is guided by the Territory Records Office Standards and Guidelines and advice provided by TRO staff. It is imperative therefore that two-way communication is established and maintained between the TRO and the Directorate to facilitate best practice recordkeeping. Key contacts in TRO are:

Territory Records Office	Phone number
Director:	(02) 6207 0194
Deputy Director	TBC
Senior Advisor – Information Governance	(02) 6205 8613
Performance and Compliance Officer	(02) 6205 4872
Archives ACT	

Senior Advisor – Information Access	(02) 6205 3510
Archives Officer:	(02) 6207 5726
ACT Government Copyright	
Copyright Manager (Wed & Thu only):	(02) 6205 0186

TRO maintains a website and contact can be made by following the link or email address as follows:

https://www.territoryrecords.act.gov.au/functions/contactus

tro@act.gov.au

In relation to problem rectification or dispute resolution, the Directorate recognises that disputes may arise as follows:

- Where the Director of Territory Records does not approve a disposal schedule;
- Where the Director of Territory Records finds an element of the Records Management Program unsatisfactory; or
- Where the Directorate finds compliance with a requirement of the Director of Territory Records onerous or untenable.

2.4.5 Operational Instructions

Consistent with the provisions of the *Territory Records Act 2002,* the Directorate has in place arrangements for:

- Advising the Director of Territory Records about outsourcing any of the Directorate's recordkeeping responsibilities;
- Allowing the Director of Territory Records to examine the operations of Directorate's Records Management Program;
- Consulting with the Director of Territory Records for assistance, advice and training in relation to records management; and
- Allowing the Director of Territory Records to report on the Directorate's compliance with the Act and its Records Management Program.

Dispute Resolution

The Directorate's Records Manager maintains a close working relationship with the TRO and it is the preference of the TRO to liaise directly with the Records Manager concerning any Directorate recordkeeping matters. However, a Directorate officer may, at any time, refer a problem or an issue to the TRO for a solution. This includes any matter that is the subject of dispute with the Director of Territory Records. The Records Manager will endeavour to negotiate a settlement with the Policy Officer in the Territory Records Office.

The Director of Territory Records and the Records Manager shall make every possible effort to resolve matters by negotiation.

Should the Director of Territory Records and the Records Manager not resolve a matter, the Territory Records Advisory Council and the Chief Information Officer with responsibility for the Directorate Records Management Program shall make every possible effort to resolve the matter by negotiation.

Disputes not resolved to the satisfaction of the Chief Information Officer with responsibility for the Directorate's Records Management Program or the Territory Records Advisory Council shall be resolved through mediation.

A mediator shall be selected from persons qualified in the field of records management. The parties will implement the determined process and conclude the matter as directed.

2.5: Implementing the Records Management Program Procedure

2.5.1 Purpose

The purpose of this procedure is to ensure the implementation and review of the Directorate's Records Management Program in compliance the *Territory Records Act 2002*.

2.5.2 Scope

The procedure sets out the mechanism by which the Directorate will implement and promulgate the Records Management Program.

2.5.3 Responsibilities

The procedure applies to Records Manager / Records Management staff, and any staff, consultants and contractors with recordkeeping responsibilities.

2.5.4 Background

Better practice standards, including the International Standard on Records Management (ISO15489) emphasise the importance of having a records management policy to achieve good recordkeeping and good governance. The Directorate's Records Management Policy helps staff to understand the importance of managing records well, and sets the broad standards that staff must follow to achieve good records, information and data management.

2.5.5 Operational Instructions

Section 16 of the Territory Records Act sets out a number of elements the Directorate's Records Management Program must contain. These include arrangements for:

- Establishing policy, practices and procedures for creation, capture, control, managing, access, storage, retention and disposal of records;
- Notifying the Director of Territory Records about outsourcing of the organisation's records management arrangements; and
- Preserving records that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

In accordance with the *Territory Records Act 2002* and consistent with Territory Records Office Standards and Guidelines, the Directorate's Records Management Program will be implemented and promulgated via a number of mechanisms but not limited to:

- The Approval of the Records Management Program by the Director-General as Principal Office;
- The establishment and implementation of the Directorate's Recordkeeping Procedures;
- The development and maintenance of business tools such as Records Disposal Schedules and Functional Thesaurus;
- Implementing a disposal program for the disposal of time expired records;
- The use of compliant recordkeeping business systems;
- The use of education and awareness strategies including using the Directorate's Intranet to regularly promote recordkeeping;

- Reporting on the Records Management Program and providing recordkeeping advice to the Executive and staff;
- Embedding recordkeeping training as part of staff induction, as well as advice to staff on exit processes;
- Resourcing the Records Management Program with appropriately qualified Records Management staff;
- Ensuring the Records Management Program is accessible to all staff, contractors, consultants and members of the public;
- Ensuring the Records Management Program is regularly monitored, reviewed and updated as appropriate (at least every 5 years);
- Regular liaison with the Territory Records Office on the use and interpretation of Standards and Guidelines;
- Reporting on the Directorate's Recordkeeping activities through the Annual Report mechanism; and
- Provide a copy of the Records Management Program to the Director of Territory Records in accordance with Section 17 (3) of the *Territory Records Act 2002.*

2.6: Incorporating Records, Information and Data Management into Business Processes Procedure

2.6.1 Purpose

The purpose of this procedure is to provide all staff with information about incorporating records, information and data management aspects into all business processes.

2.6.2 Scope

The procedure emphasises the need to incorporate records, information and data management into all business processes.

2.6.3 Responsibilities

The procedure applies to all staff, consultants and contractors.

2.6.4 Background

Better practice standards, including the ACT Government's Records, Information and Data Standard and the International Standard on Records Management (ISO15489) emphasise the importance of having a sound records management framework to achieve good recordkeeping and good governance. The Directorate's Records Management Policy helps staff to understand the importance of managing records well, and sets the broad standards that staff must follow to achieve good records, information and data management.

2.6.5 Operational Instructions

Records, information and data governance is a defined process the Directorate follows to ensure high quality information exists throughout the complete lifecycle. The key focus areas of records, information and data governance include availability, usability, integrity and security. This includes establishing processes to ensure important records, information and data assets are formally managed throughout the enterprise, and the records, information and data can be trusted for decision-making. Often the processes used in records, information and data governance include accountability for any adverse event that results from information quality.

ACT Government's digital recordkeeping initiatives will make government services simpler, faster and easier to use. These initiatives are enabled by interoperable information, systems and processes that make it less costly and easier to share information, improve information quality, reduce unnecessary duplication and reduce the impact of structural changes in government.

The Directorate supports digital transformation initiatives by ensuring that information systems are interoperable, and created and managed in accordance with standards endorsed by government.

Any system deployed in the Directorate to manage records, information or data must be capable of continuous and regular operation in accordance with responsible procedures. The Directorate endorses the principles as outlined in AS ISO 15489 - "A Record system should:

- Routinely capture all records within the scope of the business activities it covers;

- Organise the records in a way that reflects the business processes of the records creator;
- Protect the records from unauthorised alteration or disposal;
- Routinely function as the primary source of information about actions that are documented in the records; and
- Provide ready access to all relevant records and related metadata".

To facilitate effective decision making, it is imperative that sufficient records, information and data management characteristics are applied in an accurate, efficient and timely manner.

Identify the value of transactions, communication and processes

Recordkeeping exercises risk management principles where judgements are made as to what is created and captured based on the perceived severity of the impact of not keeping a record. This valued judgement is based on the likely consequences and it is to be expected that the level and standard of documented evidence needs to match the circumstances.

To enable the Directorate to move to an outcomes-focussed approach, requires that records, information and data be treated as an asset that may be built upon, shareable (within the appropriate security framework), standardised (using endorsed standards), accessible and governed formally. This procedure forms part of Directorate's Records Management Program and is established to guide staff when considering the generation and capture of business records, information and data and how this information asset resides within the overall business need.

2.7: Business Systems Procedure

2.7.1 Purpose

The purpose of this procedure is to ensure that records, information and data managed in the Directorate's business systems are protected, inviolate, accessible and capable of retrieval, and are preserved in good condition for the length of time they are needed.

2.7.2 Scope

The procedure applies to all Directorate's business systems.

2.7.3 Responsibilities

The procedure applies to all staff, consultants and contractors.

2.7.4 Background

The Directorate has many business systems designed specifically for operational requirements. In accordance with Territory Records Office Standard for Records, Information and Data, these business systems should be capable of making and keeping full and accurate records. They should routinely perform fundamental recordkeeping processes on a continual basis – either individually or through linked operations – so that the full range of the Directorate's business activities are properly documented. These systems do not have to be dedicated recordkeeping systems. They can be business systems (such as database applications or web content managers) that incorporate the functionality required to keep records. They do not need to be large or centralised or accessible by everyone in the Directorate, but their recordkeeping role must be clearly identified and recorded in the Directorate's Data Architecture Register. Business systems lacking recordkeeping functionality must have the ability to export records to a compliant recordkeeping system to satisfy compliance requirements.

Territory Records Office has developed an assessment tool to assist business units to identify recordkeeping functionality within business systems - https://www.territoryrecords.act.gov.au/__data/assets/pdf_file/0005/585113/Business-Systems-and-Digital-Recordkeeping-Functionality-Assessment-Tool-WCAG-Copy.pdf.

This procedure complements ACT Government Cloud Computing Policy to ensure the protection of Government business and information through a risk managed approach.

2.7.5 Operational Instructions

In order to capture, maintain and provide evidence over time, the Directorate's business systems must be capable of performing various fundamental recordkeeping processes. These processes govern the following operations:

- **Capture** – formally determine that a record should be made and kept;
- **Registration** – formalise the capture of a record into a designated system by assigning a unique identifier and brief descriptive information about it (such as date, time and title);
- **Classification and indexing** – identify the business activities to which a record relates and then link it to other records to facilitate description, control, retrieval, disposal and access;

- **Access and security** – assign rights or restrictions to use or manage particular records;
- **Appraisal** – identify and link the retention period of a record to a functions-based disposal schedule at the point of capture and registration;
- **Storage** – maintain, handle and store records in accordance with their form, use and value for as long as they are legally required;
- **Use and tracking** – ensure that only those employees with appropriate permissions are able to use or manage records and that such access can be tracked as a security measure; and
- **Disposal** – identify records with similar disposal dates and triggering actions, review any history of use to confirm or amend the disposal status, and maintain a record of disposal action that can be audited.

In addition to meeting the metadata requirements, recordkeeping compliant systems must be self-documenting, self-contained as set out in the *Territory Records Office Standard for Records Information and Data* *and the* *Australian Government Recordkeeping Metadata Standard*.

The Directorate's primary business system dedicated to managing records is HPE CM9 (previously known as TRIM). A complete list of Directorate business systems is detailed in the Data Architecture Register.

Protection and Security of Digital Records and Systems

Most of the records, information and data contained in the Directorate business systems are of a 'Sensitive' nature. In accordance with ACT Government Security Policy Framework, and ICT Security Policy, sensitive and private information must be protected against unauthorised access or modification, external disclosure and other forms of misuse. Staff should, for the protection and security purposes, lock their computers when not at their workstation.

Cloud Storage

Digital records may be stored in cloud arrangements before they have been appraised. However, the Directorate must make careful assessments including an assessment of the potential risks to the security, accessibility and reliability of records, information and data, and identification of appropriate mitigation strategies.

3 - CAPABILITY PRINCIPLE

3.1: Records Management Performance Framework Procedure

3.1.1 Purpose

The purpose of this procedure is to ensure that the Directorate has key performance indicators and measures to implement its Records Management Program.

3.1.2 Scope

The procedure establishes obligations for the Records Manager / Records Management staff to ensure appropriate key performance indicators and measures are in place to implement the Directorate's Records Management Program.

3.1.3 Responsibilities

The procedure applies to the Records Manager, Records Management staff, consultants and contractors undertaking recordkeeping functionality.

3.1.4 Background

For records, information and data, relevant measures will include the extent of coverage for existing records disposal schedules, the provision of training and the success of that training, the use of endorsed locations, the results of annual physical file censuses, digital and physical storage requirements, internal audits of the Records Management Program, quality control checks on data entry and other processes including destruction quantities.

3.1.5 Operational Instructions

The Directorate has key performance indicators and measures to implement its Records Management Program including but not limited to:

Performance indicators	**Measured by**
Training requirements - Ensuring induction training is provided to new staff, and they have access to recordkeeping systems. Online and Core Capability training will also facilitate and serve as a refresher and reminder for existing staff of the importance of recordkeeping.	Percentage and details of staff trained and feedback on the success of the training can be provided to the Records Manager, including the number and frequency of staff actioning E-learning modules
Education and awareness strategies – the Records Manager / Records Management Unit to implement education and awareness strategies including: • Using Directorate's Intranet as a vehicle for communication • Emailing Managers / Supervisors	Raising the level of recordkeeping awareness in the Directorate and ensuring recordkeeping compliance and overall organisational performance through efficient information processes and use.

• Provision of Help Desk and telephone advice • Attendance at line area meetings • Information awareness month promotions / posters / brochures	
Business Systems Development Engagement The Records Manager / Records Management Unit to be involved and consulted in Business System Development and upgrades for recordkeeping and information management implications	Ensure business system being developed and / or upgraded have had a records and information impact assessment completed.
Business Tools - The Records Manager / Records Management Unit must ensure that important business tools such as the Functional Thesaurus and Records Disposal Schedules are monitored and kept up to-date and they reflect the Directorate's business.	Ensure Business tools meet compliance requirements in accordance with Territory Records Office Standards.
Descriptive Standards - An important measure is to ensure records are titled appropriately consistent with the Directorate's classification standards to facilitate access and retrieval.	Quality control checks of record titles by Records Management staff and feedback provided to line areas.
Disposal Program – Ensuring the Directorate has Records Disposal Schedule coverage its business and that these Schedules are implemented to dispose of business information in a timely manner.	Sentencing and disposal of records in a timely manner. Reporting the details of records to be destroyed to TRO.
Performance Reporting – Reporting on the performance of the Records Management Program. This includes development and implementation annual plans that maintain or improve records, information and data management capabilities.	The reporting of the implementation of the Directorate's Records Management Program in the annual report requirements is also an important performance indicator. This also includes generation of regular reports from the recordkeeping system of files created to ensure consistency and what files are due for destruction, to maximise efficiencies.
Accountability - The Records Management Unit must also undertake yearly record census activities and account for all files maintained onsite.	The results of the record census to be reported to Senior Management.
Quality Assurance - The Records Manager / Records Management Unit should assess the Directorate's Records Management against the ACT Public Service's recordkeeping maturity model and checklist	Reporting the results to Senior Management and TRO of the effectiveness and compliance.

Resource Allocation	The Records Manager to ensure there are sufficient human, financial and physical resources to do the work required. This includes ensuring there are appropriately qualified staff available to meet work requirements.
Ongoing Skills Improvement and Training	Participation of RMU staff in professional development and training opportunities conducted by industry associations.

Endorsed Locations:

To be fully accountable, the Directorate must know where all its records, information and data are located, and to have access to them. The following are endorsed record locations for the Directorate:

Description	**Custodian / Address**
Physical files - Ground floor file room and compactus	Records Management Unit - 11 Moore Street City
Physical files – CSD compactus various floors	CSD compactus on various floors – 11 Moore Street City
Digital Recordkeeping System (HPE CM9)	Records Management Unit - 11 Moore Street City
Whole of Government Electronic Document Records Management System	Shared Services Digital Records - Mitchell
CMS Business system (formerly CHYPS & YJIS)	Child Youth and Family Division -11 Moore Street City
HomeNet Business System	Housing ACT Division - Nature Conservation House, Cnr Benjamin Way & Emu Bank, Belconnen
Physical files - 1st floor File compactus	Housing ACT - Nature Conservation House, Cnr Benjamin Way & Emu Bank, Belconnen
Physical records - Mitchell Repository	Shared Services Record Services - 9 Sandford Street Mitchell
Physical records Hume Repository	The Information Management Group - 10 Sleigh Place Hume
Physical files- ACT Together	ACT Together - 26 Thynne St, Bruce

Refer also to Procedure 7.2 Protection and Security for more information on endorsed locations.

3.2: Capability Assessments and Maturity Development Procedure

3.2.1 Purpose

The purpose of this procedure is to help the Records Manager / Records Management staff to assess the capabilities of the Directorate to manage and control records, information and data in a consistent way.

3.2.2 Scope

The procedure establishes obligations for the Records Manager / Records Management staff to prepare and undertake the annual assessment of the Directorate's records, information and data management capabilities. The assessment results requires the approval of the Director-General (as Principal Officer) and subsequently the forwarding of the results to the Territory Records Office (TRO).

3.2.3 Responsibilities

The procedure applies to the Records Manager, Records Management staff, consultants and contractors undertaking recordkeeping functionality.

3.2.3 Background

TRO's Standard and Guidelines provide strategic direction for the Directorate's records, information and data management and articulate their application in a digital age. The TRO Standard for Records, Information and Data sets out seven principles which guide the management of information assets in the ACT Government.

The principles are:

Strategy	Capability	Assess
Describe	Protect	Retain
Access		

Each principle is supported by a TRO Guideline, advice and other tools. These tools are designed to enable the Directorate to meet baseline compliance requirements as well as to encourage and promote better practice opportunities for the management of its records, information and data.

TRO has developed a self-assessment tool (ACTPS Recordkeeping Maturity Model and Compliance Checklist,) consistent with the above principles to assist the Directorate to assess its capability and maturity level. The assessment tool sets out different levels of maturity depending on the size and scale of the organisation. Given the Directorate's human service interaction and delivery role, it is expected that the Directorate should reach a high level of maturity with regard to their information governance arrangements.

Information governance is critical in obtaining the greatest benefits from records, information and data assets. The Records Manager in conjunction with the custodians of business systems should consider records, information and data in line with the following:

- Who is the custodian of the records, information and data collected;
- How records, information and data collected contributes to the overall governance of the Directorate and the ACT Government;
- How information and data is obtained from other sources;
- Defining standards for data collected, where possible in alignment with classification, metadata standards, alignment with legislation, integrity, authenticity, access optimisation and efficiency of collection;
- That data collected meets client needs/expectations , or contributes towards better outcomes for clients;
- Defines currency profile of information;
- In conjunction with the security policy protocols define who has access or is able to discover the information;
- Ensures as little information as possible is not stored in an isolated format (e.g. paper or a disparate system);
- Aligns and is understood within the risk framework;
- Who may benefit from access to that information, and where to place that information so it is accessible and where possible, available for statistical analysis;
- That the information is appraised in relation to prevailing legislation and standards, in terms of information quality, recordkeeping and destruction;
- Advice, guidance and where appropriate, agreement from the Directorate's ICT Strategy Committee to proceed;
- Ensures that records information and data, valuable to others is discoverable and sharable; and
- Services are client-centric, and driven by information and knowledge.

All areas of the Directorate need to meet certain essential requirements to manage their records. Better practice records and information governance can help the Directorate to:

- Improve its business processes through faster access to and retrieval of information;
- make better-informed decisions through quicker access to all of the relevant information;
- lower compliance costs, such as in responding to FOI requests, and enhance their ability to provide accurate, timely and transparent responses to legislative and regulatory requirements;
- reduce business and reputational risks and improve business continuity;
- reduce the cost of staff looking for information across many information sources; and
- Save on the costs of creation, storage, retrieval and handling of records, information and data in all formats and across all locations.

3.2.4 Operational Instructions

Information governance maturity assessment necessitates the requirement to:

- Identify and liaise with key organisational contacts;
- Record the whereabouts of Records, Information and Data using the Directorate's Architecture Register; and
- Incorporate business improvement plans into the Directorate's annual work plans.

The TRO has identified four maturity levels that describe the sophistication and performance of an organisation's information governance arrangements. The TRO's maturity assessments model is derived from the ARMA International Information Governance Maturity Model and identifies four stages of information governance maturity:

- In Development - This level describes an environment where there is a developing recognition that information governance has an impact on the Directorate and that the Directorate may benefit from a more defined information governance program. The Directorate is vulnerable to redress of its legal, regulatory, and business requirements because its practices are ill-defined, incomplete, nascent, or marginally effective.

- Essential - This level describes the essential or minimum requirements that must be addressed to meet the Directorate's legal, regulatory, and business requirements. This level is characterised by defined policies and procedures and the implementation of processes specifically intended to improve information governance. The Directorate may be missing significant opportunities for streamlining the business and controlling costs, but they demonstrate the key components of a sound program and may be minimally compliant with legal, operational, and other responsibilities.

- Proactive - This level describes a Directorate-wide, proactive information governance program with mechanisms for continuous improvement. Information governance issues and considerations are routinely integrated into business decisions. For the most part, the Directorate is compliant with industry best practices and meets its legal and regulatory requirements. The Directorate can pursue the additional business benefits they could attain by increasing information asset availability, as appropriate; mining information assets for a better understanding of client and customer needs; and fostering the Directorate's optimal use of information assets.

- Transformational - This level describes an organization that has integrated information governance into its infrastructure and business processes such that compliance with the organisation's policies and legal/regulatory responsibilities is routine. The Directorate recognises that effective information governance plays a critical role in cost containment, competitive advantage, and client service. It implements strategies and tools for ongoing success.

After determining its maturity, the Directorate may – based on its defined business needs and risk tolerances – target different levels of anticipated maturity achievement and/or different areas of the organisation for each of the Principles.

3.3: Communication and Training Procedure

3.3.1 Purpose

The purpose of this procedure is to ensure that the Directorate has a recordkeeping communication and training plan in place to support the implementation of the Records Management Program.

3.3.2 Scope

The communication and training procedure is developed by the Records Manager / Records Management Unit in consultation with People Management Branch. This procedure establishes the communication and training strategies to implement the Directorate's Records Management Program. This communication and training procedure is a working document and must be updated as necessary to reflect the current recordkeeping and Directorate operating environment.

3.2.3 Responsibilities

The procedure applies to new staff (either transferring from another Directorate or new to ACT Government) with a responsibility emphasis for supervisors and managers as well as the Records Manager, Records Management staff, consultants and contractors undertaking / providing recordkeeping functionality.

3.2.4 Background

This recordkeeping communication and training procedure is designed to:

- Assist new staff with understanding how and when recordkeeping training is to be undertaken and who provides the training;
- Help staff better understand their role and responsibilities within the recordkeeping context; and
- Help staff in the Directorate familiarise themselves with specific emphasis on recordkeeping obligations for new workers.

3.2.5 Operational Instructions

The Directorate's intranet page provides all new starters with the recordkeeping information they need to know. To complete the CSD Orientation staff need to;

- Complete the CSD Orientation E-learning course and the assessments (available under the Community Services Directorate and Online Learning headings on the CSD Learning Management System);
- Register for and attend the Welcome to CSD: Meet the Executive session (available under the Community Services Directorate heading on the CSD Learning Management System);
- Arrange a time with your supervisor to develop an Individual Performance Agreement; ensuring there is a focus on recordkeeping responsibilities and obligations;
- Complete a Site or Team (Work Health and Safety) induction with your supervisor; and
- Managers and supervisors need to complete Request Access to CM9 (TRIM) Form via the CSD RMU website one week prior to commencement of new staff.

New staff to undertake the following Recordkeeping Training:

Recordkeeping Training	Provided by	Timeframe for completion
Face to face desktop HPE CM9 (TRIM) Training	**CSD RMU**	**One week after commencement**
The provision of "How to" online training to the Directorate's Recordkeeping system	**Learning management System** (Capabiliti)	**One month after commencement**
Core competency e-learning material for Recordkeeping	**Learning management System** (Capabiliti)	**3 months after commencement**

Other communication and training strategies to be employed by the Records Manager and Records Management staff include:

- Telephone, communicating with staff about recordkeeping processes and procedures;
- Email – the provision of a generic email address (CSDRMU@act.gov.au) to encourage liaison with staff;
- Help desk assistance – the ability to remote access to staff HPE CM9 desktops to assist and promote correct recordkeeping processes;
- Attending line area meetings to promote recordkeeping;
- One-on-one training and group training sessions to promotion consistent recordkeeping practices;
- Monthly emails to line area managers about statistical information and better recordkeeping practices;
- Intranet – promoting recordkeeping through the Directorate's Records Management website as well as providing monthly recordkeeping information to staff;
- Newsletters, including the promotion of Territory Records Office Newsletters;
- bulletin board – the use of bulletin boards to promote pertinent recordkeeping information;
- Liaising and training using Directorate technology such as WebEx / Jabber;
- Employee engagement and satisfaction surveys;
- Promotion of Information Awareness Month; and
- Territory Records Office website.

4 - ASSESS PRINCIPLE

4.1: Identifying a Territory Record Procedure

4.1.1 Purpose

The purpose of this procedure is to enable staff, consultants and contracts to identify Territory Records and the circumstances in which these records need to be managed.

4.1.2 Scope

The scope of this procedure is to define what a Territory Record is and the circumstance in which they are to be managed.

4.1.3 Responsibilities

The procedure applies to staff, consultants and contractors undertaking Directorate business.

4.1.4 Background

The *Territory Records Act 2002* (the Act) defines a record as '*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*'.

While the term 'record' has a specific meaning, in practice it can at times be difficult to distinguish between records and other types of information or data. Although the Act only applies to records, its principles can be applied to all ACT Government information and data holdings.

In the Directorate, records are considered important assets, and some are vital to the Directorate's business activities. They help to inform, plan for and achieve outcomes that are relevant and valuable to the community, business and Government.

Records, help to:

- Drive collaboration and communications
- Preserve knowledge for reference and re-use by the community and Government;
- Provide the foundation for sustainable and effective products and services;
- Outline responsibilities;
- Support decision-making;
- Document rights and entitlements;
- Make up the corporate memory of an organisation; and
- Provide stakeholders with transparency around, and accountability for, government operations.
- To support the benefits identified above, records, information and data need to be:
- Trustworthy, and managed accountably;
- Readily accessible, understandable, useable and securable;
- Valued as critical to business operations;
- Governed by appropriate risk management approaches; and
- Maintained to meet business, government and community purposes.

4.1.5 Operational Instructions

The Directorate makes, uses and maintains, but is not limited to, the following categories of records:

- **Administrative** – forms, correspondence, procedures, contracts, reports, photographs, publications, policies, guidelines, media releases, proposals, strategic and business plans, guidelines, minutes of meetings etc.
- **Financial** – forms, reports, invoices, financial statements, vouchers, payments, journals, receipts, remittances, budget estimates, credit notes, sales etc.
- **Programs** – agreements, correspondence, reports, maintenance history, impact statements, tendering documentation, disaster plans, proposals, policies, procedures, minutes of meetings etc.
- **Projects** – correspondence, notes, reports, contracts, plans, drawings, budget estimates, feasibility studies, tendering documentation, logs, functional and technical specifications, and minutes of meetings contract variations etc.
- **Cases** – personnel and human resources, child development clients, housing clients, CYF clients, complaints, lawsuits, contracts etc.
- **ICT** – procedures, workflow diagrams, archives and backups etc.
- **Regulatory and compliance** – authorisations, reports, statements etc.

Directorate staff will need to make a decision about the evidential value of a document, and the level of importance before determining whether a document is a corporate record or not. While the above might indicate that all records, information and data the Directorate receives or creates should be retained as corporate records. In reality however, some of the information could fall under the Normal Administrative Provisions of the Act and could be destroyed as a routine process.

5 - RETAIN PRINCIPLE

5.1: Creating Records Procedure

5.1.1 Purpose

The purpose of this procedure is to ensure that records created by staff, consultants contractors and service providers are complete and accurate.

5.1.2 Scope

The procedure is to ensure full and accurate records are created and managed to support the Directorate's operations and the interests of the community.

5.1.3 Responsibilities

The procedure outlines responsibility for all staff, consultants, contractors and service providers.

5.1.4 Background

In accordance with the *Territory Records Act 2002*, there is a requirement for the Directorate to make and keep full and accurate records of its activities. Full and accurate includes providing enough evidence in the records to demonstrate what business activities were undertaken. This includes outlining: what happened, who was involved, what decisions were made, what directions were given, actions taken, when it happened and, by implication, what didn't happen or wasn't recorded.

Records are made to meet business needs, accountability and evidentiary requirements and community expectations. On a day-by-day basis, the Directorate conducts business that affects the public and its clients and, in doing so, records are made and kept about its actions. The aim is to ensure full and accurate records are created and managed to support the Directorate's operations and the interests of the community.

Records need to be made in a form that will ensure they survive for as long as they are needed or mandated and that can be read and understood in the context in which they were created and used.

5.1.5 Operational Instructions

Directorate staff, consultant and contractors are responsible for determining if the documents and information they create or receive in the course of their duties are official records. The *Territory Records Act 2002* and Government policy require official records to be created, registered, maintained and disposed of according to Territory Records Office (TRO) procedures and records disposal authorities approved by the TRO.

The Territory Records Office has created an assessment tool to assist ACT Government employees to decide if you have an official record or some other type of material - http://sharedservices/territoryrecords/Is%20it%20a%20record/. By answering "yes" or "no" to the series of questions, you will be guided to the most likely result for the item, document or

information in question. If you are still unsure if the material is a record or not, contact the Records Manager for further advice.

Records should be created to meet future needs for evidence and information.

Records should be created:

- To document decisions made at meetings;
- When substantive business is conducted by the telephone or email;
- Formal decisions that affect business; and
- When face-to-face contact occurs and decisions or actions are made or taken.

Records should be accurate and should correctly reflect what was done, decided or communicated. They should also capture any subsequent resulting actions and decisions (e.g. minutes of meetings are signed, copies of outwards communications are signed or initialled etc.).

Records should be complete and should not only contain the content but also the structural and contextual information necessary to document a transaction and preserve the chronological relationship between the collective records.

Records should authentically show the business transactions that they represent (i.e. the records have not been tampered with or otherwise altered, unless authorised, detectable) and be recorded in a corporate recordkeeping system.

5.2: Capturing Records Procedure

5.2.1 Purpose

The purpose of this procedure is to ensure that records are systematically captured into recognised recordkeeping systems.

5.2.2 Scope

This procedure is to be used for incoming and outgoing paper and digital records that need to be formally managed as a collection within a file cover or digital container.

5.2.3 Responsibilities

This procedure applies to all staff, consultants and contractors.

5.2.4 Background

Records need to be accessible both now and in the future in line with *Section 15 of the Territory Records Act 2002*. To be accessible they must be effectively captured, described and controlled.

Capture is the process of deciding which records should be registered into a recognised recordkeeping system – manual or digital. How records should be captured into a recordkeeping system will depend on the nature of the system.

In manual filing systems this is usually done by attaching the record to a physical file and assigning a folio number to it. Papers should be placed on file in a logical sequence of records, usually chronological.

Recordkeeping systems capture specific information (metadata) about records, files etc. so that the records are identified, described and managed in a systematic and consistent way. The system maintains metadata about records forever, as an indication of the records' life history.

All the Directorate businesses, irrespective of their unique business activities, require systems that can capture full and accurate records and perform processes for managing those records over time. In order to be full and accurate, records must be authentic, reliable, complete, unaltered and useable, and the systems that support them must be able to protect their integrity over time.

5.2.5 Operational Instructions

Records are to be captured in recognised recordkeeping systems whenever there is a business need for evidence and future information retrieval. Some common records that must be captured in recordkeeping system(s) include:

- **Decisions, discussions and recommendations** – important Directorate business conducted orally in meetings or through face-to-face contact, such as over the counter in a shop front;
- **Client information** – business activities with regard to the management of Child, Youth and Families, Housing and Child Development clients. This includes reports, decisions, discussions and recommendations, including the creation and management of case notes;

- **Sending and receiving business correspondence** – records sent or received by email, fax or post;
- **Significant telephone conversations** – records documenting decisions or commitments conducted via the telephone; and
- **Electronic commerce** – records from transactions conducted online.

For more examples, refer to types of records detailed in Procedure 5.1: Creating Records.

When should records be captured?

Records are to be captured in a recognised recordkeeping system as soon as they are made or received. It is the responsibility of a staff member, consultant and contractor who makes or receives a record to ensure that it is incorporated into the recognised recordkeeping system.

How to capture records

(a) Manual systems – Paper files

Individual records that document a set of business activities have certain relationships with each other, for example a letter and a reply. It is essential that these relationships are preserved by being kept in one record, in chronological order and managed as a collection within a file cover

Staff must promptly attach all records they receive or make to an appropriate officially registered Directorate record. All records placed on files must relate directly to the file title. Documents are to be in date order and be folio numbered in ink at the top right-hand corner of the record. Responsibility for folio numbering rests with all staff.

If for any reason a folio has to be removed from a file, a Folio Removal Advice must be placed on the file indicating which folios have been removed and why, the date they were removed, the subject of the folios and the file to which they have been moved.

To avoid damaging legal documents, photographs etc. place them in an envelope with the contents described on the outside and attach it to the file.

'Post it' type notes or sticky labels are not to be used for action comments that have ongoing value to the contents of a file. A file note should be written and placed on the file, or the relevant record should be neatly annotated by hand and include name, initials, signature and date. Typed file notes printed and signed are also acceptable.

(b) Business systems – Digital records

Digital capture will entail registering documents from the Directorate's authoring applications such as email, Microsoft Word or Excel into a recognised and recordkeeping compliant business system. In order for business systems to be considered recordkeeping compliant certain attributes need to be embedded in the system to satisfy the Australian Government Recordkeeping Metadata Standard (AGRMS), as endorsed by Territory Records Office.

Business systems may also serve as recordkeeping systems, but to do so they must be capable of performing various fundamental recordkeeping processes as identified previously in this procedure. The Territory Records Office has developed a business system recordkeeping functionality

assessment tool checklist to assist the Directorate to undertake a detailed assessment of our current business systems and aligning it with the principles of Territory Records Office Standards.

The corporate recordkeeping system for the Directorate is currently HPE CM9 (formerly known as TRIM). A list of Directorate business systems that capture and maintain the organisation's information can be found in the Data Architecture Register of the Records Management Program.

The same principles and guidelines that apply to the storage and security of paper based records also apply to digital records for as long as the records are required and mandated by the relevant records disposal schedules. This means that digital records should:

- Be full and accurate;
- Be controlled in a systematic, compliant and reliable manner for as long as the record is required;
- Be locatable, retrievable and able to be read and used;
- Be technology enabled in that the tools and processes are in place to enable the protection and preservation of digital records; and
- Be accessible now and in the future as records deemed to be Territory Archives.

5.3: Tracking Records Procedure

5.3.1 Purpose

The purpose of this procedure is to track the movement and use of Directorate records to identify outstanding actions required for records, monitor the usage of the corporate recordkeeping system, and to assist with audit functions.

5.3.2 Scope

The procedure applies to all records.

5.3.3 Responsibilities

The procedure applies to staff, consultants and contractors who have access to identified and recognised corporate business systems.

5.3.4 Background

The location of the Directorate's records, information and data must be known at all times. There are two main reasons for tracking the movement and audit activity of records:

- To enable records to be found; and
- To record and maintain all transactions relating to an individual records or detail in the corporate recordkeeping system as evidence of what has happened to the record throughout its life. Such transactions include registration and classification, modification, security and access, physical movements (where appropriate) and ultimate disposal.

It should be possible to obtain a movement history and audit trail of all the Directorate's records.

The Directorate's Records Management Unit and Shared Services Record Services maintain compliant recordkeeping systems. The respective systems must be updated each time a change is made to record e.g. when a physical files has passed to a different person or sent for storage, to record who has accessed a record. Any changes of physical location of a paper-based file must be notified to either CSDRMU@act.gov.au or SSACTRecordservices@act.gov.au .

5.3.5 Operational Instructions

Best practice records management is based on principles of accountability and efficiency and is founded on the international Records Management Standard AS ISO 15489.

For purposes of accountability, the access, location and audit history of records must be maintained at all times. The action record on the file cover must indicate the receiving staff member's name when passing a file from one officer to another. If all action is complete and the file is being returned for storage, the relinquishing staff member must sign off on the file cover and annotate it for Put Away (P/A).

Returning files

If the file is no longer needed it should be annotated 'P/A' (for Put Away) on the file cover and returned to either the Directorate's Records Management Unit or Shared Services Record Services, depending on who created the file.

File census

A file census should be arranged by the Records Manager annually. Files and records registered in a corporate electronic recordkeeping system must be tracked to ensure that all movements of physical records are traceable and auditable. The Directorate's recognised recordkeeping system is HPE CM9. This system must track the issue, transfer between persons and return of items to their 'Home' location or storage, as well as who has accessed the record and the disposition or transfer to any other authorised external organisation, including an external secondary storage service provider.

Business Systems

All business systems that store Directorate records, information or data must have the ability to capture and maintain a record history, including the ability track document version control as well as access and security for all staff members with authorised access. The business system must be able to produce an audit trail for all changes made and track who made the change.

Digital records should be linked to, associated with or contain the metadata necessary to reflect the nature of the transaction (for example by email) and track the record throughout its development and use. This metadata includes:

- The structure of the record, that is, its format and the relationships between the elements comprising the record, which should remain intact,
- The business context in which the record was created, received, used, and edited, for example the draft versions and approval of a final version of ministerial correspondence, and
- The business process of which the transaction is a part, the date and time of the transaction and the participants in the transaction. All links between documents held separately but combining to make up a record should be present and accessible via the recordkeeping system.

5.4: File Management Procedure

5.4.1 Purpose

The purpose of this procedure is to ensure that Directorate staff are aware of the File Management processes involved to achieve uniformity and consistency over the Directorate's records.

5.4.2 Scope

This procedure sets out the File Management processes to be followed, together with appropriate naming conventions and protocols for paper-based file and digital records.

5.4.3 Responsibilities

All staff, consultants and contractors must comply with this procedure.

5.4.4 Background

Records is a generic term used to describe paper based files, digital documents, information and data. Records bring together in one aggregate, (be it digital container or physical file cover) all related information (documents) for a specific activity or transaction including key decisions made, who they were made by and when they were made. The record contains the history on a particular activity, usually in chronological order and in a way that facilitates current reference and future retrieval, and it protects the documents from loss or damage.

5.4.5 Operational Instructions

New records should be created when:

- A new function, business transaction or subject comes to hand.
- A new client has been identified.
- The subject matter has changed and the title no longer describes the contents of the record.

Emails and other digital records should be captured into the recordkeeping system as soon as possible to facilitate their control and management. With regard to client records, each client should have a separate record which is cross-referenced to related records (e.g. other family members).

How to create / request new records

- To create a new digital container / and or record refer to the Directorate's intranet on e-learning for recordkeeping.
- To order a new paper-based record, use the 'eFile Request Form', located on the Directorate's Records Management Intranet page.

Titling records

The title of a record should reflect its contents, and 'tell the story' of an activity, project or case, helping staff to find relevant information quickly. Thoughtless titling can have serious effects not only on the value of the record for administrative action but also on the quality of reference services later on.

All Directorate record titles must begin with a Function term, followed by an Activity gained from the authorised *Whole of Government Functional Thesaurus*. All record titles may include a subject term if a suitable one exists in the thesaurus. Free-text is a mandatory requirement to further specify the contents of the record. The terminology used in the Functional Thesaurus is directly linked to the *Whole of Government* and Directorate Records Disposal Schedules for consistency purposes.

All record titles must be double-checked for spelling errors, particularly where client names are being recorded, and conform to the Directorate's Data Entry Standard.

For further advice please refer to the Directorate's advice sheets:

- Advice Sheet 4: Rules for Selecting Functions, Activities, and Subjects; and
- Advice Sheet 14: Instructions for Free Text Titling of Files.

Staff can make suggested changes or additions to the terms in the thesaurus by using the Thesaurus Suggestion Form. The Records Manager is responsible for ensuring the quality and integrity of the Directorate's thesaurus is maintained at all times.

Security of Records

A record is to be assigned a security classification at the earliest stage possible during creation. The Record will be given the highest security classification of the documents to be placed on the file / digital container. Refer to Procedure 7.2 – Records Security for further advice.

File thickness, parts or amendments

The thickness of a paper-based file should be confined to approximately 200 folios or 2.5 cm thick. When a file is full and is still in current use it should be closed and a new part created. The file title remains exactly the same for both the old and new parts.

Refer to the Directorate's Records Management Unit Operations Manual (HPE CM9 - 2016/10177) for more details.

Attaching papers to files

Documents are to be placed in chronological order with the oldest paper at the back of the file and the most recent papers on top. The file request form is always the first document on the file.

Folio numbering

All documents on a file are to be folio numbered in the top right-hand corner in ink. This is good administrative practice in the event that files are subpoenaed or subject to legal processes such as Freedom of Information requests or hearings by the Ombudsman or ACT Civil and Administrative Tribunal.

Plastic sleeves used to place photographs, maps, legal documents etc. on a file without damaging them must also be folioed. The plastic (using appropriate stickers) should be folioed rather than damage the documents.

Amending file titles and contents

Staff must not attempt to alter or correct a paper-based file title by writing over the label on the file cover. If a file title is considered inappropriate because growth has led to a change in the scope or new folios go beyond the original scope of the file title, submit an eFile Request Form to the Directorate's Records Management Unit or Shared Services Record Services for amendment. Refer to the Directorate's Records Management Unit Operations Manual for more details.

Temporary files

A temporary file should only be created when all search procedures have been completed and the Directorate's Records Manager or Shared Services Record Services are satisfied that genuine steps have been undertaken to locate the file. Refer to the Directorate's Records Management Unit Operations Manual for more details.

Alteration to or cancellation of records

Staff are not to alter, cancel or destroy a registered record. Failure to observe this requirement contravenes the *Territory Records Act 2002* and will create serious inaccuracies in the recordkeeping system making retrieval difficult.

Returning files

When action has been completed on a paper-based file or if further action is not expected in the immediate future, staff should forward the file to either the Directorate's Records Management Unit or Shared Services Record Service for storage. Staff should ensure that:

- All current action is complete;
- Columns on the front cover have been completed;
- The file is not over- or under-classified;
- All papers have been correctly folio numbered;
- Documents are not loose, clipped or stapled to the inside cover. They should by properly attached to the file; and
- The correct paper quality is used, i.e. recycled or archival paper.

Retrieving files

Paper-based files stored in an off-site facility may be retrieved by submitting a request to the Directorate's Records Management Unit or Shared Services Records Service by telephone or email CSDRMU@act.gov.au or SSACTrecordservices@act.gov.au .

Closing files

Once a paper-based file is closed, no further documentation of business transactions will be added to it. Responsibility for the maintenance of files rests with staff while files are in their possession.

Preservation of files

Damaged files should be returned to the Directorate's Records Management Unit or Shared Services Record Services for replacement of covers as required. Sticky tape or other adhesive tapes must not be used for patching up papers on file. If documents need mending contact the Directorate's Records Manager or Shared Services Record Services for advice.

5.5: Digitisation Procedure

5.5.1 Purpose

The purpose of this procedure is to ensure that the processes of, and requirements for, the digitisation of records, information and data reflect the requirements of the Territory Records Office Standards.

5.5.2 Scope

The procedure is to be used when decisions and actions taken by staff, service providers, consultants and contractors relate to the digitisation of records, information and data. This procedure also applies to organisations that provide outsourced services on behalf of the Directorate.

5.5.3 Responsibilities

The procedure applies to all staff, consultants and contractors,

5.5.4 Background

Digital records like other formats, provide evidence of the day-to-day business activities the Directorate conducts that affects the public and its clients. They are subject to legislation such as the *Territory Records Act 2002* and the *Freedom of Information Act 2016* and to legal processes such as discovery and subpoenas. Digital records made or received by the Directorate are Territory records.

5.5.5 Operational Instructions

The *Records Disposal Schedule – Source Records* is the official authority for the disposal of Territory Records that have been converted into another format.

When converting a record from one format to another, the source record is the record being converted and the converted record is the result of the conversion. For example, if the source record is a hard copy document, the result of the conversion is a digital copy of the document. The requirement to retain the source record is dependent on the value of the source record, and retention of the resulting record must comply with the Territory Records Office *Standard for Records Information and Data.*

Examples of such conversions are:

- Digitisation of a paper original;
- Microfilming of a paper original;
- Digitisation of a microfilm;
- Conversion of a digital record from one software format to another;
- Conversion of a database to a set of PDF files and a spreadsheet.

When undertaking the digitisation of records, the following should be considered:

- Does the converted record contain the “full and accurate” information contained in the source record?
- Does the converted record meet the Directorate’s business needs?
- Does the converted record meet legal, financial and other requirements?

- Can the converted record be accessed and retained for as long as it is required?
- Can the source record be disposed of?

The answers to these questions will determine whether the converted record can be considered a reliable source of information, allowing the source record to be destroyed.

Another consideration when converting records is whether the conversion is pre or post action conversion.

Pre-Action conversion is where the conversion is carried out as soon as the record is received. For example a letter is received and scanned immediately upon receipt.

Post Action conversion is where conversion is carried out after any action has been taken on the records. For example the digitisation of existing paper-based files in which the action has been completed.

Technical standard

The following are considered the technical standard acceptable output for the scanning / digitalisation of records:

Output file formats

TIFF, PDF PDA/A JPEG 2000 (recommended for photographs).

Resolution
200 to 300 DPI /PPI recommended for most documents.

Colour resolution or bit depth

- Black and white documents: 8 bit greyscale
- Colour documents where colour is not critical. 8 bit colour
- Colour documents where colour is critical. 24 bit colour

Compression

Lossless compression where no information is irretrievably lost and where the decompressed object will always appear exactly the same as the original.

Quality Assurance

- Basic quality criteria checks against the original should include:
- Smallest detail legibly captured (e.g. smallest type size for text);
- Clarity of punctuation marks, including decimal points;
- Completeness of details (e.g. acceptability of broken characters missing segments of lines;
- Dimensional accuracy compared with the original;
- Scanner- generated speckle (speckle not present on the original);
- Completeness of overall image area (i.e. missing information at the edges of the image area);
- Density of solid black areas;
- Colour fidelity;
- Page numbers compared to the original (e.g. did all page scan, especially if documents were two sided); and
- Page sequencing (e.g. did all pages scan in correct order.

These quality checks must be undertaken before the original version / source record is destroyed.

5.6: Managing Copies of Records Procedure

5.6.1 Purpose

The purpose of this procedure is to provide all staff with information about the process of, and requirements for, producing copies of Territory records.

5.6.2 Scope

The procedure ensures that minimum duplication of records occurs, and that the existence of copies of records is acknowledged and controlled.

5.6.3 Responsibilities

All staff, consultants and contractors who create or use records are responsible for managing all copies of records they create.

5.6.4 Background

Technology has made the copying of records, both hardcopy and electronic, very easy. This has resulted in large quantities of copies of records being made. Copies that are themselves an essential part of a business transaction or of a different form of record can become records in their own right, and these will need to be captured into the Directorate's recordkeeping. Satisfying all the differing needs may result in a record existing in more than one location and one form. However, it is necessary to ensure that minimal duplication occurs and that the existence of copies is acknowledged and controlled.

For records, information and data maintained in the Directorate's business systems, Shared Services ICT backs up this data in line with industry standards and practices using an enterprise wide application methodology.

5.6.5 Operational Instructions

If it is necessary to create and maintain a copy of an existing record, other than for convenience or reference, the copy should include:

- Reference to the original record (e.g. in the footer if it is a digital document) sufficient for any staff member to differentiate the copy from the original and to facilitate the location of the original record; and
- Metadata detailing the authorised recordkeeping system to which the copy belongs.

If the copy is to replace an original, the copy (including all the metadata, evidence and features applying to the original) is to be registered into the authorised recordkeeping system which controlled the original.

The original records may be destroyed providing that the replacing copy can be reliably authenticated as a true copy and preserved for the period stated in an appropriate record disposal schedule. However, if any significant feature of the original cannot be copied, the original must be retained.

Where the copy is in digital form all the metadata, structure, and features applying to or included in the original and the original's container (such as an electronic file) must be preserved.

In some cases it may be necessary to copy an original record to facilitate its preservation. For example the copying of Adoption Registers not only serves to provide a reference copy of the Register for access purposes but serves to protect the original from continual use as an historical record. Refer to Procedure 5.5 Digitisation and 7.1 for Preservation.

5.7: Records Disposal Schedules Procedure

5.7.1 Purpose

The purpose of this procedure is to help Records Management staff develop and implement records disposal schedules.

5.7.2 Scope

This procedure applies to all Directorate records.

5.7.3 Responsibilities

The procedure applies to the Records Manager / Records Management Unit staff, consultants and contractors who have recordkeeping responsibility. Records Manager is responsible for managing, monitoring and approving records disposal within the Directorate in liaison with the Territory Records Office.

5.7.4 Background

The Territory Records Office (TRO) under the auspices of the *Territory Records Act* 2002 *(*the Act) has the responsibility for the regulation of recordkeeping policy throughout ACT Government. This mandate also includes the authorisation of records for retention or destruction (after their value has been determined during appraisal) through legal instruments known as Record Disposal Schedules (RDS). TRO also assists the Directorate by:

- Monitoring and providing guidelines and advice for appraisers;
- Setting mandatory standards for record disposal schedules;
- Authorising all records disposal schedules; and
- Giving directions for identifying Retain as Territory Archives (RTA) material.

It is a requirement under the Directorate' Records Management Program and the Act to notify the TRO of all files destroyed in accordance with approved RDS and Whole of Government Records Disposal Schedules.

5.7.5 Operational Instructions

Record Disposal schedules (RDS) are legal documents (Notifiable Instruments) issued under the Act by the TRO in conjunction with the Territory Records Advisory Council for the retention and or disposal of ACT government records. A key component of a RDS is the disposal class which outlines:

- The unique class number,
- Record description; and
- Disposal action and trigger to be applied to the record.

RDS' are also used to indicate classes of records for which destruction is not authorised. The Act provides that records are not to be disposed of without the consent of the TRO unless the action of disposal is positively required by law, or takes place in accordance with a normal administrative practice of which the TRO does not disapprove.

RDS specify classes of records and the **minimum** length of time they should be kept. RDS' are used to 'sentence' records.

Appraisal

The TRO defines appraisal as "the process of evaluating business activities to determine which records need to be captured and how long they need to be kept, to meet business needs, the requirements of organisational accountability and community expectations".

Appraisal, using the Designing and Implementing Recordkeeping Systems (DIRKS) methodology involves analysing the business or operations of the Directorate to identify its recordkeeping needs. Appraisal focuses on:

- The need for documents or records generally;
- The needs of business or operation itself;
- Requirements for the Directorate to be accountable;
- Community expectations that certain records will be created, maintained and retained or destroyed appropriately;
- Examining the interests of stakeholders; and
- Carrying out risk analysis to assess stakeholder/s requirements for records including the retention duration.

The result of appraisal is decisions about which records should be created or captured and for how long they should be kept. These (disposal) decisions are recorded in RDS which then can be applied to records. Creation and capture decisions are promulgated through the Directorate's Records Management Program.

5.8: Sentencing Records Procedure

5.8.1 Purpose

The purpose of this procedure is to help Records Management staff understand and perform the task of sentencing records, information and data.

5.8.2 Scope

The procedure is to be used by Records Management staff, consultants and contractors for the sentencing of the Directorate's records, information and data.

5.8.3 Responsibilities

The procedure applies to the Records Management / Records Management Unit and staff, consultants and contractors who have recordkeeping responsibility.

5.8.4 Background

Sentencing is the process of identifying and implementing appraisal decisions (discussed later in this procedure) contained in relevant Record Disposal Schedules and applying the appropriate disposal action to a record. Sentencing allows the Directorate to apply the decisions made about classes of records to individual records. Together appraisal, sentencing helps the Directorate to identify which records should be retained.

5.8.5 Operational Instructions

There are five basic steps in sentencing:

- Determine the appropriate function and activity of the record. This can be done by examining an existing record or when creating a new record.
- Identify the disposal class.
- From the disposal action in the class, identify the trigger event and a date when the record can be disposed of; alternately, identify that the record is to be Retained as Territory Archives.
- If the trigger event has already occurred (such as action is completed), confirm and implement the disposal action.
- If the trigger event has not occurred (e.g. the record is still in active use), set a review date for the future.

For older legacy records, the steps relating to setting the review date, confirming whether the disposal trigger has occurred and confirming the disposal decision may take place simultaneously. For example, staff may look at an accounting record, match it to the correct Finance and Treasury Management class in the Whole of Government Online Records Disposal Schedule, calculate the review date as seven years from action completed, note that action was completed eight years ago, and therefore confirm that the record can be destroyed immediately.

Digital Records

The general principles for sentencing are the same for all records no matter what their format. Although it is possible to set up a digital system to keep every record until you look at each one and

decide whether to delete or save it, this will be very time consuming. One of the reasons for installing a digital system is to automate processes. You can instruct the system to delete a record at a time (years) after it has completed its transaction.

It is important to have a review or quality control procedures in place to make sure disposal actions are being implemented correctly. For further information regarding sentencing refer to the Directorate's Advice Sheet number 5 - *Steps for Classifying and Sentencing a File*.

Appraisal

The TRO defines appraisal as "the process of evaluating business activities to determine which records need to be captured and how long they need to be kept, to meet business needs, the requirements of organisational accountability and community expectations".

The result of appraisal is decisions about which records should be created or captured and for how long they should be kept. These (disposal) decisions are recorded in RDS which then can be applied to records. Creation and capture decisions are promulgated through the Directorate's Records Management Program.

5.9: Destruction of Records Procedure

5.9.1 Purpose

The purpose of this procedure is to ensure that Directorate's records, information and data are destroyed in a planned, systematic, consistent and authorised way.

5.9.2 Scope

The procedure relates to all records, information and data.

5.9.3 Responsibilities

This procedure applies to all Directorate staff, consultants and contractors that have the authority to make decisions about the destruction of the Directorate's records. The Records Manager in consultation with the Territory Records Office is responsible for managing, monitoring and approving records disposal within the Directorate.

5.9.4 Background

Destruction also referred to as disposal and it infers any action that changes the circumstances of a record or removes a record from its usual setting. Such actions pose risks to the information that can be obtained from records and if not controlled can mean that we lose evidence about business activities.

'Disposal' when used by the Territory Records Office can mean:

- Destruction of records;
- Damage to or alteration of records;
- Transfer of the custody of records;
- Transfer of the ownership of records;
- Separation from or disturbance to the contextual information, software, hardware, or other equipment on which records depend; or
- Rearrangement.

Under the *Territory Records Act 2002* the Territory Records Office regulates the disposal of records. Legally, disposal of records can only be carried out if:

- The Territory Records Office gives permission;
- There is a law positively requiring a particular disposal action;
- The disposal is a 'normal administrative practice' that the Territory Records Office has not disapproved; or
- It is to return the records to the rightful custody of a public body of the Commonwealth or a State.

Destruction also relates to the deletion of records, information and data from the Directorate's business systems in accordance with approved and authorised Record Disposal Schedules.

5.9.5 Operational Instructions

The Territory Records Office authorises the destruction of records through legal instructions such as *Whole of Government Records Disposal Schedules*. The destruction of records normally occurs after records have been sentenced to ensure consistency and uniformity. This process ensures that the Directorate's records are disposed of in a timely and systematic manner.

Before any record can been destroyed, sentencing should be undertaken to ensure records have been accorded the appropriate Records Disposal Schedule. Sentencing involves determining the appropriate RDS, disposal class for the record and implementing the disposal action in a timely and efficient manner. To ensure transparency, the Records Manager / Records Management staff should obtain authorisation for the destruction of records from appropriate business areas to satisfy accountability.

Normal Administrative Practice

The NAP provision of the Act allows for the destruction of ephemeral material without the need for formal authorisation. The following are examples of documents and information that can be destroyed under NAP:

- Working papers i.e. rough notes, calculations, statistical and research data used in the preparation of correspondence;
- Draft versions of documents that show no significant changes or annotations relating to the formulation of policy or procedures and legislation (i.e. draft charts, minutes);
- Duplicate documents (i.e. information copies of records already held on file or internal and external publications held for information);
- Facilitating instructions (i.e. general instructions on formatting rather than content);
- Personal notes and messages; and
- Ephemeral information (e.g. brochures from outside organisations, that have no continuing value and are generally needed for a few hours or days)

NAP is not designed as a replacement for approved RDS, which also forms part of the Directorate's Records Management Program.

Methods destruction

Records may only be destroyed using one of the following methods:

Paper Records:

- Pulping
- Shredding

Digital records maybe deleted from business system once they are time expired in accordance with RDS or NAP provisions.

Unlawful destruction

Under the *Territory Records Act 2002* a penalty applies for unauthorised disposal. Other laws, like the *Crimes Act 1914*, also have penalties for destruction or falsification of records. The Directorate is accountable for its records and how it maintains them. Properly implemented disposal authorisation from the Territory Records Office is a valid means of showing why records were destroyed.

The Whole of Government Records Disposal Schedules

Records Disposal Schedules set out:

- The types of records an agency must make in relation to its business activities;
- How long those records must be kept to meet business and accountability requirements; and
- Which of those records have ongoing value to the community as Territory Archives and must be preserved indefinitely for the benefit of present and future generations.

The *Whole of Government Records Disposal Schedules* are designed to cover records common to all or most government agencies. Common records relate to administrative functions such as finance and accounting, travel, property management, personnel etc.

The Directorate specific Records Disposal Schedules

The Directorate's specific schedules cover unique (operational) records such as those relating to disability, housing and community services programs, and children, youth and family programs. These schedules are approved by the Director of Territory Records under the provisions of the *Territory Records Act 2002*.

6 - DESCRIBE PRINCIPLE

6.1: Metadata Procedure

6.1.1 Purpose

The purpose of this procedure is to ensure that not only do all staff apply sufficient and accurate metadata to their records, information and data but that metadata is instrumental in the design and configuration of all business systems.

6.1.2 Scope

The procedure relates to all records, information and data.

6.1.3 Responsibilities

This procedure applies to all staff, consultants and contractors. The Records Manager / Records Management Unit in conjunction with business system owners are ultimately responsible for monitoring and ensuing appropriately metadata is applied to records, information and data.

6.1.4 Background

Metadata can be described as information about information. Records, information and data need to be described so that people know and understand their context and purpose, and can find them easily when they need to. This procedure complements the Shared ICT Business Application Policy and the Metadata for Web-based Resources Standard to ensure data standards are appropriately maintained. Metadata can be used to identify, authenticate and contextualise information and the people, processes and systems that create, maintain and use it. It allows users to control, manage, find, understand and preserve information over time. Some examples of metadata are:

- title
- author
- any registration number or other unique identifiers
- date created or received
- subject matter
- format
- history of use.

In addition to this content, records, information and data should be linked to, or contain the metadata necessary to reflect the nature of the transaction (for example by email) and track the record throughout its development and use. The metadata includes:

- The structure of the record, that is, its format and the relationships between the elements comprising the record, should remain intact;

- The business context in which the record was created, received, used, and edited, for example the draft versions and approval of a final version of ministerial correspondence; and

- The business process of which the transaction is a part, the date and time of the transaction and the participants in the transaction. All links between documents held separately but combining to make up a record should be present and accessible via the recordkeeping system.

6.1.5 Operational Instructions

The Territory Records Office Standard for Records, Information and Data, and accompanying Metadata Guideline provide guidance for staff with implementing or decommissioning business systems. Metadata is required to ensure that records are authentic, reliable, understandable and usable evidence of business activity. However, the extent of metadata applied to records and the way it is managed can be influenced by the sensitivity and significance of the records it relates to.

Metadata requirements for records systems

Business systems used to manage records, information and data should be configured to meet the requirements of an Electronic Document Records Management System (EDRMS) and recommended records management metadata fields provided by the Territory Records Office. This includes making full use of system audit trails and whole of government business classification scheme and thesaurus.

Business classification information is an important metadata element that is crucial to ensuring that the value of records, information and data is understood. It is a hierarchical scheme for identifying and defining the functions, activities and transactions the Directorate performs in the conduct of its business. A business classification scheme is developed as a result of identifying information, data and records management requirements. This tool assists the Directorate to correctly assign business classification scheme terms to records, information and data and is known as a 'thesaurus'. A thesaurus allows common terms to be linked to the defined terms as outlined in the approved business classification scheme.

The Territory Records Office maintains the Whole of Government Recordkeeping Thesaurus, which should be used by all ACT Government organisations.

The ACT Government's Digital Recordkeeping Policy for the ACTPS requires that digital recordkeeping be considered in all ICT systems. The Directorate must consider when acquiring, upgrading or replacing digital business systems, including entering into software as a service arrangements, what records will be created in the system and their metadata requirements. Business systems may capture and maintain records and their metadata internally, or may export records and their metadata to another system such as an EDRMS.

7 - PROTECT PRINCIPLE

7.1: Preserving Records Procedure

7.1.1 Purpose

The purpose of this procedure is to ensure that records, information and data that has been identified as having long-term or permanent value are accessible, retrievable and are preserved for the length of time they are needed.

7.1.2 Scope

The procedure applies to all records, information and data that need to be protected from loss or destruction to meet ongoing access requirements in accordance with the *Freedom of Information Act 2016* and the *Territory Records Act 2002*.

7.1.3 Responsibilities

The procedure applies to all staff, consultants and contractors.

7.1.4 Background

The life expectancy of records is directly affected by the medium and conditions under which they are made, stored, used and maintained. The Directorate's records, information and data that has been identified as having long-term or permanent value, irrespective of their format, will require appropriate migration strategies in place, as well as (for paper based records) appropriate storage conditions and handling processes of a quality sufficient to preserve them for as long as required. This procedure complements ACT Government Cloud Computing Policy to ensure the protection of government business and information through a risk managed approach.

If these records are inappropriately stored and handled they will deteriorate very quickly. The causes of deterioration can relate to poor quality of paper, increased use of records, and poor storage conditions. Analogue tapes can also deteriorate through lack of use, overuse, or playback on poorly maintained playback devices. Storage conditions and handling processes should protect records from loss or destruction.

Appropriate environmental and housing conditions, a program of ongoing maintenance and, where necessary, migration strategies, are important and critical measures. These processes should be undertaken to prolong the life of the Directorate's records, information and data that have been appraised as having long-term or permanent archival value.

7.1.5 Operational Instructions

Protecting and handling record formats – Paper files

Paper files contain a collection of documents such as written or typed correspondence, printed material (pamphlets, reports or brochures), thermal paper, photographs. Since all the items on a file, including the cover, are paper-based, staff need to consider the potential long-term value of the records they are making and filing. Where paper records are assessed as having long term value, then it is recommended that documents and publications be maintained on archival quality paper.

Care of digital records, information and data

Restrictions on physical storage locations do not apply to digital records, which may be stored in cloud arrangements before they have been appraised according to Territory Records Office's Standard for Records, Information and Data and accompanying Access Guidelines. The Directorate must, however, make careful assessments of their digital records that may be stored and managed in cloud or other off-site arrangements. This includes an assessment of the potential risks to the security, accessibility and reliability of records, information and data, and identification of appropriate mitigation strategies. Territory Records Office advice outlines some of the risks and restrictions of using off-site storage for digital records, information and data is available on their website.

Preservation / migration dependencies

A key characteristic of records is that they cannot be understood in isolation. In order to provide context for the record, additional information about the work process or the business system may be required to ensure the records are understandable, to prove the reliability of the evidence, or if records need to be moved from one system to another in the future. Required system information necessary for migration and preservation may include:

location	business rules implemented	privacy management
system issues/faults	file formats	data structures
size	security	data and class models
workflow routing rules	audit trails	

File management

Before placing paper based files in storage staff are to ensure that the files are free of dust and unaffected by mould, insects or active deterioration. Staff are to ensure:

- All file containers are of archival quality;
- All file containers are labelled;
- Items appropriately fit the container (they should not be folded);
- Files are to be stored on their spine within the container; and
- Thin items that are stored on their edge must be supported to avoid curling or sagging.

Records that contain information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage are to be identified and preserved in secure but readily available facilities.

Maps and plans

Maps and plans are made on a wide range of materials such as tracing and offset papers, plastic film and photosensitive and synthetic papers. Maps and plans can be difficult to handle because they are usually large and can easily tear and tend to sag. Enough space should be allowed for their safe manoeuvring when viewing. It is important to ensure that:

- Map and plan drawers and packaging are free of dust and unaffected by mould or insects before maps and plans are placed in them;
- Maps and plans are stored flat inside plan cabinets that are labelled;
- Maps and plans are not folded as this will damage them. If a plan must be folded to fit on a paper file, the plan should be copied, the copy placed on file and the original plan stored in dedicated plan storage; and
- Items should not be stored on the top of shelving and cabinets as they will be exposed to excessive light and be vulnerable to water damage from fire sprinklers.

Magnetic media

Magnetic media refers to any record format where information is recorded and retrieved in the form of a magnetic signal. Types of magnetic media that hold the Directorate's records include video and audiotapes, tapes used in digital recording processes, hard discs, and floppy discs.

Magnetic media is not to be stored in paper and cardboard containers as these generate dust. They should be stored in cases made of an inert plastic. Cases should be strong enough to protect these media from physical damage, and they should seal properly.

Cassettes and tapes should be wound to the end of one side after use. They should not be left in a partly wound state for any length of time.

Photographs

Photographic images can be produced from exposed photographic film negatives or from a digital file created by a digital camera. The various formats of modern photographic images create storage and preservation issues.

Photographic images produced electronically must meet current standards for electronic images. If the images are to be published or retained long-term or permanently, they should be created with a minimum resolution and dimensions required by current standards wherever possible and stored in a manner that ensures their ongoing accessibility over time.

Handling and care

The following handling and care requirements are applicable to Directorate records:

- Labels should never be applied directly to photographic material;
- Never write on the back of a photographic print as this will damage the image;
- Metal pins, staples, paper clips, rubber bands or adhesive take should not be used with photographic images;
- Storage and packaging should be in a container of archival quality. PVC sleeves should not be used;
- Prints and negatives should be individually packaged in bags or envelopes designed for the purpose;

- Loose material should be packed in small groups in archival files or folders and then boxed;
- Oversized material should be stored in drawers, folder or boxes suitable for the size of the items;
- Slides should be stored in slide boxes, albums or hanging files made of an appropriate archival quality material;
- X-rays are to be treated as negatives and stored in archival envelopes or plastic sleeves; and
- Electronic images are to be stored in the TIFF format for long-term retention.

7.2: Protection and Security Procedure

7.2.1 Purpose

The purpose of this procedure is to ensure that all records, information and data is protected from inappropriate and unauthorised access. This includes appropriate storage, preservation, security, control plans and adequate retention.

7.2.2 Scope

The procedure relates to all records, information and data.

7.2.3 Responsibilities

All staff, consultants and contractors having access to the Directorate's records, information and data must comply with this procedure.

7.2.4 Background

The Directorate's businesses generate, disseminate, handle, store and dispose of large volumes of records in various formats (e.g. paper, and digital). Therefore, protection and security is the concern and duty of care of every staff member, consultant and contractor.

ACT Government policies on security

The central policy for protective security is ACT Government's Protective Security Policy Framework. It applies across ACT Government and provides a framework for agencies in their approach to the protection and security of people, assets and information in a way that is consistent.

Sensitive information may only be shared with other business units or agencies on a 'need to know' basis and in accordance with and the relevant legislation such as the *Information Privacy Act 2014*, the *Health Records (Privacy and Access) Act 1997* and the *Children and Young People Act 2008*.

Most of the classified material the Directorate manages is 'Sensitive'. Sensitive and private information must be protected against unauthorised access or modification, external disclosure and other forms of misuse. It is essential to assign enforceable and manageable security classifications or Dissemination Limiting Marker (DLMs) to those records, information and data that must be stored with limited access arrangement, such as records with privacy, Freedom of Information (FOI) or commercial sensitivity.

7.2.5 Operational Instructions

The following requirements are to be adhered to when applying security classifications or DLMs to records, information and data:

- The record, information and data is to be classified at the earliest stage possible during creation;
- The security classification is to be record specific;

- A record must not bear a lower classification than the highest classification of any of its appendices or attachments;
- Individual sections and paragraphs may influence classification of the whole record; and
- Each document of a record is to be classified at least as highly as the most highly classified paragraph on that page. The classification of the whole record must be at least as high as its most highly classified page.

Security classifications and Dissemination Limiting Markers (DLMs)

Security classifications or DLMs are be allocated to a record or an individual documents according to the degree of privacy, commercial or legal damage or other sensitive circumstances that might result from unauthorised access or disclosure of the record.

The confidentiality or security status of every record and document is to be established at the time of creation/registration and must be given one of the following security classifications:

Security Classifications:

- **Unclassified**
- **Protected**

Dissemination Limiting Markers (DLMs):

- **For Official Use Only (FOUO)**
- **Sensitive**
- **Sensitive: Personal**
- **Sensitive: Legal**
- **Sensitive: Auditor-General**
- **Sensitive: Cabinet**

Cabinet Documents

Cabinet documents are to be marked **Sensitive: Cabinet**. Sensitive: Cabinet records may have, by their very nature, restrictions on access and special storage requirements and may in certain circumstances require application of a national security classification such as PROTECTED.

The handling requirements for Sensitive: Cabinet are determined by the ACT Cabinet Office and outlined in the ACT Government Cabinet Handbook.

Restrictions on handling classified material

The following restrictions for staff handling highly classified material include:

- Access control devices needed to operate stand-alone photocopiers (e.g. card-key) must be secured when not in use;
- Registers must be maintained for classified photocopying in which the title of the document, its classification, the name of the person who carries out the photocopying and the number of photocopies produced should be recorded;

- Staff must have appropriate security clearances where appropriate; and
- Written approvals must be presented before photocopying of classified material is carried out by the staff of the area.

Physical files bearing "Protected" security classifications are to be stored in locked cabinets when not in use. Copies of classified material should be destroyed by secure means, or placed in an appropriate repository, e.g. the Directorate's Records Management Unit or Shared Services Record Services. Approved methods of destruction are shredding or pulping (secure recycling).

User permissions for digital material

Limited access is the means of restricting access to digital information and is not a security classification.

Access to the corporate recordkeeping system is restricted to Directorate staff and, where appropriate, contractors and consultants. For password and access maintenance users must conform to Shared Services ICT Password Policy.

Passwords are strictly confidential. Directorate staff are subject to disciplinary action by the Directorate and under the *Territory Records Act 2002*, the *Crimes (Offences against the Government) Act 1989* or the *Public Sector Management Act 1994* for unauthorised access to the Directorate's business records or misusing privileged information.

Staff, contractors and consultants must be cleared to the appropriate security level for the records they need to access in order to carry out their duties.

Marking of classified records

All classified paper based records must be clearly marked with the appropriate classification at the top and bottom of each document. The classification is to be placed on a record when it is first prepared to protect all drafts and copies including waste copies.

The classification on photographs, drawings, maps and similar records is to be marked on each record in a position where it will not obstruct or obscure information of images critical to the document's context or authenticity. The classification of photographic negatives, film, microfiche and similarly formatted records is to be marked on the containers.

The classification of removable computer discs, CDs, DVDs, tapes and similarly formatted records is to be visible from the container and, where possible, when opening the contents. The classification must be immediately evident on the screen for any electronic record or on any hardcopy record produced.

Review of classifications

Security classifications are to be reviewed regularly to determine if the classification is still warranted or requires changing.

File security

Directorate staff must ensure the adequate security of all records. Practices to be adopted to ensure the sound protective security management of business information, papers, files and records include:

- Ensuring security classified files are locked away when not in use;
- Ensuring access to security classified files is allowed only to authorised personnel;
- Not showing or passing records to any person not authorised to see or have them;
- Not taking records home; and
- Not leaving records unattended in public work areas, vehicles or public places.

7.3: Storage and Handling Procedure

7.3.1 Purpose

The purpose of this procedure is to ensure that records, information and data are stored so that they are accessible, retrievable and are preserved in good condition for the length of time they are maintained.

7.3.2 Scope

The procedure applies to all records, information and data.

7.3.3 Responsibilities

The procedure applies to staff, consultants and contractors who make, use and/or are responsible for records, information and data.

7.3.4 Background

All Directorate staff must ensure the safekeeping and proper preservation of records, information and data. This includes ensuring records that are held by someone else (e.g. contractors, consultants, outsourced providers e.g. out of home carers) are held under arrangements that provide for the safekeeping, proper preservation and return of the records.

Appropriate storage conditions ensure that records are protected, accessible and managed in a cost-effective way. The purpose served by the record information and data, especially as it relates to the physical form and its use and value will dictate the nature of the storage facility and services required to manage the records for as long as it is needed.

It is important to determine efficient and effective means of maintaining, handling and storing records before they are made and then reassess storage arrangements as the record's requirements change. Storage options must take into account access and security requirements, environmental, technological and physical conditions. This applies equally to digital records when storing in a cloud facility. It is important that records are stored in conditions that ensure that they are accessible and retrievable for the length of time they are retained.

7.3.5 Operational Instructions

The Territory Records Office Standard and accompanying Guidelines outline requirements for the Directorate to ensure the security, storage and preservation of records, information and data to protect the interests of the organisation and the rights of employees, clients, stakeholders and citizens, now and into the future.

Physical storage environment

It is imperative that all paper records are stored in official file covers that have been created using the *Whole of Government Thesaurus* and registered by the Directorate's Records Management Unit Shared Services Record Services or Whole of Government Electronic Document Records Management System (EDRMS).

Directorate paper based files, when not in use, should be stored in lockable containers appropriate for their sensitivity and security requirements. Appropriate access services and controls are to be maintained for stored records. All the Directorate's records are to be stored in cost-effective conditions as appropriate for each record format.

The following are minimum requirements for the storage of physical records:

- The physical environment is to be kept tidy, clean and free from dust;
- Records should not be exposed to direct sunlight and should be kept away from other sources of light and heat as much as is practicable;
- The physical environment is to be kept free of insects and rodents;
- Food is never to be stored or consumed in a records storage area; and
- The records area should be well ventilated.

Any records that include security classifications as described in Procedure 6.2: Protection and Security are to be stored in appropriate locked cabinets when not in use.

Long-term storage areas should not have outside windows, and ultra-violet (UV) filtered lighting should be used. An optimum temperature and relative humidity for records storage will depend on the media being stored. However, air-conditioning should be available in order to maintain a constant temperature and relative humidity. Options for regular fumigation of storage areas should be investigated and applied as appropriate.

The location of the storage area should be in an area where there is minimal risk of damage from natural disasters such as fire, flood etc. For further information on disaster preparedness and recovery refer to Procedure 7.5 Disaster Preparedness and Business Continuity.

Storage of files temporarily not in use

Staff going on leave should transfer all files to the person dealing with those matters in their absence.

Digital environment

The following are minimum provisions to be made for the storage of digital records:

- Digital records and metadata that are still required for either a limited period of time or permanently must be migrated to new systems when upgrades occur; and
- Backup procedures appropriate to the value of records (including the storage of regular backup discs or tapes off-site) are to be identified through service level agreements and implemented by Shared Services ICT.

Endorsed locations

The location of all the Directorate records (digital and paper based) are controlled by compliant recordkeeping systems, including integrated business systems. A list of business systems endorsed to maintain records, information and data locations is outlined in the Directorate's Records,

Information and Data Architecture Register. Refer also to Procedure 3.1 Records Management Program Performance Framework.

All records, information and data must maintain appropriate metadata and ensure security access controls are applied, and digital records, information and data is backed up regularly as part of routine ICT practice.

7.4: Outsourcing Procedure

7.4.1 Purpose

The purpose of this procedure is to ensure that recordkeeping operations and services that are outsourced by the Directorate meet responsibilities and accountability requirements.

7.4.2 Scope

The procedure applies to the Directorate's operations and services that are outsourced internally within government or externally to a service provider. Refer to Attachment D of the Records Management Program for a list of outsourced activities.

7.4.3 Responsibilities

The procedure applies to staff that are responsible for preparing and signing contracts and service level agreements and staff responsible for the Directorate's Records Management Program.

7.4.4 Background

The Directorate may outsource many of its business activities, but not the responsibility or accountability for those business activities. Even when the Directorate outsources a function or activity it still retains ultimate responsibility for the provision of the service.

Therefore, the Directorate is responsible for ensuring that records that belong to the organisation but that are in someone else's possession are held under arrangements that provide for the safekeeping, proper preservation and return of the records.

7.4.5 Operational Instructions

Agreements or contracts controlling outsourcing will:

- Identify classes of records and their owners;
- Bind the third party entity to follow records management controls set by the Directorate, including creation, control, custody, storage, security, ownership, disposal and access;
- Bind the third party entity to abide by the legal disposal provisions of the relevant archival legislation or other instruments;
- Establish an access regime to records held by the third party entity, addressing the interests of the Directorate, compliance authorities (including audit and ombudsman functions) and members of the public in accordance with relevant Freedom of Information, Privacy and other legislation and statutory obligations;
- Define record storage provisions;
- Require that any subcontractor engaged by the third party entity is subject to the same level of compliance with these requirements; and

- Ensure that records are maintained, transferred and disposed of in a controlled manner following completion of the outsourcing contract or agreement.

Planning

Responsibilities for making, maintaining and disposing of the Directorate's records of outsourced functions and activities are to be included in the planning process and subsequent contracts and agreements. This will include clear instructions in the outsourcing contract about:

- The specific or general types of records the contractor must make in carrying out the contract.
- How records are to be maintained by the contractor.
- What records, if any, can be destroyed under the Directorate's Records Disposal Schedules and the method of destruction.
- The types of records that are not to be destroyed if they may be needed for any legal action or inquiry.
- Contract management.

The agreement or contract should include sufficient lead time for records issues to be addressed during the final stages of a contract or agreement. The Directorate must ensure that:

- Records management issues are well monitored during the final stages of an outsourcing contract or agreement and reported to the relevant authority as required;
- There is appropriate sign-off on reports of records management activities at the expiry or termination of an outsourcing contract or agreement; and
- Restrictions on the contractor's use of information in the records must be made clear in the outsourced contract.

A contractor must be made aware of the Directorate's requirements under the *Territory Records Act 2002* and any standards, codes and guidelines produced under the Act.

The Director of Territory Records must be informed about any outsourcing (internal or external) for all or any part of the Directorate records management.

7.5: Disaster Preparedness and Business Continuity Procedure

7.5.1 Purpose

The purpose of this procedure is to ensure that the Directorate has a Records Recovery Plan as part of its Business Continuity Framework to protect and recover records. The Disaster Preparedness Plan provides the Directorate with a detailed set of procedures to follow in the event of an accident, emergency or disaster.

7.5.2 Scope

The procedure applies to all records, information and data. This procedure complements the ACT Government's Shared ICT Business Application Policy for business continuity. This procedure also complements the Directorate's Risk Management Framework and other policy documents concerning business continuity.

7.5.3 Responsibilities

The procedure applies to all staff with the responsibility for the creation and management of records, information and data.

7.5.4 Background

The Directorate's Records Management Programs establishes a regime for the proper care of records, information and data of the organisation, particularly records of archival or enduring value. This includes preservation strategies and disaster prevention and recovery. The Directorate has a Business Continuity Framework in place that outlines processes to be undertaking following a disaster or critical incident. This document complements that framework.

The Directorate also has in place agreements for the provision of recordkeeping services, including storage of records with two service providers. Both providers have established processes in place in the event of a disaster which accords with ACT Government legislation, standards and principles.

7.5.5 Operational Instructions

Preservation strategies

All Directorate staff are to treat records carefully, to implement adequate storage standards and records handling practices, and to use archival quality materials for records expected to have a long life. Preservation of electronic records requires strategies to migrate records to new systems in such a way that the records can be maintained as reliable and authentic evidence over time.

The Directorate and its employees are responsible for preserving records for as long as required by law and business requirements. A major threat to the preservation of records is the risk of disasters, natural or otherwise.

Records that have deteriorated over time or suffered damage by use or through disastrous events may require specific conservation treatments by experts. In some cases conservation may be undertaken by copying records onto another medium such as film or electronic formats. Advice on suitable treatment and on the availability of experts is available from the Directorate's Records Manager.

Risk assessment

One of the key elements to any recovery from a disaster is identifying the possible risks that could cause damage to or loss of records held by an area. These may include:

- Flood;
- Fire;
- Earthquake;
- Mite or insect damage;
- Vermin damage;
- Hard disc failure;
- Backup failure;
- Storage medium failure; and
- Sabotage or other deliberate acts that may damage or destroy records.

This list is not comprehensive but it does identify possible risks that could cause damage to the Directorate's records regardless of format. A comprehensive risk assessment for the Directorate's records is to be carried out as part of any disaster preparedness and recovery program. The Directorate's Risk Management Framework document provides guidance on conducting a risk assessment.

The intention of disaster planning is to be able to restore the operation of the Directorate in an orderly and effective manner in accordance with a plan in the event of an emergency action. That is, the type of emergency that may arise has been considered and assessed, and the best and most cost effective types of prevention and recovery action have been put in place.

A critical component of disaster or contingency planning is prevention. A risk assessment is a vital tool for identifying potential risks to the Directorate's records and forms an important part of disaster prevention. A risk assessment will also aid in the identification of vital records for the purpose of disaster recovery.

The preparation for a disaster includes:

- Assembling and training of a disaster recovery team;
- Identifying and marking of priority material;
- Preparing documentation including local emergency and other service numbers needed in an emergency, lists of staff contact numbers, floor plans, access to keys etc.;
- Providing contact procedures (including out of hours) for the Directorate's Records Manager and other specialist staff, e.g. trained archive personnel and trades people for the supply of equipment and vehicles;
- Access to appropriate equipment, e.g. a refrigerator for saving wet documents;

- Ensuring adequate space and equipment for dealing with an emergency is organised, assembled and maintained; and
- Testing and reviewing the disaster plan on a regular basis.

Disaster Recovery

In the case of a disaster causing significant damage to records, such as a flood, fire or explosion, contact the Records Manager. The Records Manager will assess the situation, recommend a program of action and, upon acceptance of the plan, start recovery action.

Recovery action should be taken to restore the disaster site and materials to a usable condition. The action should include:

- An immediate assessment of damage;
- A decision about the urgency and type of action required. For example, what action is required on site or off site, is immediate action or gradual conservation program required. This decision will be made in consultation with conservation experts;
- Removal of any damaged material;
- Performing conservation action where required; and
- Reviewing performance of the plan and team and upgrade if necessary.

Business units should include development of a business resumption or recovery plan in order to identify the arrangements necessary to resume business activity. The plan should contain the following:

- The names and contact details (including after-hours telephone numbers) of all people/ organisations with responsibility for the implementation of some part of the disaster recovery plan;
- Arrangements for alternative accommodation;
- Arrangements for temporary office infrastructure including office furniture and equipment, telecommunications, and computer equipment;
- Alternative sources for the supply of essential goods and services if contractors suffer a disaster;
- Details of suppliers of essential services and goods which have business resumption plans in case they are also affected by the same disruption that has interrupted the functioning of the Directorate's business; and
- An analysis of the incident needs to be carried out by impartial reviewers, either by outside consultants or a senior management team made up of officers not involved in the disaster event. If this is not possible due to the organisation's size then some of the reviewers should be from other organisations.

A post-incident analysis

Review the business resumption plan whenever:

- A key member of the disaster recovery team leaves the business unit;
- A new Work Health and Safety officer or First Aid officer is appointed; and
- The section or business unit moves location.

Check the contents of your disaster kit every month to ensue all items are in working order and replenish items where necessary.

A disaster prevention and recovery plan sets out the strategies and activities for preventing disasters, for preparing an appropriate response to and recovery from disasters should they occur and for resuming normal business. The disaster prevention and recovery plan is not designed to provide an answer to each and every type of disaster that could happen, but rather is provided to identify the methods on how to recover from a disaster if one were to occur.

The disaster prevention and recovery plan will define the roles and responsibilities of staff, what other resources will be required, the location of backups, how the plan is to be implemented etc.

Copies of Disaster Prevention and Recovery Plans for the Directorate's internal and outsourced providers is available by contacting the Directorate's Records Manager at CSDRMU@act.gov.au.

7.6: Vital Records, Information and Data Procedure

7.6.1 Purpose

The purpose of this procedure is to enable Records Manager / Records Management staff to ascertain what records of the organisation are considered vital to inform disaster preparedness and business continuity.

7.6.2 Scope

The procedure ensures identification, protection and preservation of records of the organisation that are considered vital to inform disaster preparedness and business continuity.

7.6.3 Responsibilities

The procedure applies Directorate's Records Manager / Records Management Unit staff, and any contractors or consultants undertaking recordkeeping functionality on behalf of the Directorate.

7.6.4 Background

The Directorate is responsible for a wide range of Human Services functions in the ACT. These functions include services for: Children, Youth and Family Support; Multicultural Affairs and Community Development; Aboriginal and Torres Strait Islander Affairs; Public and Community Housing; Supported Accommodation; Homelessness; Disability; Therapy and Community Services and Child and Family Centres. The Directorate has policy and procedures embedded in Business Continuity Plans for its critical functions and ICT systems, all of which form part of the organisation's Business Continuity Framework. This document complements the Directorate's policy and procedures which outline the organisation's framework. In the event of a disaster, it is critical for business continuity and for re-establishing the operations of the Directorate that vital records or a copy of them is preserved.

Although all measures are taken to prevent accidents and disasters, such as off-site backup of discs and digital records, essential preparation must be undertaken to ensure vital records are preserved. Vital records planning is one part of disaster prevention and recovery planning. It may be useful to think of a vital records program as the preparation required in trying to prevent damage in the event of a disaster, as opposed to restoring business operations once damage has been done.

7.6.5 Operational Instructions

All business functions performed by the Directorate are important, with some being critical for the welfare of our clients and for compliance with legislation. The Directorate has established an agreed system of assigning levels of criticality to business activities to assist in business continuity processes.

The following describes categories and definitions for critical business activities for use within the Directorate:

Category 1: Activities that cannot be left for more than 48 hours, during an extreme disruption event, or the clients or organisation will suffer irreparable/severe damage – i.e. those critical

activities with a “drop dead deadline”. This category also includes processes that assume this level of criticality at specified times throughout the week/month/year.

Category 2: Activities that cannot be left for between 2 and 10 working days, during an extreme disruption event, without causing severe damage to clients or the organisation.

Category 3: Activities that, while important for the organisation, do not have the same significant impact if not undertaken for more than 10 days during a significant disruption event.

From a recordkeeping perspective, vital records can be identified as any record that details the Directorate’s interaction with a client or citizen. Vital records includes records of the following business units, as well as records of defunct areas:

- Child Youth and Family records, in particular Adoption, Care and Protection and Youth Justice records
- Housing ACT including – citizen and property files
- Disability ACT client files (defunct
- Therapy ACT client files (defunct)

Whilst the Directorate business systems (CMS formerly CHYPS, YJIS, HomeNet) will contain relevant information to vital records they cannot however, reproduce the complete content of a physical file. The Directorate’s recordkeeping system (HPE CM9 also known as TRIM) is also considered a vital controlling record that facilitates access and retrieval to vital controlled records.

There are measures which can protect vital records in the event of disaster. These can include:

- Fire proof storage;
- Closing compactus at night (to limit the spread of fire);
- Duplication; and
- The remote storage of back-up data including portable storage devices.

Some of the Directorate’s vital records may already be in electronic form, so they can easily be duplicated and held at a remote location.

Assessment of the likelihood of particular types of disaster and the most cost effective means of preventing them must be made. Once the cost of different levels of protection against the cost of potential loss of records has been made, decisions about protection methods can be made.

It is appropriate for the Records Manager, in conjunction with each business unit to assess for business continuity planning, vital records that are critical for the achievement of the Directorate’s objectives. Business unit managers are responsible for assessing business continuity risks and for planning for the continuity of business processes or services that are under their control. For planning purposes it is essential that the Directorate has identified the location and whereabouts of all its records. The following table identifies where the Directorate’s paper-based records are stored:

Location (internal)	11 Moore Street	Ground floor file room and compactus
		Various compactus on various floors
	NCH (Housing ACT)	1st floor compactus
Location (External)	Mitchell – (Shared Services Record Services)	Building 6/7 - 9 Sandford Street Mitchell

	Hume (The Information Management Group)	Hume – 10 Sleigh Place Hume
Format / Quantity	Paper-based files	250,000
	Electronic	CMS (formerly CHYPS & YJIS) and HomeNet

Strategies for protecting vital records include:

- Copies of the original records may be made and dispersed to a different part of the Directorate or to an off-site storage facility. Any storage locations must meet the records management storage standard requirements.
- Originals or copies may be lodged with Shared Services Record Service or with an approved commercial storage company.
- The Directorate may also hold various copies of important vital records in business systems such as CMS (formerly CHYPS) & YJIS) and HomeNet.

Vital protection records

Vital records protection is one part of disaster prevention and recovery planning. It may be useful to think of a vital records program as trying to prevent damage in the event of a disaster and disaster recovery is trying to restore business operation once damage has been done.

Vital records are defined as "those records that are essential for the ongoing business of the organisation and, without which the organisation could not continue to function effectively". Therefore, they are records that are necessary to re-establish the organisation in the event of a disaster. Vital records include records essential for the:

- Resumption and/or continuation of operations (including records which are needed to conduct emergency operations during a disaster);
- Re-creation of the legal and financial status of the business unit; and
- Fulfilment of obligations to ACT Government and outside interests.

For example:

- the Directorate's disaster management or business continuity plan;
- employee details, including contact information;
- delegations of authority;
- current customer and stakeholder records or registers;
- contracts, titles, and other signed original legal records;
- licences, leases, permits which enable the Directorate to operate or perform a particular action;
- insurance records;

- financial information e.g. current or unaudited accounting records;
- infrastructure plans, operational policies and procedures;
- records relating to current or potential litigation; and
- records protecting the legal and financial rights of those clients the Directorate is responsible. This includes Child Youth and Family client records, and citizen records of Housing ACT.

In the event of a disaster, it is critical for re-establishing the operations of the Directorate that these records or a copy of them is preserved. Although all measures are taken to prevent accidents and disasters, such as off-site backup of discs and electronic files, it is worth some preparation to ensure vital records are preserved.

8 - ACCESS PRINCIPLE

8.1: Access to Records, Information and Data Procedure

8.1.1 Purpose

The purpose of this procedure is to ensure public access to the Directorate's records, information and data under the provisions of the *Territory Records Act 2002* (TRA).

8.1.2 Scope

The procedure applies to all records, information and data subject to the TRA and the *Freedom of Information Act 2016 (FOI Act)*.

8.1.3 Responsibilities

This procedure applies to all staff to help to facilitate the public's access to Territory records information and data, when appropriate. The Directorate's Records Manager and Records Management Unit are responsible for coordinating access to the Directorate's records in response to requests made through Archives ACT. The Directorate's Information Officers and Freedom of Information Unit are responsible for coordinating access to Directorate records in response to requests made under the FOI Act. This includes responding to requests from Cabinet Office for advice on the release of Executive records.

8.1.4 Background

The FOI Act provides members of the public with a right of access to ACT Government records and information that are less than 20 years old. The TRA, *part 3: Agency Records-Access* provides members of the public with a right of access to ACT Government records that are more than 20 years old.

The relationship between the TRA Act *and the* FOI Act ensures a consistent and principled approach to public access to records.

The Directorate must therefore manage its records in accordance with the Territory Records Office Standard for Records, Information and Data to ensure the information remains accessible over time. This includes:

- Responding to requests for access in a timely manner;
- Migrating electronic records to ensure that information is accessible in a current system;
- Providing finding aids to records;
- Ensuring that unauthorised destruction of records does not take place;
- Providing a secure storage environment to prevent loss or damage; and
- Conserving records.

The Access provisions for Cabinet Records are outlined in section 31B of the TRA. Access to Cabinet Records is coordinated by the Cabinet Office and can be released for public access after ten years. Furthermore, section 16(2)(i) of the TRA requires the Directorate to make arrangements for

preserving records containing information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

Records will be made available for access unless they belong to a category of record that is exempt from access. See Procedure 8.4 for exemptions

8.1.5 Operational Instructions

The Directorate will comply with the Territory Records Office Standard for Records, Information and Data by embedding the following into business processes and organisational culture:

- Encouraging openness of records, information and data: The Directorate will promote a culture of openness in relation to its records, information and data. This includes developing policies and practices that do not unnecessarily restrict access, either by the public or by other areas of government.
- Ensuring records, information and data can be found, accessed, used and re-used when appropriate: The Directorate will plan and implement strategies to ensure records, information and data are made, managed and preserved in accessible formats for as long as they are required by Government or the community.
- Enabling appropriate public access: The Directorate will establish open, equitable and consistent mechanisms to support members of the public to exercise their rights to access records, information and data.

Open Access Information Scheme

The new FOI Act commenced on 1 January 2018 and introduces an open access regime that ensures regular disclosure of certain categories of government information. An ACT Government website was created to support a pro-disclosure culture by providing a central, searchable interface to enable the community to access government information. The Directorate will progressively make open access information available through this website. Find out more about Open Access Information

Other records not identified through the Open Access Information Scheme may be available for public access under the provisions of the *FOI Act 2016*.

The Directorate's instructions relating to the publication of information under the open access scheme can be found on the Intranet website - http://incommunityservices/Governance/Pages/Open-Access-Information-Scheme.aspx.

Records older than 20 years

ACT Government has a common access point for Territory Records under the provisions of the *Territory Records Act 2002*. The initial requests for access to ACT Government records should be made via Archives ACT. The Directorate's Records Manager will respond to requests for access to records from Archives ACT.

Most records older than 20 years are automatically open to the public. However, there are some records that are exempt from public access by a declaration of the Director of Territory Records.

The Directorate's instructions relating to facilitating archives access requests can be found on the Directorate's Intranet and a master copy is also in the recordkeeping system CSD-2018/000085 - RECORDS & INFORMATION MANAGEMENT - Policies & Procedures - Application for access to records requests from Archives ACT Guidelines – 2018.

Register of 28 declarations

The Directorate must maintain an up-to-date Register of Section 28 Exemption Declarations of all records and classes of records that are exempt from public access in accordance with the *Territory Records Act 2002*. In conjunction with the Register, the Directorate's recordkeeping system will also be notated to indicate a record, or class of records are exempt. The Records Manager is responsible for maintaining the section 28 register.

The Register of Section 28 Declarations must include:

- Sufficient detail to identify the records which have been exempted;
- A copy of or reference to the Directory of Territory Records declaration; and
- The date of the decision.

A review of the register is to be completed on a regular basis and not less than every five years. In accordance with TRA, these exemption are maintained in a register of classes of records that are exempt from access.

Copyright

The ACT Government owns the copyright of records created by the Directorate as a result of its business activities. Copyright in records held but not created by the Directorate, (e.g. letters written by members of the public to the Directorate's Business Units) will normally be owned by the creator of the item.

It is to be made clear to clients that the provision of copies of records does not constitute any copyright permission or signing over of any rights in records. Written permission is required from the copyright holder to publish any information from Territory records or any research arising out of access to the Directorate's records. It is the responsibility of the person wishing to publish to obtain permission from all copyright holders.

8.2: Protection of Aboriginal or Torres Strait Islander Heritage Procedure

8.2.1 Purpose

The purpose of this procedure is to ensure the identification, protection and preservation of records containing information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

8.2.2 Scope

The procedure ensures identification, protection and preservation of records containing information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

8.2.3 Responsibilities

The procedure applies to all staff as well as the Directorate's Records Manager / Records Management Unit staff, and any contractors or consultants undertaking business on behalf of the Directorate.

8.2.4 Background

The ACT Government's response to the *Bringing Them Home Report* included a commitment to assist indigenous Australians to trace links to their families and communities. This requirement is to aid in the fulfilment of that commitment.

The Report noted that individual records containing name and family information about Indigenous people that could potentially assist in family reunion may be discovered serendipitously from time to time. The Directorate procedures must therefore include arrangements for preserving such records where they exist or are discovered. Business units are advised to contact the Records Manger to discuss any records that they may need to be preserved for such purposes.

In addition, section 16(2)(i) of the *Territory Records Act 2002* also requires the Directorate to make arrangements for preserving records containing information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

8.2.5 Operational Instructions

A specific *Records Disposal Schedule (RDS)* has been developed to assist the Directorate in identifying and preserving Aboriginal and Torres Islander heritage.

This RDS takes precedence when information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage is found during sentencing process using another RDS.

Where a record has been identified that may establish links with their Aboriginal or Torres Strait heritage, the record is to be retained under the specified RDS. The record is also annotated in the notes field in the Directorate's digital recordkeeping system to show it has been identified and therefore preserved.

Directorate records relating to any of the following are to be retained:

- Records identifying an Aboriginal or Torres Strait Islander by name.
- Records providing genealogical data that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.
- Records providing social data, (e.g. Longitudinal Studies, Linguistics studies, hospital morbidity tabulations), that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.
- Records providing cultural data, (e.g. records relating to artefacts, translation and interpretation of Aboriginal or Torres Strait Islander art) that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.
- Records providing environmental data, (e.g. studies into animals and plants, including food and medicine) that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

The Directorate must not dispose of any records where it is aware of possible legal action for which the records may be required as evidence or if there is a current records disposal freeze in effect. This includes cases pending or already lodged at the National Native Title Tribunal, the Ngambra Circle Sentencing Court or the Jervis Bay Court.

8.3: Public Access to the Directorate's Records Management Program Procedure

8.3.1 Purpose

The purpose of this procedure is to assist the Records Manager / Records Management Unit staff or trained staff to provide either a full or abridged copy of the Records Management Program to members of the public.

8.3.2 Scope

The procedure ensures the Directorate's Records Management Program is accessible for public access.

8.3.3 Responsibilities

The procedure applies to Directorate's Records Manager / Records Management Unit, or trained staff.

8.3.4 Background

In accordance with section 21 of the *Territory Records Act 2002*, the Directorate must make its Records Management Program available for public inspection without charge. The Program as approved by the Director-General (as Principal Officer) consists of a Policy Statement, Records Management Procedures, including a comprehensive list of authorised Records Disposal Schedules and a Records, Information Data Architecture Register. The Directorate's Records Management Program must also accord with the Territory Records Office Standards and Guidelines. This procedure complements ACT Government's Web Accessibility Policy and Standard so that records, information and data is easy to understand and accessible by all people, regardless of age, ethnicity or ability.

It should also be noted that, in accordance with section 16(2) (i) of the *Territory Records Act 2002* the Directorate must also outline in its procedures, arrangements for preserving records containing information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage.

8.3.5 Operational Instructions

The Directorate's Records Management Program is available via a number of sources including the Open Access Information Scheme portal. To facilitate this access, an ACT Government website was created to support a pro-disclosure culture by providing a central, searchable interface to enable the community to access government information. More information is available via the following website. Find out more about Open Access Information.

The Program is also available via the Directorate's website www.communityservices.act.gov.au

Alternatively, members of the public may contact the Records Manager on telephone 62054804 or email CSDRMU@act.gov.au to make arrangements to obtain a copy of the Directorate's Records Management Program.

8.4: Public Access to Records, Information and Data and Access Exemptions Procedure

8.4.1 Purpose

The purpose of this procedure is to help all staff understand which types of records, information and data are accessible under access provisions of legislation and what exemptions can be applied to government information if considered unsuitable to be released into the public domain.

8.4.2 Scope

The procedure outlines which types of records, government information and data are accessible under access provisions of legislation and what exemptions are in force if deemed not in the public interest to release.

8.4.3 Responsibilities

The procedure applies to all staff to help to facilitate public access to Territory records, information and data where appropriate. The Records Manager and Records Management staff, are responsible for coordinating access to the Directorate's records in response to requests made through Archives ACT. The Directorate's Information Officers, and Freedom of Information Unit staff responsible for coordinating access to Directorate records in response to requests made under the *Freedom of Information Act 2016.*

8.4.4 Background

The Directorate's Information Management and Governance Framework provides for access to records information and data, as legislated by the *Territory Records Act 2002*, *Freedom of Information Act 2016*, *Information Privacy Act 2014* and the *Health Records (Privacy and Access) Act 1997*. The ACT Government framework relating to public access to records, information and data is governed by provisions and processes outlined in various Acts.

8.4.5 Operational Instructions

The *Freedom of Information Act 2016 (FOI)*, enables the ACT Government to adopt a pro-disclosure culture. The FOI Act has changed the way the Directorate responds to FOI (access applications) requests and makes available through publishing the information requested when not personal affairs. FOI applies to all records, information and data 20 years older or younger.

The Directorate's procedure for responding to FOI requests can be found here. All records are subject to a public interest test before disclosure and publication. Some information is taken to be contrary to the public interest to disclose if it falls within one of the following 15 categories

- Information disclosure of which would be contempt of court or Legislative Assembly etc. (s 1.1)
- Information in possession of a court or tribunal (s 1.1A)
- Information subject to legal professional privilege (s 1.2)
- Information disclosure of which is prohibited under law, including (s 1.3)
- Sensitive information (s 1.4)
- Information in possession of Auditor-General (s 1.5)
- Cabinet information (s 1.6)
- Examinations under Australian Crime Commission (ACT) Act 2003 (s 1.7)

- Information in possession of Human Rights Commission (s 1.8)
- Identities of people making disclosures (s 1.9)
- Information relating to requests to cost election commitments (s 1.10)
- Information in electoral rolls and related documents (s 1.11)
- Information in possession of Ombudsman (s 1.12)
- National, Territory or State security information (s 1.13)
- Law enforcement or public safety information (s 1.14)

FOI Information Officer (decision maker) needs to justify their decisions to not release information and must record the exemption in the Directorate's Disclosure Log. For further Directorate policy and procedures related to FOI information can be found here.

Access to Archival Records Under Part 3 of the Territory Records Act

All ACT Government records (both physical and digital that are 20 years old are available for public access upon request to Archives ACT. The Directorate will take all reasonable steps to assist with the request and answer within a reasonable time. In some circumstances, some records may be exempt from public access as approved by the Director of Territory Records.

How and when to seek a Section 28 exemption under the TRA

In the event of an Archives access request, the FOI team and the Directorate's Records Management Unit may identify classes of records that are subject to restricted access and publication under authorised exemptions of the *Territory Records Act 2002* (TRA). The Records Manager in consultation with the FOI unit must make an application to the Director of Territory Records for an approved exemption.

The Director of Territory Records may declare a record or class of records older than 20 years to be records which are exempt from release. Exempt categories are:

A. the disclosure of the record would, or could reasonably be expected to—
    I. endanger the life or physical safety of a person; or
    II. prejudice law enforcement; or
    III. unreasonably disclose information about any person (including a deceased person); or
    IV. be a contempt of court or the Legislative Assembly; or
B. the record is subject to legal professional privilege.

Where a record to which an exemption declaration applies under the TRA, the record can be requested under the FOI Act. The Directorates FOI procedures apply and can be found here.

Records examination by the Records Manager and FOI Unit

The Directorate's FOI Unit should review the requested records and make sure there are no documents that contain information deemed to be contrary to the public interest to release under FOI Act including sensitive records as defined in the Children Young People Act 2008, or the Housing Assistance Act 2007, taking the following into account:

- The need to protect personal information is diminished after 20 years. For example, names and addresses of housing tenants can be released after 20 years.
- Look for personal information of a private nature relating to particular incidents involving the person. For example police involvement or child protection issues.

In the event that a record is likely to continue to be sensitive in nature, the Director of Territory Records may approve the section 28 declaration. When the Director of Territory records has declared a record to be exempt, the Directorate will clearly mark relevant documents on the file/s and the Directorate's recordkeeping system as they are processed. The Directorate will notify Archives ACT of the exemption and include the details of the exemption (for example, the function and activity and/or class numbers, reason for exemption and the exemption number) in a minute to the Archives ACT and save all documents on to the Directorate's recordkeeping system.

To check the section 28 Declarations currently in place, see Directorate's website. There is also a master copy in the recordkeeping system – record container CSD-2018/000056 - RECORDS & INFORMATION MANAGEMENT - Information Access & Use - Register of records exempt from public access under section 28 of the Territory Records Act 2002.

The Territory Records Office maintains a copy of all ACT Government exemptions which can be found on their Territory Records Office intranet site.

Information Privacy Act (IPA) 2014

The IPA regulates how personal information is handled by ACT government entities and includes an individual's access to and correction of that information.

The Territory Privacy Principle 12 and 13 articulate rights for individuals to access and correct their personal information. The Directorate's instructions regarding IPA can be found on the organisation's website.

Section 59 of the FOI Act also highlights how a person can make a request to the Directorate to consider amendment to personal information.

Health Records (Privacy and Access) Act 1997

Health records created by any ACT Health facility are confidential documents and remain the property of ACT Government. Requests for health information which the Directorate is a record holder can be requested from the FOI Unit. Copies of health records are not released to consumers or third parties without a written request and signed authorisation from the consumer. Requests to access health records are assessed under the ACT Health Records (Privacy and Access) Act 1997. Fees may apply.

ACT Health and the ACT Human Rights Commission provide guidance and advice on how to gain access to health records. Information for record keepers and information for consumers of health services in the ACT can be found on the ACT health website. The Directorate's policy and procedures relating to access to health records can be found on the Directorate's website .