RECORDS MANAGEMENT PROCEDURE COR114

BACKGROUND

The *State Records Act 1997* creates a legal framework for the management of official records in the possession of Ministers, government departments and authorities. The Department of Treasury and Finance (DTF) will manage its official records in accordance with its obligations under this Act and other legislation.

OBJECTIVE

This procedure supports the Records Management Policy (COR133) and demonstrates how compliance with the policy is achieved. The presentation of content in this document aligns with the six outcomes described in the State Records Adequate Records Management Standard (ARMS).

The procedure facilitates the application of adequate records management by providing information and instruction about business processes and use of the corporate records management system Objective. This document is further supported by training materials and other documentation available to all staff on the DTF intranet.

SCOPE

This procedure applies to all DTF workers accessing and utilising the DTF records management system.

Whilst this procedure supports the Records Management Policy (COR133) and provides a framework for records management within DTF; individual branches may find it necessary to develop policies and procedures that relate specifically to their unique records, provided they are not in conflict with this procedure.

This procedure establishes a governance and compliance regime for the management of official records and documents, regardless of format. It ensures that official records are managed from the time of creation until their disposal.

DEFINITIONS

Adequate Records Management Standard (ARMS) is an across-government standard that has been developed to assist agencies to meet the requirements of the *State Records Act 1997*.

Approved Service Provider (ASP) is a company approved by State Records for the storage, retrieval and destruction of temporary value records. The company has entered into a Deed that establishes the legal framework for the provision of such services.

Business Classification Scheme (BCS) is defined as an articulation of the functions and activities of the organisation from the analysis of business activity. The structure of the scheme is hierarchical, moving from the general to the specific.

General Disposal Schedule (GDS) is a disposal schedule that covers the functions and/or records common to a number of agencies irrespective of the purposes for which those agencies were specifically established.

Objective is the approved DTF records management system for the capture and maintenance of official records.

Official Record is a record of a business transaction, exchange of information, or decision undertaken in the course of the department's operations. Therefore any record created by a worker in the course of their duties constitutes an official record.

Normal Administrative Practice (NAP) is defined as the concept that material can be destroyed according to 'normal administrative practices'. This provides for the routine destruction of drafts, duplicates and publications, with the test that it is obvious that no information of continuing value to the organisation will be destroyed.

Records Disposal Schedule (RDS) is an agency specific disposal schedule that relates to records that an agency creates in order to carry out the specific operations for which it was established.

State Records Act 1997 is an Act providing for the preservation and management of official records.

PROCEDURE

DTF is committed to complying with government records management requirements. This procedure supports compliance with the department's Records Management Policy (COR133) and the ARMS. DTF will comply with these requirements in the following manner:

Outcome 1 Records Management is planned:

The Records Management Unit has developed records management policies and procedures to provide direction and guidance for managing official records.

All branches have a responsibility to consider records management in their business planning processes, including the creation of any policies, procedures and guidelines to meet unique local operational needs.

DTF has invested in a State Records compliant records management system Objective and configured it to meet the unique operating needs of the business. The system has many features with searching and security being key attributes to its functionality.

New line-of-business (business specific) systems need to consider records management as a selection criterion of the procurement process to meet the compliance expectations of State Records.

<u>Business Classification Scheme (BCS)</u>

As part of the planning process, the DTF records management system has been appropriately configured so records are captured into a structured BCS which recognises standard administrative and unique operational functions and activities of the business.

To ensure appropriateness of the structures, each branch must periodically review its BCS in collaboration with the Records Management Unit, and reviewed at minimum during times of any internal or administrative change.

While administrative records are managed in a BCS structure defined by a GDS (predominantly GDS15), unique operational records are managed by a State Records approved DTF RDS.

The initial two folder levels (function and activity) of the BCS are locked down and cannot be altered by workers. Any changes sought in respect to modifying the BCS structure need to be referred to the Records Management Unit for discussion and consideration.

While files cannot be created at the function level (first folder level) of the BCS structure, capacity exists to create files at the activity (second folder level) and subsequent lower folder levels should they exist.

Outcome 2 Records Management is resourced:

The DTF Records Management Unit has experienced and qualified workers in the management of both physical and electronic records and the DTF records management system Objective. The DTF Records Management Unit provides direction and guidance to branches in the management of physical files, documents and other records. There is an expectation that branches also have sufficiently skilled resources to manage their own records.

Workers are encouraged to adopt good records management practices and are expected to attend in-house training. All workers are expected to attend 'Records Management Awareness' training on commencement in DTF and a refresher session every three years.

Workers accessing Objective are also expected to attend Objective training appropriate to their activity requirements in the system. Records management training dates and booking is available online via OurDevelopment and supported by course outline and training materials available on the DTF intranet.

Outcome 3 Records Management is monitored and reviewed:

The Records Management Unit has and will continue to develop and make available regular Objective operational effectiveness reports.

The Records Management Unit will report progression against the requirements of the ARMS.

Branch heads are accountable for ensuring branch records management practices and performance levels are achieved in accordance with DTFs records management program.

Outcome 4 Records are created, captured and controlled:

Workers have a responsibility to create records in all instances where there is a need for the department or an individual to be accountable for, and/or provide evidence of, decisions made and actions taken.

<u>Document Creation:</u>

The majority of DTF workers are currently using network drives and other data storage locations to manage electronic content. Over time there will be a gradual transition towards embracing Objective to store and manage electronic content in line with the expectations of State Records. Scanning technologies have been introduced to support the transition process in minimising (in a State Records approved manner) the retention of physical content.

For those not currently using Objective to manage electronic content, a 'physical document' should be created to recognise the existence of physical or electronic content not captured in Objective. From a business continuity perspective, this activity will ensure Objective accurately reflects content held in physical files.

Workers are responsible for creating official records in all instances where there is a requirement to be accountable for, and/or provide evidence of, decisions made and actions taken. Records

must be created on the transaction of business, or as soon as practicable afterwards. Workers need to ensure official records are captured in Objective (electronically or as a physical document) and placed into a file upon creation or receipt.

A record may be created in any format that is appropriate for its purpose (i.e. e-mail, facsimile, minute, letter etc). Templates and the DTF Style Guide will assist in the creation of these records. Refer to the DTF Intranet for further information.

If a worker does not have access to capture official records into Objective, they are responsible for ensuring the records are provided to another worker that can.

The documents that should be captured in Objective include but are not limited to:

- claims;
- complaints;
- customer/stakeholder complaints;
- file notes;
- Freedom of Information enquiries (central processing by Corporate Services);
- incoming correspondence;
- inter-agency enquiries;
- ministerials;
- minutes;
- outgoing correspondence;
- planning matters;
- project documents including related correspondence;
- records of discussion; and
- tenders/quotes.

Once a document has been entered into Objective it will be given a system generated unique document number (physical ID). The document and associated file number must be recorded on the electronic document, in the space provided by the template, or in the top right hand corner of the document.

Hard copy documentation placed in physical files must be placed in chronological order with the oldest document at the bottom of the file.

All official records created electronically outside of Objective must be printed and filed in the appropriate physical file.

The process associated with creating and managing a document in Objective can be found in training materials on the Objective page of the DTF intranet.

Incoming Documents

Official documents received by DTF are to be recorded in Objective as a physical document in the related file. Where the incoming documents are received by the DTF Records Management Unit, they will be scanned and saved electronically (text searchable pdfs) in Objective in addition to a physical document being created. DTF Branches are encouraged to do similarly.

Official documents are to be filed in the appropriate physical file, or travelling document cover (blue cover) when it is not immediately attached to the parent file. Original content held in the blue cover to be placed on the parent physical file once management of the content is finalised.

Outgoing Documents

Unless an electronic copy has been placed in Objective in the appropriate file, all outgoing documents must be registered in Objective as physical documents. The system generated document number (physical ID) and associated file number must be recorded on the outgoing document prior to printing and processing.

Similarly, unless an electronic copy has been placed in Objective, a hard copy of all outgoing documents must be placed on the appropriate physical file upon creation or receipt, or as soon as practicable afterwards.

File Creation:

All Corporate Files must be created within Objective.

New files are created when:

- a new project or activity commences;
- correspondence needs to be/has been actioned and no file exists relating to the function and activity documented in the correspondence; and
- annual files reach their use by date and there is a demonstrated need to create a file for the following year.

With the exception of those branches which create their own files, workers are required to contact the Records Management Unit, Corporate Services via email 'DTF:Records Management' when a new file / new file part needs to be created. Requests must contain the following information:

- the location in Objective where the file is to be created and located;
- file title (use appropriate descriptive words in line with approved naming conventions);
- subject/file description;
- custodian (who is requesting the file);
- file's home location (e.g. branch location/compactus); and
- any security, confidentiality or access restrictions necessary (e.g. security group).

For those who have responsibility of creating files in Objective, the process is thoroughly documented in training materials on the Objective page of the DTF intranet.

File and Physical Document / External Agency File Movement:

When physically moving a file, physical document or external agency file, workers are responsible for updating Objective to reflect the change. If a worker does not have access to the records management system or blocked by security, they are responsible for advising a worker who can update Objective on their behalf.

Documents not travelling with the relevant physical file should be placed in travelling covers (blue plastic folder) and be moved to the appropriate custodian in Objective. This enables those documents travelling outside their parent file to be tracked and located.

If a worker does not have access to Objective and/or cannot locate the information they are looking for, they should contact an Objective key user within their branch to assist them in searching and updating records.

Physical files must not leave DTF. Travelling document covers should be created and relevant documents copied and placed within the cover for all instances where access is required off-site. Original documentation should always be retained on the parent file where possible. This is to prevent original documentation becoming lost or inaccessible.

It is the branch's responsibility to ensure that when a worker leaves DTF, changes branch or positions in DTF; custodian relationship to files and physical documents are updated as required.

Emails

An official email is one received or created by a worker in the course of their duties. It may record a business transaction, the exchange of information, or a decision. Work related emails are official records of the department and are to be captured and managed accordingly.

Where workers are not currently using Objective to save emails to files, the email must be printed and captured as physical documents and placed in the appropriate physical file. The capture of relevant emails on network drives should also be considered where the capacity does not exist to save to Objective.

A worker can decide when an email message discussion is completed and when it should be captured. While duplication of emails in Objective should be avoided, it is realised this may be necessary due to security reasons. As a general rule, the worker who created the email has responsibility to capture it in Objective.

External Agency Files

Files received from government departments, Ministers or portfolio entities (Motor Accident Commission, Essential Services Commission of South Australia and Office of the Treasurer) are to be created as 'External Agency Files' in Objective, with file numbering and titling identical to that of the external agency file.

A copy of the External Agency File documentation and any relating documents (i.e. response) must be filed on an appropriate corporate file prior to the External Agency File being returned.

The process associated with creating and managing an External Agency File can be found in training materials on the Objective page of the DTF intranet.

Outcome 5 Records are secure and accessible as appropriate:

The Records Management Unit is responsible for managing both the security and access to Objective.

For ease of access, only active physical files should be held by workers. Inactive physical files should either be stored in the relevant branch's central filing area, managed to off-site retention or if appropriate, forwarded to the Records Management Unit.

Restricted files such as budget papers, Cabinet submissions, HR matters, personnel files etc that contain confidential and/or sensitive information must be stored in a secure filing system.

The Records Management Unit will manage access to electronic files within Objective by assigning appropriate security controls over access to the files. This ensures confidentiality and security of confidential and/or sensitive information.

When a request for a file to be created is lodged, workers must advise the sensitivity of the required file. This will determine confidentiality and security controls for both the physical file and the corresponding electronic version held in Objective.

If confidential documents are added to files not initially marked as confidential or sensitive, the worker responsible for the information must advise the Records Management Unit, to ensure security and access restrictions are reviewed for the file.

Archiving of records to State Records SA or Approved Service Provider (ASP):

The processes associated with listing permanent/temporary retention records for transfer to off-site storage are similar in nature, they do vary in detail. These processes are documented on the DTF intranet site. Branches should liaise with the Records Management Unit for direction and guidance.

Records eligible for transfer to State Records SA:

- classed as permanent under General Disposal Schedule No.15 (GDS 15) or under one of the department's records disposal schedules;
- no longer in active/frequent use;
- not subject to a current Freedom of Information request or court case; and
- approved by the Branch Head and Manager, Administration.

Records eligible for transfer to the department's ASP:

- classed as temporary under GDS 15 or under one of the department's RDSs;
- no longer in active/frequent use;
- either not yet eligible for destruction, or a decision has been made to retain the records longer than the recommended time frame; and
- approved by the Manager, Administration and the relevant Branch Head.

The Records Management Unit manages the temporary retrieval of both permanent and temporary records stored off-site. Permanent records are held by State Records while temporary records are stored off-site with an ASP. Contact the Records Management Unit to retrieve archived records.

Access to Objective

On receipt and processing of an appropriately authorised and completed 'Access Request for Treasury Objective', the Records Management Unit will configure a new user/modify user based the requested security access to DTF records. Workers will be given access to Objective that is appropriate to their operational needs and are expected to attend those Objective training modules aligned to their use of Objective.

PC logon credentials are used to access the Objective environment. While within the work environment a 'single sign-on' feature exists to enable users to access Objective by simply clicking on an icon on their desktop, remote access methods may require logon credentials to be inserted.

Workers should never divulge their logon and password credentials to another person. All activity undertaken by a worker (including even viewing a record) is captured by the audit functionality of Objective.

The Records Management Unit must be advised in a timely manner of any user changes affecting user access to Objective.

Security within Objective

Objective is highly configurable in respect to security. Flexibility via privileges exists to provide; see, open, create, edit, delete, security and administrator access to a record.

While security by default inherits down through the BCS and file to documents, at any stage of the parent hierarchy structure privileges can be changed.

Objective is a single DTF database which enables collaboration and sharing of records between users in different branches of DTF.

On creation of a record in Objective, a user can define the work area or workers who will be granted access and the nature of that access (e.g. see, open, edit, create).

Typically branches will have their own secured area within Objective to share and collaborate on records with branch workers. It will be the branch decision if they wish to share their records with other branches, sections and workers.

Where security does not provide workers the opportunity for changing privileges on a structure, file or individual record, an appropriately authorised request should be lodged to the Records Management Unit via email distribution DTF:Objective Support.

Workers do not have the necessary privileges to delete records within an Objective file. An appropriately authorised request via email providing justification for the deletion should be lodged to Records Management Unit via email distribution DTF:Objective Support.

Freedom of Information (FOI)

The Freedom of Information Team, Corporate Services provide strategic advice and administrative support in the management of the Department's obligations under the *Freedom of Information Act 1991* (FOI Act). The FOI Act provides individuals and organisations with the right to request and access documents held by South Australian Government agencies, Local Government Authorities and Universities.

All documents held by the Department are subject to access under the FOI Act. The definition of a document includes, but is not limited to: letters, minutes, reports, photos, memos, file notes, drafts, and anything in which information is stored or from which information may be reproduced.

If a member of the public has a legitimate need or right to see records that have been transferred to State Records SA, but are restricted from public view, they may make an application to view those records to the responsible agency under the provisions of the *Freedom of information Act 1991*, or *Privacy Act 1988*.

For further information relating to the management of FOI records refer to *Procedure – Freedom of Information COR126* or contact the Freedom of Information Unit.

Outcome 6 Records disposal is managed:

All official records managed by DTF have a prescribed life span, defined by approved disposal schedules. The disposal of official records can only occur within the provisions of the *State*

Records Act 1997, and require the approval of a branch head and State Records prior to destruction.

Destruction is the irreversible removal of information from the department's official records. It may only be carried out in circumstances where the:

- records to be destroyed have been approved for destruction;
- destruction method is secure and effective;
- destruction method is appropriate to the format of the records to be destroyed; and
- destruction is documented.

It is important that following the destruction of eligible official records, no other copies remain in the possession of the department. This approach ensures:

- copies are not mistakenly deemed to be of an official nature; and
- the department complies with the State Records archiving practices.

Records may only be destroyed if they:

- are covered by GDS 15 or one of the Department's RDSs;
- are designated as temporary records in the above RDSs;
- have fulfilled any relevant retention time criteria set in the above RDSs;
- are not subject to an active Freedom of Information request or court case;
- are no longer in active use within the department; and
- have been approved for destruction by the Branch Head, Manager, Administration and State Records SA.

Disposal - Administrative records (T&F files)

The Records Management Unit is responsible for the disposal of 'T&F' files. Branches are responsible for regularly reviewing/auditing their storage areas and advising the Records Management Unit of inactive 'T&F' files. The Records Management Unit will dispose of all inactive 'T&F' files according to the relevant disposal authorities (General Disposal Schedule (GDS) or Records Disposal Schedule (RDS)).

Records being destroyed in accordance with Normal Administrative Practice (NAP) or under authority of GDS 15 where the disposal action allows destruction one year or less after the last action, do not require State Records approval for destruction.

Disposal - Branch specific records

While the Records Management Unit does not have responsibility for the disposal processes associated with branch specific files and records (eg Super SA, SAFA and RevenueSA), these records must be disposed of in accordance with GDS and RDS authorities or otherwise approved by State Records.

Branches conducting their own disposal programs must do so in a planned and coordinated manner. The branch must maintain a record of all disposed files.

Branches will regularly review/develop RDSs, in collaboration with the Records Management Unit, to ensure disposal schedules cover all official records managed by the branch.

Branches must assign responsibility for the disposal of branch records to an appropriately skilled worker.

Disposal - Records not held in Objective

Records not held in Objective (e.g. in a departmental business system, on a network drive, emails etc.) may still be eligible for destruction. The same criteria and requirements apply.

It is important that a full and accurate record is kept of the records destroyed, the provisions under which they were destroyed (which disposal schedule class), the date of destruction, the approval of the Branch Head, Manager, Administration and State Records and the signature of the destroying officer. Please contact the Records Management Unit for further assistance.

Destruction of records

Unauthorised destruction of records is a serious offense. Branches, sections and workers are encouraged to contact the Records Management Unit of DTF prior to undertaking any destructive activity.

RESPONSIBILITIES

Under Treasurer
Section 13 of the *State Records Act 1997* requires the Chief Executive of an agency to ensure that the official records of the agency are documented and preserved in line with legislative requirements. These requirements ensure that appropriate government standards are upheld and that the integrity of records and the interests of staff and stakeholders are protected.

Branch Heads and Senior Managers
Are responsible for ensuring:

- all staff within their branch/section adhere to DTF's records management policies and procedures and have access to the knowledge and tools that support these ongoing;
- employees, consultants, and contractors receive records management training relevant to their roles and responsibilities;
- advice is sought from the Records Management Unit prior to the development or purchase of recordkeeping tools; and
- whole-of-department initiatives are complied with.

Workers *(including employees, contractors, consultants and providers of outsourced DTF services)*
Are responsible for:

- adhering to DTFs records management policies, procedures and practices;
- creating records that adequately record business activity, including decisions made and actions taken;
- protecting and safeguarding records in their possession;
- not removing, destroying or deleting records without authority to do so;
- ensuring all official records form part of DTFs record holdings; and
- ensuring all activity carried out on records is recorded and maintained.

RELATED DOCUMENTS

- COR133 Records Management Policy
- COR124 Procedure – Exchange of Information
- COR126 Procedure – Freedom of Information

FURTHER INFORMATION

Contact DTF Records Management on [redacted], or

- email DTF:Records Management for file creation and physical records requirements;
- email DTF:Objective Support for all matters relating to the *Objective* system.

[redacted]

UNDER TREASURER

19 / 12 / 2013