



ACT
Government

Community Services

Records, Information and Data Management Policy

Records Management Program

JUNE 2018

ACT GOVERNMENT
GPO BOX 158 Canberra City

COMMUNITY SERVICES DIRECTORATE - RECORDS, INFORMATION AND DATA MANAGEMENT POLICY

Policy title: Records, Information and Data Management Policy

Published: 2018

Legislation: *Territory Records Act 2002*

Purpose

This policy, authorised by the Director-General as Principal Officer, in association with the Chief Information Officer forms part of the records, information and data management framework for the creation, capture and management of records, information and data of the Community Services Directorate (the Directorate).

This policy, along with supporting procedures, business tools and systems, training and communication strategies are essential elements of the records, information and data management framework.

Scope

This policy applies to all full-time and part-time staff, volunteers, consultants, contractors and outsourced providers.

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

Policy statement

Information, data and records are vital corporate assets and their management is the responsibility of all who work directly and indirectly for the Directorate.

This policy provides the basis for how the Directorate and its employees can adhere to legislative and better-practice requirements for records, information and data, including what is outlined in:

- the Territory Records Act 2002;
- the Directorate's Records Management Program;
- the Standard for Records, Information and Data;
- various guidelines to implement the Standard for Records, Information and Data; and
- international standards.

The Directorate and its employees must make, keep and manage full and accurate records, information and data in a timely manner to support business needs, government accountability, legal and regulatory obligations, community expectations and historical purposes.

The Directorate is committed to the proper management of records, information and data as mandated by the *Territory Records Act 2002* and will ensure records, information and data are retained for as long as required in a readily accessible form.

This policy should be referenced within most organisational policies and procedures to ensure its application is widespread and consistent.

Definition of records, information and data management

Records are information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or in the course of conducting business. Records, information and data management covers, but is not limited to, the creation, keeping, protection, preservation, storage and disposal of, and access to, records of the organisation.

Information, data and records management processes may be applied by all full-time and part-time staff, volunteers, consultants, contractors and outsourced providers as part of their duties. Some processes are solely carried out by the records manager and/or Records Management Unit.

Responsibilities for records, information and data management

Every employee

All staff are responsible for the creation and management of records, information and data about the work they perform for the organisation. Additional responsibilities also exist for certain categories of staff as outlined below.

Principal Officer

The Director-General as Principal Officer is ultimately responsible for the management of records, information and data, has authorised this policy, promotes compliance with this policy, delegates responsibility for records, information and data management to [name of position] (for example, SES, Senior Manager) and ensures the Records Management Program is adequately resourced.

Chief Information Officer

The Chief Information Officer is responsible for the active support of, and adherence to, this policy by promoting a culture of compliant records, information and data management, and overseeing the development and currency of strategic documents such as the Records Management Program, Records Management Procedures, Records, Information and Data Architecture Register, and Information Management plans.

Records Manager and/or Records Management Unit

The Records Manager and/or Records Management Unit are responsible for implementing and monitoring legislative and better-practice requirements for records, information and data, including the Records Management Program, this policy and organisational capabilities. An important aspect includes the identification of records, information and data management requirements, and the development, implementation and support of records, information and data procedures.

ICT professional staff

ICT staff, including Shared Services ICT staff, are responsible for maintaining the technology for business systems, including appropriate system accessibility, security and back-ups. ICT staff should

ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy, particularly in terms of the retain principle (outlined below).

Security advisor

The security advisor provides advice on security policy and guidelines associated with the management of records, information and data.

Managers and supervisors

All managers and supervisors are responsible for ensuring their staff, consultants, contractors and outsourced providers are aware of and follow their responsibilities for records, information and data management. This includes addressing records, information and data management during performance review discussions and when establishing job roles and contracts, and ensuring the Records, Information and Data Management Policy is followed. They should also advise the Records Manager and/or Records Management Unit of any changes in the business environment, such as new areas of business or the planned de-commissioning and procurement of business systems.

Volunteers, contractors, consultants and service providers

Volunteers, contract staff, consultants and service providers must create and manage records in accordance with this policy and supporting procedures.

Information, data and records management principles

The Directorate's Information, data and records will be managed according to the principles outlined in the Standard for Records, Information and Data released by the Director of Territory Records.

Refer to the Standard for Records, Information and Data and the associated guidelines in applying these principles.

Legislation and Standards

All Government organisations must comply with a range of laws related to the creation and capture of records, information and data.

Specific

Aboriginal and Torres Strait Islander Elected Body Act 2008

Adoption Act 1993

Children and Young People Act 2008

Community Housing Providers National Law (ACT) Act 2013

Disability Services Act 1991

Housing Assistance Act 2007

Native Title Act 1994

Working with Vulnerable People (Background Checking) Act 2011

General

Territory Records Act 2002

Freedom of Information Act 2016

Evidence Act 2011

Discrimination Act 1991

Human Rights Act 2004

Information Privacy Act 2014

Health Records (Privacy and Access) 1997

Electronic Transactions Act 2001

Public Sector Management Act 1994

Financial Management Act 1996

Work Health and Safety Act 2011

International and Australian standards

Standards help guide the organisation in performing its functions. The Directorate operates in line with numerous standards, regulations, schemes, notifications, directions, delegations and memorandums that relate to the areas of responsibility.

Records management specific

AS ISO: 15489 – Standard on Records Management

SA/SNZ TR ISO: 26122 – Work Process Analysis for Recordkeeping

AS: 5044 – AGLS Metadata Standard

AS/NZS 5478:2015 Recordkeeping Metadata Property Reference Set

ISO: 16175 – Principles and Functional Requirements for Records in Electronic Office Environments.

Associated policies

A range of policies relevant to the management of records, information and data must be applied alongside this policy, including:

- ACT Government's Code of Conduct;
- ACT Government's Code of Ethics;
- ACT Government's Open Government Policy; and
- ACTPS Digital Records Policy.

Administrative directions of government

A range of Government-wide administrative directions associated with the management of records, information and data must be applied alongside this policy, including:

- Open Access Information Scheme; and
- Protective Security Policy Framework.

Endorsed locations

Only endorsed locations can be used to store records, information and data to ensure their appropriate management.

For locations to be endorsed, they must be registered with the Records Manager and/or Records Management Unit (forming part of the Records, Information and Data Architecture Register) to help ensure appropriate Records Management processes can be applied and, where appropriate, supported by the development of information management plans.

Endorsed locations include:

- Shared Services Record Services ;
- *The Information Management Group (Databank);*
- *ACT Government authorised, and/or endorsed Cloud locations; and*
- *Approved Outsourced Providers.*

Locations that are not endorsed include:

- email accounts;
- C-drives on PCs;
- portable devices;
- unapproved commercial storage facilities; and
- *Personally owned computers and devices.*

Contact the records manager and/or records management unit for the endorsement of locations.

Ownership

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

Procedures for records, information and data management

This policy is supported by the Records, Information and Data Management Procedures and forms part of the broader records, information and data management framework.

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

The records manager and/or records management unit are responsible for coordinating the development of procedures for these processes.

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

Feedback about this policy

Where there are questions or concerns regarding this policy, its application or how it relates to other policies or directives, contact:

Kevin Knudsen
Records Manager
62054804

Review of this policy

This policy was endorsed by the Director-General as Principal Officer in June 2018 and will be reviewed at least every five years or as required (such as after significant administrative change).