Attorney-General's Department

Information Management Policy

Purpose

The purpose of this policy is to provide guidance and direction on the creation and management of information, and to clarify staff responsibilities. AGD is committed to establishing and maintaining information management practices that meet its business needs, accountability requirements and stakeholder expectations.

The benefits of compliance with this policy will be trusted information that is well-described, stored in known locations and accessible to staff and clients when needed.

This policy is written within the context of AGD's Information Management Strategy which is located on the Information Management Services intranet page. This policy is supported by complementary guidelines, procedures and fact sheets, which can also be found on the Information Management Services page.

Policy Statement

The Attorney-General's Department (AGD) is committed to a governance, people, process, and technology approach to the management of information.

AGD's information is a corporate asset, vital both for ongoing operations and also in providing valuable evidence of business decisions, activities and transactions.

There is an expectation that AGD will work towards meeting the requirements of the *State Records Act, 1997* and other relevant legislation and is committed to creating and keeping accurate and reliable information to meet its obligations.

AGD will implement fit-for-purpose information management practices and systems to ensure the creation, maintenance and protection of reliable information. All information management practices in AGD are to be in accordance with this policy and its supporting procedures.

Scope

This policy applies to all AGD employees (ongoing, contract, casual, full-time, part-time) and is the policy for all business units (including statutory authorities) that are administratively supported by AGD. It incorporates:

- Information, records and data regardless of media and format (including but not limited to hard copy documents, electronic documents or file, email, handwritten notes, digital data and multimedia) received or created in the conduct of AGD business.

- All business applications used to create, manage and store information (records management systems, databases, line of business systems, email, websites, social media applications) managed in-house and offsite.

Legislative Framework

- *State Records Act, 1997* and other information management standards such as:
    - Adequate Records Management Standard (December 2013)
    - Australian Standard on Records Management AS ISO 15489-2002
    - South Australian Recordkeeping Metadata Standard (August 2015)
    - Management of Official Records in a Business System Standard (October 2011)
    - Functional Specification for Records in a Business System Standard (October 2011)
    - General Disposal Schedule No 30 – For State Government Agencies in South Australia (January 2016)
    - General Disposal Schedule No 21 – For Management and disposal of source documents and digitised versions after digitisation (February 2014)
- AGD Records Disposal Schedules
- Electronic Transactions Act, 2000
- Evidence Act, 1929
- Freedom of Information Act, 1991
- Privacy Act, 1988 (Commonwealth)
- Public Sector Act, 2009
- Digital by Default Declaration
- AGD information and records management policies and procedures

Creation and maintenance of information

Business information must be created and captured by everyone subject to this policy. Information created should provide a reliable and accurate account of business decisions and actions. It should include all necessary information to support business needs, including names, dates, times and other key information to capture the business context.

All business information created and received should be captured into line of business systems or the AGD records management system for corporate records. AGD intends that all current line of business systems should be assessed for compliance against the Business System Minimum Mandatory Recordkeeping Requirements (available from the Information Management Services Intranet page). Any new line of business system implementations will use the functionality requirements to define system requirements during the requirements gathering and design phases.

This approach allows AGD to store and manage digital information, removing the need for hard copy files.

Any physical records must be accurately tracked so they are able to be found on demand within a reasonable timeframe.

Access to Information

Information is a corporate resource to which all staff may have access, except where the nature of the information requires restriction. Access restrictions should only be in place when there is a business need or when restricted access is required by legislation. It should not be imposed unnecessarily but should protect:

- Individual staff, or client privacy
- Sensitive material such as security classified material

Access restrictions should also ensure that information:

- Is available, when appropriate, for use
- Is not subject to unauthorised use
- Cannot be altered, and
- Cannot be inappropriately destroyed

Information security should be applied in accordance with the SA government Information Security Management Framework (ISMF) and AGD Information Security Management System (ISMS).

Freedom of Information (FOI) requests should be managed in accordance with the AGD FOI Policy.

AGD adheres to the Information Privacy Principles Instruction for the management of and access to personal information.

Retention and Disposal

Records, including data in business systems, must be retained for the minimum periods set out in State Records approved Records Disposal Schedules (RDS) or General Disposal Schedules (GDS). The retention periods in these schedules take into account all business, legal and government requirements for the information. AGD uses a number of general and agency-specific schedules to determine retention, destruction and transfer actions for its information. (Refer to *'Disposal Schedules Fact Sheet'*; *'Sentencing Guidelines'; 'Temporary Records Storage Procedure'; 'Permanent Records Storage Procedure';* and the *'Destruction of Official Records Procedure'* for information on how to determine retention periods and approval processes for destruction of records).

Retention periods should be applied to records at the time of creation, either using system functionality or as an intellectual exercise undertaken outside of the system.

Records likely to be used in a legal case, subject to a FOI request, or covered by a disposal freeze must not be destroyed even if the minimum retention period has been reached.

Some information can be destroyed in the normal course of business. This is information that is of a short-term, facilitative or transitory value (i.e. has no continuing value to AGD). Destruction of this type of information is referred to as 'Normal Administrative Practice' (NAP). (Refer to the *'Normal Administrative (NAP) Fact Sheet'* and the *'Destruction of Official Records Procedure')*.

Original records, deemed permanent in a RDS or GDS, must be retained permanently in their original format (including hard copy). Digital copies may be made for reference purposes. Permanent digital records must remain accessible over time until the SA Government has a digital archive. Refer to Information Management Services for advice on storage of Permanent digital records.

Original hard copy records, deemed temporary in an RDS or GDS may be destroyed if an accurate representation of the original (i.e. a scanned image) is captured in a records management or line of business system that meets the requirements of the AGD Business System Minimum Mandatory Recordkeeping Requirements.

Hard copy records can be stored offsite as part of a centrally managed contract with an approved offsite storage provider for temporary records, or with State Records as per the *State Records Act, 1997* for permanent records. Records may only be stored if they have been sentence and listed in accordance with procedures associated with the storage provider. (Refer to *'Temporary Records Storage Procedure* and *'Permanent Records Storage Procedure').*

Training

All employees should be inducted into AGD's information management policy and practices. Business Units should induct and train employees in specific recordkeeping procedures applicable to their unit. Business Units can contact Information Management Services for further information or to arrange tailored training.

Planning and Resourcing

Business Units should define what records must be made and kept of business processes, and document these requirements. Information management should be planned and budgeted for particularly where changes to systems and practices have been recommended through audits or monitoring of current practices. Business Continuity Plans should identify vital records and that strategies are in place for ensuring these records can be accessed in the event of failure or disaster. Refer to the AGD Business Continuity Policy.

Roles and Responsibilities

Information management underpins and supports the delivery of core business. All employees have a responsibility to ensure that reliable and useable information is created and managed, and is kept for as long as it is needed for business, accountability and historical purposes. Responsibilities include:

Chief Executive Officer (CEO)

- The CEO is ultimately responsible for the management of information within the agency, ensuring that AGD has a program for managing its information to meet business objectives and legislative requirements.

Business Unit Heads, Executive (SAES) or Senior Management equivalent

- Support of, and adherence to, this policy by promoting a culture of compliant information management

- Ensure business processes and procedures define records to be made and kept for business and accountability purposes

- Ensure line of business systems meet recordkeeping requirements

- Ensure staff receive information management training relevant to their roles and responsibilities

- Utilise AGD's supplier contracts for offsite records storage

- Where required develop and maintain Records Disposal Schedules for their business unit

- Ensure digital and physical records are retained for required periods, and disposed of according to authorised processes.

- Act as the CEO's delegate for destruction of records approval in their business units (refer to '*Destruction of Official Records Procedure*')

Information Management Services

Under the leadership of the delegated senior executive (Executive Director Projects & Technology) Information Management Services is responsible for overseeing the management of information across AGD consistent with the requirements described in this policy. This includes:

- Provision of training, advice and general support to staff (increase awareness of information management strategy, policy, guidelines and practices and coordinate the provision of generic induction and training in records management for all employees).

- Creation, development or acquisition and implementation of information management products and tools, including systems to assist in the creation of complete and accurate information

- Development and implementation of strategies to enable sound information management practices

- Monitoring compliance with information management strategy, policy and procedures

- Advising Executive Management of any risks associated with non-compliance

- Coordination of the transfer of permanent records to State Records

- Coordination of the transfer of temporary records to offsite storage and manage the storage contract on behalf of business units

- Coordination of the sentencing and destruction of temporary physical records held in offsite storage, and provision of advice on in-house sentencing and destruction for business units.

- Facilitation of the reporting on information management on behalf of AGD.

All employees

All staff are responsible for the creation and management of information as defined by this policy and its related legislation.

- Create records to adequately document business activities
- Capture records in approved business systems during the business process or as soon as practical after completion
- Protect records in their possession
- Not remove, destroy or delete records without authority

Where can I get more information?

More information, including AGD procedures, guidelines and fact sheets, can be sourced from Information Management Services.

Intranet:
http://intraagd.agd.sa.gov.au/Corporatefunctions/InformationManagement/InformationRecordsManagement.aspx

Email:
AGD:Records Management