Records and Information Management – Responsibilities of Senior Managers

Purpose

This document forms part of the framework for the creation, capture and management of ACT Government records, information and data. It is designed to provide senior managers responsible for recordkeeping with a consistent approach to promoting compliance with the *Territory Records Act 2002* (the Act).

Context

The Act requires ACT Government agencies to comply with standards and codes for records management approved by the Territory Records Office (TRO). The TRO's *Standard* and *Guidelines for Records, Information and Data* underpin the operation of the records and information management framework in the ACT Public Service and require agencies to designate a single, identified senior manager, usually at the Senior Executive level, who is responsible for delivering the organisation's Records Management Program.

Scope

This document sets out the activities and outcomes that designated senior managers must ensure are achieved in their agencies as part of that Program.

Organisational Outcome

Strong recordkeeping culture and performance is vital in supporting ACT government business processes as well as the broader ACT community through accountable and accessible government. By applying the seven principles of the Standard on Records, Information and Data, an organisation will be well positioned to comply with its recordkeeping obligations and to perform its organisational records information data management functions efficiently and effectively.

Information, data and records management principles

ACT Government information, data and records must be managed according to the principles outlined in the Standard released by the Director of Territory Records.

Senior Manager Responsibilities

ACT Government designated senior managers are responsible for ensuring records, information and data management practices within their organisation align to these principles so that business requirements and community expectations are met.

While all staff are responsible for the creation and management of records, information and data about the work they perform for the organisation, senior manager responsibilities ensure that the organisation has resources, including professional skills and knowledge, in place to promote compliance and enhance performance.

The information below can assist senior managers to understand their role by setting out the key actions agencies must undertake in response to each of the records, information and data management principles.

Note: 'Information Governance' is used in the document to encompass all records, information and data management.

Description	Senior Officer Responsibilities	Tasks Performed in the Agency
The Strategy Principle seeks to establish and support an organisation-wide plan for achieving a robust state of records, information and data management.	• **Ensures the agency has a complete, approved and implemented Records Management Program (RMP).** The RMP comprises of four core parts which must reflect the operations and practices of the agency. The agency Records Manager is responsible for the development of the RMP, the agency ICT Manager, and agency Security Advisor, the agency information privacy officer, the agency FOI coordinator must be informed and consulted during the development. • **Ensures the agency has or has plans to adopt and implement Whole of Government initiatives related to records, information data**. • **Promotes the importance of information governance and supports information as an asset.**	• Records, information and data management planning • Documenting records information and data management policies and procedures • Development and maintenance of strong records information and data management culture through awareness and promotion campaigns and other appropriate channels

The Capability Principle seeks to establish, monitor and improve the agency's information governance knowledge and ability through a supported learning and development program. The Capability principle aims to ensure that an organisation has skilled resources and enough funding to support its strategic and tactical records, information and data management operations.

- **Ensures the agency has access to sufficiently skilled staff for information governance.** The agency must have access to the advice and services of an Information Governance professional. The Act requires an agency to demonstrate it has enough resources to support and improve the agency's records, information and data management requirements and develop maturity.
- Position Descriptions must include relevant records, information and data management skills and knowledge for the position.
  - o Large agencies and Directorates should generally have a full-time dedicated Information Governance manager at the SOGC level or above.
  - o Smaller agencies may assign Information Governance tasks at a suitable level to one or more staff members who also carry out other functions.
  - o Where only junior staff are assigned Information Governance tasks the agency should expect to engage professional records and data management advice through consultants or contractors from time to time, such as when:
    - developing, implementing and reviewing a RMP,
    - developing or reviewing a records disposal schedule or
    - developing or acquiring business systems that will create and use ACT Government records, information and data.

- Conducting induction and refresher training for all staff on records, information and data management responsibilities
- Establishing assigning and maintaining designated Information Governance roles
- Supporting ongoing professional development for Information Governance staff
- Budgeting for records information and data management activities
- Monitoring and reporting on records information and data management activities and performance

- **Ensures the agency has financial resources available for performing and undertaking records, information and data management activities.**
  The agency should understand how much is spent on records, information and data management, and, for budget purposes, what activities are included in managing the agency's records, information and data requirements.

- **Ensures the agency has a training plan for records, information and data management.**
  The agency must have a training plan for records, information and data management for agency staff. This will include at minimum, induction training (highlighting the roles and responsibilities of records, information data management stakeholders within the ACTPS) and basic training on records, information and data management specific to the agency's operations (for example EDRMS basics).

The agency's designated Information Governance Professionals must have access to continuing professional development opportunities. As a guide, records managers should have or obtain relevant qualifications or equivalent experience at the diploma or degree level. Other records management staff should have or obtain qualifications or equivalent experience at the Certificate III or IV level.

The Assess Principle seeks to establish processes and tools that help an organisation to understand its business

- **Ensures the agency has authorised and up to date records disposal schedules applicable to all its business activities.**
  An analysis of business process and activities, including legislative and regulatory requirements and community

- Appraisal of agency business processes and activities to

activities and the evidential and recordkeeping requirements that arise from them. Compliance with the Assess Principle should result in the development of tools such as Business Classification Schemes and Records Disposal Schedules that inform responses to other requirements such as security, privacy and open government principles.

expectations, helps an agency to understand its information management requirements as well as what information it generates and how it is used to support business practices and community memory. Records Disposal Schedules also consider and reflect the risk profile of the agency by identifying retention periods and destruction expectations for the agency's records, information and data.

- **Ensures records, information and data that have identifiable factors for higher consideration** (such as significance, risk, security, and privacy) **are kept on ACT Government premises, in authorised locations and managed as per policy requirements.**
  This understanding helps to inform a range of business information management requirements and practices (such as storage, handling, sharing and access).

- **Ensures there is a formal, defined process for introducing new records and data-generating systems, as well as documented processes used to upgrade and or decommission business systems.**
  Policy and procedures exist within the agency for the acquisition of business systems that include assessment and identification of core metadata elements of the business system. Each business system is captured in the Architecture Register and has an information management plan.

The Describe Principle seeks to establish a process that enables the description of records, information and data in the organisational context. The Describe

- **Ensures business systems, whether they are purpose built to manage records** (such as an electronic document records management system [EDRMS]) **or are developed to perform some other function** (such as a client management, case management, finance or human resource system) **are designed so they include specific metadata elements to**

establish recordkeeping requirements
- Development of business classifications schemes
- Development and approval of records disposal schedules
- Development and commissioning of records-capable business systems

- Development and application of controlled naming conventions for unstructured information in records and other business systems (See Assess principle).

principle helps to ensure that information and information systems are discoverable, searchable and reliable, through standard described metadata and tools (such as a business systems architecture register and information management plan). The describe principle, ensures actionable, consistent and relevant control of an enterprise information ecosystem.

efficiently meet the business needs and ongoing system integration requirements, and with details documented and reviewed at a business specified period.
This means business system owners have involved and included agency Information Governance professionals in the planning for and development of a business system to ensure appropriate understanding, description and control.

- **Ensures the describing metadata elements of a system** including its records, information and data, are managed appropriately so the authenticity, usability and reliability of the information asset is fit for purpose, understood and protected.

- Classification of business systems data, records and documents according to a business classification scheme (see above) so that their context and significance can be understood

- Development and implementation of audit logs and other metadata schemas that make information discoverable and understandable and document its use

- Documentation of the management and use of business systems and the records and data they contain

- Preservation of metadata about obsolete systems and destroyed records

The [Protect principle](#) seeks to enable organisations to identify and apply appropriate protection measures and mechanisms to their records, information and data and information

- **Ensure that the agency has identified records, information and data protection requirements.**
Agencies that understand their records, information and data assets can apply controls around information security (such as privacy, and PSPF) to ensure integrity, usability and completeness is retained.

- Designation, monitoring and maintenance of endorsed storage locations for both hard copy records and digital records and data

systems, based on the assessed requirements. ACT Government organisations must have documented processes to support the appropriate security, storage and preservation of their records, information and data for as long as is required.

- **Ensure appropriate physical protection measures are in place in a range of circumstances including during records and data storage and handling, outsourcing, digitisation and migration and business continuity planning.**
  Agencies know where their records and data are stored and have assessed each location's conditions. Including:
  - physical locations such as onsite, endorsed locations
  - digital locations such as EDRMS or business systems.
- **Practice and actively promote, appropriate handling and storage measures.**

- Regular transfer of non-current records to appropriate secondary storage (only on ACT Government premises for hard-copy records with archival value)
- Development and monitoring of contract clauses and other risk mitigations for records and data held in cloud and other off-site arrangements
- Training of staff in their obligations not to destroy ACT Government records and data
- Inclusion of records and data management expertise in digitisation and migration plans and processes
- Registration and movement control and monitoring of hard copy records
- Establishment of business continuity and disaster response plans

The Retain principle seeks to enable organisations to establish business processes to support the legal retention and destruction of records, information and data. The Retain Principles helps organisations to comply with legal, regulatory and business requirements of information retention as well as supporting community memory, through Territory Archives.

- **Ensures that the agency has implemented and regularly reviewed Records Disposal Schedules** relevant to the functions of their agency (see Assess above).
- **Ensures that the agency has a regular sentencing program in place** for the appraisal and destruction/retention of records, information and data as an ongoing concern.

- Regular, routine and documented sentencing operations
- Consultation with and reporting to TRO on records destructions
- Secure and authorised destruction processes
- Application of processes to protect records of significance to Aboriginal and Torres Strait Islander people

The Access principle seeks to support appropriate information sharing within government, as well as public access to government information. The Access principle aims to equip organisations with the understanding and skills to confidently use and re-use information in the interest of government and the broader community.

- **Encourages openness, use and reuse of records, information and data** by ensuring policies and practices do not unnecessarily restrict access, either by the public or by other areas of government.
- **Reviews and supports plans implemented** 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.
- **Ensures open, equitable and consistent mechanisms are in place** to support members of the public to exercise their rights to access records, information and data within 28 days.

- Timely responses to requests for public access to archival records through ArchivesACT
- Registration of public access declarations under section 28 of the Act
- Sharing of metadata and other tools that support records information and data discovery
- Participation in Activities that promote public access to government information

Definitions

Senior Manager Responsible: An officer at the Executive Branch or Group Manager level, who holds the responsibility for records management and/or information governance function within an agency.

Information Governance: Encompasses all records, information and data management professionals and their activities

Abbreviations

EDRMS: Electronic Document Management System

FOI: Freedom of Information

PSPF: Protective Security Policy Framework (ACT)

RMP: Records Management Program

References

- Standard and Guidelines for Records, Information and Data
- Standard for Records, Information and Data
- *Territory Records Act 2002*