Overview of disposal and destruction of ACT Government records, information and data

Purpose

This Records Advice articulates the Territory Records Office's position on the disposal and destruction of records as authorised by the *Territory Records Act 2002*. This advice should be used in managing ACT Government records, and can also be applied to other government information and data holdings.

Background

The orderly, authorised destruction of some categories of records yields benefits to ACT Government organisations by:

- reducing the cost of unnecessarily storing records which are no longer required for business, accountability or community purposes;
- making efficient use of resources by ensuring that high quality records storage environments are used only to store the significant records of government;
- improving the retrieval of active records, with easier and quicker to access possible as a result of the reduced volume of records, in both hard and digital systems;
- reducing the risk and associated costs to organisations of having to identify, examine and produce records through Freedom of Information and other processes that might have been legitimately destroyed.

Definitions

Disposal

Disposal is the range of processes associated with implementing a records disposal schedule. It is most often thought of as destruction of records, but the term also has other meanings:

- Destruction – the process of ensuring that records, information and data are physically destroyed or deleted so that they are no longer usable or accessible. Destruction of records, information and data must be properly authorised, irreversible, secure, documented and must use processes appropriate to the media used. See also the **Retain Principle** for information on **authorised destruction methods**.

- Transfer to a secondary storage provider (Temporary Retention) – hard copy records that are not in day to day use may be transferred to secondary storage, such as with ACT Record Services. ACT Government organisations may also use external storage providers provided that there are appropriate contractual arrangements in place, and they can demonstrate compliance with the ***Territory Records Act 2002***. Further information can be found in the **Retain Principle** to prepare records for transfer.
- Archiving – records, information and data that have been designated as 'Retain as Territory Archives' (RTA), must be kept and appropriately stored to ensure continuing access and availability to the public once they enter the open access period. For physical records this will usually involve transferring files and other media to secondary storage such as Records Services. For digital records it may involve moving records, information and data offline, restricting them from further alteration or transferring them to a digital repository. Copying digital records to CD-ROM or other portable storage media is not acceptable for archiving long-term records, but may be adequate for records, information and data that only needs to be retained for a short period. Also see the **Protect** and **Retain Principles**.
- Transfer of ownership – records, information and data may be transferred to a new owner as part of the sale or privatisation of an ACT Government organisation or by donation to a community or other appropriate group. Transfers of ownership must be authorised by the Director of Territory Records.

Destruction

The process of ensuring that records, information and data are physically destroyed or deleted so that they are no longer usable, retrievable or accessible. Destruction of records, information and data must be properly authorised, irreversible, secure, documented and must use processes appropriate to their media.

Records disposal and destruction

ACT Government organisations and individuals may only destroy records if the Director of Territory Records has issued an applicable Records Disposal Schedule that authorises the destruction. Records Disposal Schedules must also be endorsed for use by an organisation's Principal Officer (usually the Director-General or equivalent) by including them in the organisation's Records Management Program.

Records Disposal Schedules

All ACT government records must be classified according to a Records Disposal Schedule before they can be approved for destruction or other forms of disposal. Only the Director of Territory Records can approve a Records Disposal Schedule.

The Territory Records Office maintains a set Records Disposal Schedules for common functions which are carried out by most ACT Government organisations. Organisations must also identify any and all specific functions they carry out, and work with the Territory Records Office to develop an authorised Records Disposal Schedule for the records that document those functions.

Organisational concurrence for disposal

After records have been assessed against a Records Disposal Schedule and identified as suitable for destruction, their disposal and destruction must be managed with the agreement of the following stakeholders:

- the senior manager of the business unit responsible for the activities documented in the records;
    - in the case where Shared Services has grouped multiple transactions belonging to multiple business units within the same record, the authorisation to destroy the record is held by the appropriate executive director in Shared Services or their delegate after informing the relevant ACT Government organisations of the intention to destroy records;
- the organisation's Records Manager or equivalent;
- the Territory Records Office.

The concurrence process ensures that all remaining requirements to keep the records have expired before the records are destroyed. This may include assessing the significance of the cases the records document. It must also include an assessment of whether the records can reasonably be expected to be required for any legal proceedings, are subject to any reasonably foreseeable Freedom of Information requests or are affected by a current disposal freeze. Destruction of records subject to legal proceedings (including FOI) or disposal freezes is not authorised, even if an existing Records Disposal Schedule would otherwise permit their destruction.

Information security and privacy

Records with security classifications, as outlined in the ACT Government Protective Security Framework, or with privacy considerations as per the Territory Privacy Principles, must be handled appropriately when they are being destroyed. The Protective Security Framework provides guidance on secure destruction of sensitive documents.

Notification of disposal and total destruction

Under section 33 of the Territory Records Act, the Director of Territory Records is authorised to monitor the disposal of records by ACT Government organisations. Organisations are required, as part of the destruction approvals process to consult with the Territory Records Office before records are destroyed.

ACT Government organisations must ensure that all records identified for destruction are completely destroyed and their contents rendered irretrievable. This includes official records, G-drive copies and other references to the information destroyed. Only the metadata relating to the record should remain in official recordkeeping systems. Any information that is not destroyed in relation to the record will still be subject to legal discovery orders and other processes such as freedom of information requests.