Environment and Planning

Records Management Program

Policy

ACT Government
Environment and Planning

Introduction

The *Territory Records Act 2002* (the Act) requires ACT Government Directorates to have, and to comply with, a Records Management Program (RMP).

Within the Environment and Planning Directorate (EPD) the RMP is a suite of documents including: this policy, supporting procedures, corporate polices and work instructions, which form the framework for recordkeeping within EPD. The principle documents that form the Records Management Program are:

- *Records Management Program – Policy*
- *Records Management Program – Procedure 01 – Introduction to procedures*
- *Records Management Program – Procedure 02 – Records Lifecycle*
- *Records Management Program – Procedure 03 – Public Access*
- *Records Management Program – Procedure 04 –Business Critical Records*
- *Records Management Program – Procedure 05 – Managing and Preserving Territory Archives*
- *Records Management Program – Procedure 06 – Objective Administration*

Additional documents that support the Records Management Program include, but are not limited to:

- EPD Corporate Plan
- EPD Business Continuity Plan
- EPD Risk Management Plan
- Shared Services ICT, Acceptable Use of ICT Resources Policy
- Shared Services ICT, ICT Security Policy

Recordkeeping Policy Purpose

EPD is responsible to the community for creating records in order to inform advice and support the decisions made by the Directorate. This information is contained in records, which are created in a wide variety of formats including documents, photos, GIS data, emails, etc. These records, regardless of their format, need to be recorded, managed, and maintained to ensure they are available to the community, now and into the future.

The purpose of this policy is to establish a framework for the management of records through their lifecycle from creation to destruction.

The recordkeeping policy broadly identifies how records are used by EPD and how they will be created and maintained to satisfy business needs, legal requirements and accountability, and meet stakeholder expectations. Implementation of this policy is recognised to be evolutionary.

The recordkeeping policy:

- Outlines the scope and basis for recordkeeping within EPD
- Outlines the objectives and benefits of effective recordkeeping
- Identifies the kind of records that need to be created and maintained in order to support core business activities and meet accountability requirements
- Spells out the principles of the recordkeeping environment
- Details the obligations of staff, managers, and executives in relation to recordkeeping
- Provides a framework for staff development
- Acknowledges the essential collaboration between the Environment and Planning Directorate and other ACT Government Directorates.

These points provide the structure of the policy.

Scope

EPD is committed to achieving best practice records management as outlined in the *Territory Records Act 200*2, as well as Australian and International Standards related to Records and Information Management.

As part of this commitment, the management of all EPD records will comply with the requirements set out in the EPD Records Management Program, will meet legislative requirements outlined in *the Territory Records Act 2002*, *the Freedom of Information Act 1989*, *the Information Privacy Act 2014, the Electronic Transactions Act 2001* and any specific recordkeeping requirements detailed in the various legislations administered by EPD.

All staff within EPD, contractors employed by EPD, and external service providers under contract with EPD or the ACT Government, are obliged to comply with this policy, relevant legislation, policies and standards.

Objectives

Benefits

This policy is designed to produce the following benefits:

- More efficient access and retrieval of records
- Better quality advice to executives and ministers
- Improved customer service
- Faster and more satisfactory responses to media issues
- Enhanced decision making at both operational and strategic levels
- Greater accountability and improved knowledge management
- Improved long-term planning
- Decreased storage costs through correct disposal procedures and improved understanding of records management responsibilities

Records as Assets

EPD is committed to ensuring records in its care are treated as valuable corporate assets, critical to the business of EPD and the ACT Government. Particular value will be placed on records that establish the planning, environmental, and conservation history of the Canberra region and historically sensitive sites.

All records made or received by EPD are the property of the ACT Government. Records created by staff, received by staff, and maintained as part of their duties are owned by EPD and the ACT Government. Records do not belong to individual employees or contractors.

All staff that access records, in physical or digital form, will treat records in such as way as to ensure their preservation and continued accessibility now and into the future.

Sensitive Records

EPD is committed to ensuring records containing sensitive information, including those that contain personal information and those which enable people to establish links with their Aboriginal and Torres Strait Islander heritage are appropriately managed and preserved, and made available to individuals seeking information that connects them with their heritage.

It should be recognised that historical information held in regard to Aboriginal and Torres Strait Islander People may not have been created by individuals of Aboriginal or Torres Strait Islander heritage. Historical records held by EPD could contain information, or be presented in a manner which could be offensive to Aboriginal or Torres Strait Islander people.

When managing requests for access from individuals that are seeking connection to their Aboriginal or Torres Strait Islander heritage appropriate care will be taken to identify those records that could be considered offensive in nature, and ensure that applicants are prepared to review potentially offensive information.

Requests for access to sensitive records will be managed carefully by staff with responsibility for providing access to records.

RMP Awareness

Effective implementation of the EPD Records Management Program will require that staff be aware of the Records Management Program, relevant procedures, best practice guides, work instructions, and their requirement to ensure EPD compliance with the Territory Records Act.

All executive, managers, and team leaders have a responsibility to foster an environment that promotes good recordkeeping. This will be done through monitoring staff to ensure they understand, and comply with, the EPD Records Management Program. Managers and supervisors at all levels are responsible for ensuring that staff under their direction, including consultants and contractors, meet all the requirements of the policy and associated procedures.

All EPD staff shall:

- Understand the recordkeeping obligations and responsibilities that relate to their role at EPD
- Adhere to ACT Government policies, procedures, and standards for keeping records documenting their activities on behalf of EPD and the ACT Government
- Only destroy records under an approved Records Disposal Schedule.

Records Management Policy Principles

Full and Accurate Records

All staff within EPD will create full and accurate records of their activities and ensure that such records are appropriately stored on a correctly classified file, which can be tracked via an approved recordkeeping system.

Staff will have an awareness of, and comply with, the EPD Records Management Policy and associated procedures and work instructions.

Records management procedures will meet accountability and compliance requirements of the Territory Records Act and provide staff with clear direction about their recordkeeping responsibilities.

Records Management Procedures

The EPD Records Management Procedures will support this policy.

The procedures will outline in detail the way all staff within EPD will make, modify, use, handle and care for records, how and for how long records will be kept, and how access to them will be provided.

All documents that form part of the EPD Records Management Program will be available to staff via the EPD Intranet.

Recordkeeping Standards

EPD will conform to the Territory Records Act and Territory Records Office Standards. In cases where recordkeeping issues arise which are not covered by the EPD Records Management Policy, or associated Procedures, EPD will follow advice from the Territory Records Office and be guided by the Australian Standard on Records Management (AS ISO 15489)

Compliance with Legal and Administrative Requirements

Records of all decisions will be created. Records will also be created in all instances where there is a need for a business unit or individual to be accountable for, and/or provide evidence of, the decision-making process or actions taken. The EPD Records Management Program complies with legal requirements, including those for the provision of evidence.

Records will be uniquely identified and registered in EPD records management systems as soon as they are created, received, or is operationally feasible.

All records will be classified and titled according to the Territory Whole of Government Thesaurus and follow the EPD Best Practice Guide to naming conventions.

Compliance with the Records Management Program

The Director-General will appoint a Senior Executive in charge of Records Management. The Senior Executive in charge of Records Management is responsible for ensuring that:

- The Director-General has authorised the Records Management Program
- EPD maintains a comprehensive records management framework, including policies related to records and information management, a strategic plan for records management activities, and a risk register of ongoing risks related to the management of records
- This policy and associated procedures are kept updated and reflect internal and external recordkeeping requirements and best practice standards
- EPD business units develop procedures and performance management plans designed to include records management as a key result area
- Records Management requirements are considered in the implementation and maintenance of all ICT systems that manage records of EPD
- Records management considerations are included in corporate plans and reported in the annual report
- The Records Management Program is published on the EPD website and made available to community members in hard copy if requested

Review of Policy and Procedures

The Senior Executive in charge of Records Management will review this policy every three years from the initial approval of this policy, or at an earlier date if circumstances make it appropriate to do so.

Circumstances that may make such a review appropriate include a major change to EPD functions, a significant administrative change within EPD, or a review of the Territory Records Act which impacts administrative arrangements within EPD.

Relationship with the Director of Territory Records

EPD has in place arrangements for:

- Advising the Director of Territory Records about outsourcing of any aspect of EPD records management responsibilities
- Allowing the Director of Territory Records to examine the operation of the Records Management Program and EPD's compliance with the Act and the Program
- Consulting with the Director of Territory Records for assistance, advice, and training to EPD staff in relation to records management
- Allowing the Director of Territory Records to report on EPD compliance with the Act and the EPD Records Management Program

Recordkeeping Systems

ACT Government agencies are required to use an approved and compliant records management system. EPD utilise multiple approved recordkeeping systems for the management of EPD records. EPD principally manage records utilising electronic document and records management systems (EDRMS).

The principle recordkeeping systems used by EPD include:

- Objective
- HP RM (TRIM)
- Oracle Financials

These systems are approved for the management of ACT Government records.

Approved recordkeeping systems will manage the following processes:

- The capture and registration of records
- The storage of records
- The protection of record integrity and authenticity
- The security of records
- The disposal of records according to approved Records Disposal Schedules
- Access to records

EPD also maintain ICT systems that are not classified as recordkeeping systems. These include:

- network and local drives
- eLodgement systems
- portable storage devices
- Outlook accounts
- Access databases
- Spatial data management systems

These systems do not meet the requirements of approved recordkeeping systems and should only be used for storage of records if an approved recordkeeping system is not suitable for the specific type of record, for example storage of GIS data.

In the event a case is established to manage a record, or group of records, outside of an approved recordkeeping system, the exception will be approved by the Senior Executive in charge of Records Management and a register maintained as part of the Records Management Program.

The IMICT Committee will ensure that any IMICT systems and projects that are implemented within EPD will comply with records management legislation and standards.

The IMICT Committee will actively manage the migration of records and information stored in non-compliant systems to a compliant recordkeeping system as part of IMICT Strategic Planning.

Recordkeeping Service Providers

In the event any of EPD's recordkeeping requirements are outsourced, the Senior Executive in charge of Records Management will ensure that the service provider complies with all aspects of the EPD Records Management Program and the Territory Records Act. The Senior Executive in charge of

Records Management will ensure any items of significant historical or social value will be stored in such a way as to reduce ongoing damage to and ensure items are preserved for future generations.

Section 16 of the Territory Records Act requires EPD to notify the Director of Territory Records of any arrangements to outsource its recordkeeping functions. The Senior Executive in charge of Records Management is to facilitate timely notification.

Legislation and standards

This policy is a component of the EPD Records Management Program developed to meet the requirements of the Territory Records Act and subordinate legislation. Other relevant legislation, standards and documents include, but are not limited to:

- Territory Records Office Standards, guidelines and supporting documents
- *Public Sector Management Act 1994*
- *Freedom of Information Act 1989*
- *Information Privacy Act 2014*
- *Crimes Act 1900*
- *Evidence Act 1971*
- *Electronic Transactions Act 1999 (Commonwealth)*
- *Architects Act 2004*
- *Australian Capital Territory (Planning and Land Management) Act 1998 (Commonwealth) sections 16, 19, 25, 29 and part 10*
- *Building Act 2004*
- *Community Title Act 2001*
- *Construction Occupations (Licensing) Act 2004*
- *Electricity Safety Act 1971*
- *Gas Safety Act 2000*
- *Planning and Development Act 2007 and Planning and Development Regulation 2008*
- *Public Place Names Act 1989*
- *Surveyors Act 2007*
- *Unit Titles Act 2001*
- *Utilities Act 2000, part 5 and division 10.3*
- *Utilities (Telecommunications Installations) Act 2001*
- *Water and Sewerage Act 2000*
- *Environment Protection Act 1997*
- *Water Resources Act 2007*
- *Nature Conservation Act 1980*
- *Electricity Feed in (Renewable Energy Premium) Act 2008*
- *Utilities Act 2000*
- *Water and Sewerage Act 2000*
- *Animal Diseases Act 2005*
- *Fertilisers (Labelling and Sale) Act 1904*
- *Pest Plants and Animals Act 2005*
- *Plant Diseases Act 2002*
- *Stock Act 2005*

Security of Records

Privacy and Confidentiality

EPD will take all reasonable precautions to ensure personal information about individuals, commercial-in-confidence information, or to other sensitive information is not misused. Such information will only be shared with other organisations when it is appropriate to do so, and legislative powers allow it. More detail in regard to collection and management of personal information is outlined in the EPD Privacy Policy.

Semi-Active records security

Records which are no longer required for day-to-day work, particularly historical hard copy records will be stored in a secure offsite storage location to maximise office space and reduce the risk of inappropriate access.

Classification of Records

ACT Government EDRM systems do not currently have the capability to register file (container) level security classifications. These systems rely on group based access permissions to effectively manage information security. EPD apply dissemination limiting markers (DLM) when distributing email, as required by the ACT Government Protective Security Framework.

When security classifications are established in EDRMS environments, staff will be required to apply the relevant security classification at the creation of the record, and ensure that file level security is continuously updated to ensure it reflects the highest level of classification of the documents contained within the file.

Recordkeeping Environment

Records Preservation

Records will be stored in conditions which ensure they are accessible and retrievable and which take into account their physical characteristics and sensitivity for the length of time they are to be kept.

Those records which are identified as having enduring value to EPD and the Territory will be stored in conditions that satisfy the minimum standards for permanent retention.

Intellectual Property

EPD will ensure that copyright and other intellectual property issues are adequately addressed.

Business Continuity

EPD will implement plans to ensure that it can continue to use, and access, key records within the required business time frame, whatever the circumstances, including physical disruption.

Each business unit will take all reasonable steps to ensure that their records are at minimal risk of damage or loss due to accident or disaster and that their business continuity plans include subsequent conservation of records.

Disposal of Records

Disposal of Territory records will be done according to approved Records Disposal Schedules. These include, but are not limited to, the following schedules:

- *Land Planning and Building Records NI200491*
- *Territory Records (Records Disposal Schedule – Corporate Governance Records) NI2009-10*
- *Territory Records (Records Disposal Schedule – Ombudsman Complaint Management Records) NI2009-445*
- *Territory Records (Records Disposal Schedule – Security Coordination Records) – NI2009-452*

- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Community Relations Records) NI2009-358*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Compensation Records) NI2009-435*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Equipment and Stores Records) NI2009-436*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Establishment Records) NI2009-437*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedule – Financial Management Records) NI2009-439*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Fleet Management Records) NI2009-438*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Government Relations Records) NI2009-440*
- *Territory Records (Records Disposal Schedules – Industrial Relations Records) NI2009-441*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Information Management Records) NI2009-442*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Legal Services Records – NI2009-443*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Occupational Health and Safety (OH&S) Records) NI2009-444*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Personnel Records) NI2009-448*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Property Management Records) NI2009-449*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Publication Records) NI2009-450*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal Schedules – Strategic Management Records) NI2009-453*
- *Territory Records (Records Disposal Schedule – Territory Administrative Records Disposal schedules – Technology and Telecommunications Records) NI2009-454*
- *Territory Records (Records Disposal Schedule - Environmental Management Records) NI2011-86*
- *Territory Records (Records Disposal Schedule - Parks, Reserves and Public Places Records) Approval 2011 (No 1) NI2011-94*

Records disposal schedules will be assigned to files to ensure disposal of records is completed in accordance with the *Territory Records Act 2002*.

EPD will take all reasonable steps to reduce the cost of records storage through the implementation of an appropriate records disposal program.

EPD will ensure that record destruction is carried out in accordance with best practice applicable to the type of record and its security requirements according to the approved Records Disposal Schedules.

Access to Records

EPD will ensure its records, in whatever format, are easily accessible to authorised users, as well as available to the public via legislated public access mechanisms, such as via the Freedom of Information Act or the Territory Records Act. EPD is proactive and transparent in the release of information and will make every effort to provide simple and timely access to information.

Staff Development

Staff at all levels are responsible for educating themselves about their recordkeeping responsibilities. These responsibilities are in detailed in this policy, supporting procedures and work instructions.

Contractors and Consultants

All contracts with consultants or contractors should address records management requirements, including articulating the return of records at the completion of projects or contract periods. Any person responsible for supervising the activities of a consultant or contractor must ensure they adopt relevant recordkeeping procedures and that a process has been put in place to ensure records are provided to EPD in compliance with Territory recordkeeping requirements.

Authorisation

In accordance with Section 8 of the *Territory Records Act 2002* the policy and procedures have been authorised by the Director-General, Environment and Planning Directorate who is the Principal Officer for the Environment and Planning Directorate (EPD).

The Principal Officer must ensure that EPD complies with the *Territory Records Act 2002* in relation to its records. The Principal Officer is specifically responsible for:

- Approving the EPD Records Management Program and providing a copy to the Director of Territory Records;
- Seeking certification from the Director Territory Records for any aspects of the Records Management Program where non-compliance is necessary for EPD operations; and
- Making EPD's Records Management Program available for public inspection and identifying exempt material such as documents affecting relations with the Commonwealth, the States and Territories, or affecting the enforcement of the law and the protection of public safety, or affecting privacy.

Authorised by

Dorte Ekelund
Director-General
Environment and Planning Directorate
Date:

Environment and Planning

Records Management Program

Procedures Part 1 - Introduction

ACT Government
Environment and Planning

Table of Contents

Introduction

Recordkeeping is an integral part of employment within the ACT Government. All staff have an obligation to capture records that show evidence of key decisions made, actions taken, or advice given, whether it be to internal or external sources.

Records must be captured in such a way that they present a faithful and accurate account of the key events that have occurred. In order to be accurate the record must be shown in context, must be auditable and must be easily retrievable.

The policy and procedures that make up the Environment and Planning Directorate (EPD) Records Management Program (RMP) provide direction on how to improve recordkeeping practices across EPD and allow staff to follow a consistent approach to the creation, storage, retrieval, and disposal of records.

The purpose of recordkeeping is to:

- Manage the life cycle of records, from the design of a recordkeeping system, to the destruction of records
- Capture complete, accurate, reliable, and usable documentation of business activities to meet legal, evidential, knowledge management and accountability requirements
- Manage records as an asset and information resource
- Promote efficiency and economy, both in the management of records and in organisational activity as a whole, through sound records management practices

Purpose

Under the *Territory Records Act 2002* EPD has a responsibility to implement a Records Management Program. The Program contains a Records Management Policy which provides the framework for establishing and maintaining accurate records across EPD, and these procedures, which provide direction on how to comply with the policy purpose.

Scope

These procedures are designed to provide direction as to the why, what, who, and how of EPD recordkeeping practices. The policy and procedures have been developed in conformity with the *Territory Records Act 2002* and Territory Records Office as well as best practice guides developed by the National Archives of Australia and the Territory Records Office.

All staff within EPD, contractors working with EPD, and external vendors engaged by EPD, are obliged to comply with the requirements of the EPD Records Management Program.

Implementation

From the time of implementation all staff are required to comply with the Records Management Program in its entirety.

The Records Management Program will be made available to staff through the EPD Intranet and via electronic record systems. When the Program is updated staff will be provided with details of the update via email. Training sessions will be provided to staff following any significant update to the Program.

References

- Territory Records Act 2002
- Territory Records Office Standard for Records Management No. 1: Records Management Programs
- Territory Records Office Guideline for Records Management No. 3: Description and Control
- Territory Records Office Standard for Records Management No. 4: Access
- Territory Records Office Standard for Records Management No. 9: Records Digitisation and Conversion
- Note for File: A report on Recordkeeping in the Australian Public Service © Commonwealth of Australia 2007

Further Information

Should you require further information or clarification on particular aspects of this Program, or in cases where issues arise which are not covered by the EPD Records Management Policy or Procedures, please contact:

EPD Information Manager
Finance and Operational Support
EPDCorporate@act.gov.au

Records Management Procedures

Obligation

The Principal Officer of EPD has responsibility under the *Territory Records Act 2002* and this Program to ensure that staff of EPD make and keep full and accurate records of the business of EPD. EPD's Principal Officer, the Director-General, delegates responsibility for compliance with the Territory Records Act 2002 to appropriately qualified senior officers of the Directorate. These officers and their relevant delegations are outlined in the Directorate's delegations register. These delegations are regularly reviewed to assess their ongoing suitability.

Financial Resources

EPD will dedicate sufficient financial resources to provide for dedicated records management staff. Sufficient funds will be provided to ensure records management staff are adequately trained and qualified to perform the duties assigned to them.

EPD comply with these requirements through the positions of Information Manager, and Assistant Information Manager. EPD commits to ensuring any staff engaged in these positions will hold appropriate qualifications in the areas of records and information management or sufficient on the job experience to clearly demonstrate their ability to support EPD. If staff employed in these positions do not hold qualifications in records or information management EPD will arrange for staff to undertake, at a minimum, a Certificate IV in Records Management or a similar industry related qualification.

EPD will ensure that staff with dedicated records management responsibilities will hold a minimum Baseline security clearance, or the ability to obtain clearance to this level. If a clearance is not held at the time of appointment, EPD will arrange for a clearance to be obtained.

EPD are the custodian of an extensive range of records that establish the history of land, planning and building, of Canberra. EPD is fully committed to long term management of these records to ensure they are available to future generations of Canberran's. Preservation and conservation of records will be managed as part of the overall funding for records management and will be subject to organisation priority.

Human Resources

The creation, management and retention of records is the responsibility of all EPD staff and contractors. Individuals are responsible for ensuring that they capture records that evidence their business activities, including decisions made, actions taken, and advice given.

All records must be captured into an approved recordkeeping system, and not stored in alternative locations such as network drives, local drives, portable devices, or Outlook.

Staff are responsible for understanding what records they are obliged to retain, and also being aware of what information is of little value and can be destroyed under the Normal Administrative Practice (NAP) provisions of the Territory Records Act. Retaining personal notes, routine conversations via email, or system generated messages, slows down networks and systems and reduces the effectiveness of searching. Staff are responsible for ensuring their personal drives and Outlook accounts are purged of outdated NAP documents on a regular basis.

All position descriptions and duty statements for positions within EPD will contain a requirement to comply with the requirements of the *Territory Records Act 2002* and the EPD Records Management Program.

Senior Executive in charge of Records Management

The Senior Executive in charge of Records Management has responsibility for ensuring compliance with the EPD Records Management Program, including responsibility for:

- Strategic planning for records management activities such as resourcing, staffing and budgeting
- Ensuring good recordkeeping principles are incorporated into all business processes
- Obtaining expert advice where required on recordkeeping issues and practices
- Facilitating internal and external reporting requirements
- Ensuring appropriate resources are allocated to enable the Program to be established and maintained
- Managing staff charged with specific records management responsibilities

Records Management Staff

The Senior Executive in charge of Records Management is responsible for ensuring that positions with records management responsibilities are clearly identified and their duties outlined in position descriptions. These duties include, but are not limited to:

- Encouraging compliance with the records management program
- Incorporating recordkeeping into all business practices and processes
- Obtaining expert advice on recordkeeping
- Encouraging appropriate resourcing of the Program
- Designing, developing, and maintaining recordkeeping systems
- Preparing policies, procedures and work instructions related to efficient records management operations
- Facilitating public access to information via the Freedom of Information Act, the Freedom of Information Act, and the Information Privacy Act
- Contributing to the development and review of Whole of Government Functional Thesauri and Records Disposal Schedules that are utilised across the ACT Government
- Sentencing records against assigned Records Disposal Schedules
- Monitoring service providers

Managers and supervisors

It is the responsibility of every business manager or supervisor to support and encourage sound recordkeeping practices within their team or workgroup. Managers and supervisors must:

- Ensure that staff have an awareness of the Records Management Program and associated resources
- Make sure that staff have access to tools, procedures, and expertise to help them carry out their recordkeeping responsibilities
- Encourage compliance with the EPD Records Management Program
- Have detailed knowledge of business recordkeeping requirements in areas for which they are responsible

- Ensure that records are made as evidence of business activities and those records are captured into an approved recordkeeping system
- Provide guidance and on the job training in good records management practices
- Monitor staff to minimise the storage of records in alternate storage locations, such as local drives and Outlook

Human Resource Managers

The EPD induction and general training programs must include basic records management principles, process, and practices and the need to comply with the EPD Records Management Program.

EPD position descriptions must include reference to the requirement of EPD employees to understand and comply with the *Territory Records Act 2002.*

Web Content Manager

Web-based records must identified and maintained in line with the EPD Records Management Program. Web Content Managers are responsible for monitoring compliance, document owners are responsible for ensuring accurate version control is applied to online content.

System Administrators

System administrators are responsible for maintaining EPD systems that contain records, including maintaining the integrity and authenticity of electronic records and their associated metadata.

System administrators are required to maintain detailed records about access and security in relation to the recordkeeping system and detail unauthorised or inappropriate access.

System administrators for ICT systems will maintain records of user accounts, inappropriate access, and undertake auditing to ensure that records of EPD are protected against destruction.

Contractors and Consultants

Contractors and consultants must adhere to the EPD Records Management Program, including the need to make and keep full and accurate records as part of their service delivery to EPD.

Contracts for service delivery must include a component outlining the recordkeeping requirements that contractors and consultants are required to adhere to.

Exit Protocols

Prior to staff resignation, transfer, or extended leave, documents that need to function as records must be saved into an approved recordkeeping system. All other documents that are not corporate records must be deleted and folders cleared prior to the leave period, or departure, from EPD. This includes network drives and Outlook folders.

Network and local computer drives do not meet recordkeeping requirements and must not be used to store records that must be retained by EPD. If records have been saved to a network or local drive by staff all documents must be transferred to Objective prior to departure.

Managers are responsible for monitoring staff and ensuring that enough time is provided to action these requirements prior to leave or resignation.

If a staff member has been responsible for a business critical project or significant or long term project with the Directorate, that staff member is responsible for ensuring that they have transferred all essential email records to Objective.

In the event that a staff member exits prior to transferring their Outlook records, the relevant manager is responsible for identifying that retrieval of critical email records are required.

Restoration and access to Outlook accounts following resignation requires the authorisation of EPD's Director-General, as well as the Head of Service, before access is provided. Managers are required to send a business case outlining the reason and requirement for access to EPDICT@act.gov.au. Following submission of the business case the ICT team will progress approvals and arrange for access.

For security reasons access will only be provided to a member of the Information Management team for a limited period of time. The records team will coordinate with an appropriate subject matter expert to determine what email records should be transferred into a recordkeeping system for long term retention.

Cabinet and Executive Documents

All records that pertain to cabinet and executive documents are managed in accordance with the ACT Cabinet Handbook.

Within EPD Cabinet and Executive Records are managed by the Communication, Government Services, and Executive Support (CGSES) team. The management of these records includes the application and removal of access privileges in compliance with the ACT Cabinet Handbook.

For assistance in relation to Cabinet and Executive records email to EPDCab@act.gov.au.

Dispute Resolution

Introduction

Arrangements must be made for the resolution of disputes between the Director of Territory Records and EPD about whether EPD is complying with the *Territory Records Act 2002* and the EPD Records Management Program.

Resolution steps

EPD will resolve disputes with the Director of Territory Records though the use of the following levels of escalation.

Level 1

An action office may at any time refer a problem or an issue in dispute to the Director of Territory Records or the Senior Executive in charge of Records Management. The Senior Executive in charge of Records Management will negotiate with a Policy Officer within the Territory Records Office.

Disputes not resolved to the satisfaction of the Senior Executive in charge of Records Management or the Territory Records Office shall be escalated to level 2.

Level 2

The Director of Territory Records and the Senior Executive in charge of Records Management shall make every possible effort to resolve the matter by negotiation.

Disputes not resolves to the satisfaction of the Senior Executive in charge of Records Management (in the case of an EPD raised issue) or the Director of Territory Records (in the case of a Territory Records Office raised issue) shall be escalated to level 3

Level 3

The Territory Records Advisory Council and the EPD Senior Executive responsible for Records Management shall make every possible effort to resolve the matter by negotiation.

Disputes not resolves to the satisfaction of the EPD Senior Executive Responsible for Records Management (in the case of an EPD raised issue) or the Director of Territory Records (in the case of a Territory Records Office raised issue) shall be escalated to level 4.

Level 4

A mediator shall be selected from those qualified in the field of records management. The parties will implement the determined process and conclude the matter as directed.

Detailed procedures

Further documents that form part of this program include:

1. *Records Management Program – Procedures 01- Introduction to Records Management Program*
2. *Records Management Program – Procedure 02 – Records Lifecycle (Creation, retention, disposal)*
3. *Records Management Program – Procedure 03 – Public Access to Records*
4. *Records Management Program – Procedure 04 – Management of Business Critical Records (Business Continuity, Vital Records, Succession Planning)*
5. *Records Management Program – Procedure 05 – Managing and Preserving Territory Archives*
6. *Records Management Program – Procedure 06 – Digitisation and Conversion*
7. *Records Management Program – Procedure 07 – Objective Administration*

References

Territory Records Office Standards for Records Management

Territory Records Standard – Number 1 – Records Management Program

Territory Records Standard – Number 2 - Appraisal

Territory Records Standard – Number 3 – Records Description and Control

Territory Records Standard – Number 4 – Access

Territory Records Standard – Number 5 – Recordkeeping and Outsourced Government Business

Territory Records Standard – Number 6 – Digital Records

Territory Records Standard – Number 7 – Physical Storage of Records

Territory Records Standard – Number 8 – Business Continuity and Records Management

Territory Records Standard – Number 9 – Records Digitisation and Conversion

Territory Records Office Guidelines for Records Management

Guideline Number 1 – Records Management Programs

Guideline Number 2 – Appraisal

Guideline Number 3 – Records Description and Control

Guideline Number 4 – Access

Guideline Number 5 – Recordkeeping and Outsourced Government Business

Guideline Number 6 – Digital Records

Guideline Number 7 – Physical Storage of Records

Guideline Number 8 – Business Continuity and Records Management

Guideline Number 9 – Records Digitisation and Conversion

Glossary of Terms

A detailed glossary of terms is available on the EPD SharePoint site.

Environment and Planning

Records Management Program

Procedures Part 2

Records Lifecycle

ACT Government
Environment and Planning

Creating Records

Overview

The *Territory Records Act 2002* defines a record as:

> *"Information created, received and maintained as evidence and information by and organisation or person, in pursuance of legal obligations or in the transaction of business. This recorded information must be maintained or managed by the agency to provide evidence of their business activities. Records can be written, electronic or in any other form"*

In plain English this means that what you do on behalf of EPD and the ACT Government, must be evidenced, and retained for a long as it is relevant. The work you do often has relevance for much longer than you will work for the ACT Government, so capturing it in records allows future staff to have access to the information they need to understand what you did, when you did it, and why you did it. Keeping records is not just about what you need to do your job today, it is about what future staff will need to understand what you did, and apply it to future decision making.

While this could be seen to indicate every piece of information you receive or send needs to be retained, in reality large volumes of information you create, in particular emails you send, do not need to be retained as records. Informal email conversations, personal notes, and system messages can be destroyed under the Normal Administrative Practice (NAP) provisions of the Territory Records Act when they are no longer relevant.

Retention of unnecessary information hinders accurate recordkeeping by reducing the efficiency of electronic recordkeeping systems. Using common sense to consider the value of information you are creating, and whether to add it to a recordkeeping system, will help keep these systems running smoothly by reducing the volume of non-records stored within these systems.

All EPD employees are required to develop an understanding of what is, and what is not, a record and ensure that records that evidence decisions made, advice given, or actions taken, are retained to facilitate accurate decision making.

Creating Records

A file should be made as soon as a need is identified. If a staff member is aware that a project will be commencing shortly, the first step to managing that project should be to create a file to maintain records of that project. If certain activities are managed by financial year, on the first day of each financial year a file should be created to maintain that content. If a staff members roles involves specific transactions, such as development applications, customer complaints, Ministerials or public access processes, a file should be created as soon as the first communication is received regarding that transaction. On any occasion that records (documents that have corporate value) need to created, the first step should be to create a file to store those records. Adding documents to network folders, Objective folders, or retaining in Outlook, are not suitable locations for storage of corporate records.

When creating records staff should consider the following:

<u>*Records should be accurate*</u> and correctly reflect what has been done, decided, or communicated and also include any subsequent actions and decisions. To maintain context, all records related to a project, process, or transaction, should be maintained together in a single file. Adding sub-folders to a file can assist in sorting similar documents.

<u>*Records should be complete*</u>. In order to be complete records must contain an accurate history of all versions created, and include metadata that articulates the history and context of the record. The context, including ensuring records are retained in a correctly classified file, contributes to the completeness of a record.

Records should be authentic and show the business transactions that they purport to represent. Records should be able to demonstrate that they have not been tampered with, or otherwise altered, exempt in ways that are authorised, detectable and recorded in an approved recordkeeping system.

Legislative, administrative and budget changes must be monitored to identify the need for new records to be made, or when the requirements for certain records have changed.

Staff must identify to the Senior Executive in charge of Records Management if a change is required to recordkeeping processes or systems.

Types of Records

Below are examples of a variety of records you may encounter in your with EPD:

- Correspondence
- Procedures
- Contracts
- Reports
- Publications
- Policies
- Media releases
- Proposals
- Strategic and business plans
- Guidelines
- Licences
- Minutes
- Financial statements
- Vouchers
- Payments
- Journals
- Remittances
- Receipts
- Budget estimates
- Credit notes
- Drawings
- Plans
- Warranties
- Agreements
- Maintenance history
- Environmental impact statements
- Disaster plans
- Tendering

Corporate Records are not limited to the above examples.

In some situations the above examples will not constitute records.

Staff members will need to make a decision about the relevance of the document, and the level of importance before determining that a document is a corporate record.

When is it a Record?

EPD is required to create and maintain information in the form of records, in order to meet accountability and legislative requirements. To determine if a record has value and should be added to an approved recordkeeping system, ask yourself the following questions:

1. Does it relate to your work?
2. Does it evidence a decision you have made?
3. Does it evidence advice you have given?
4. Does it evidence advice you have received?
5. Does it evidence a transaction with EPD?

If the answer to any of these questions is 'yes' then it should be retained in an approved recordkeeping system.

Documents that should NOT be added to an approved recordkeeping system include (but are not limited to):

- Personal documents
- Routine email conversations
- System messages (such as HR21 notifications)
- Duplicates of documents already retained in an approved recordkeeping system

Understanding Functional Classification (Primary Keywords)

The ACT Government uses a thesaurus of terms developed by the Territory Records Office to obtain consistency across government. These thesaurus terms are then linked to records disposal (retention) schedules, which define the retention term for the record.

These terms are broken up by functions, with each function having a group of activities, and subjects, associated with it.

A full list of functional terms is available from the Territory Records Office intranet.

Understanding the Functional Approach

Functions – The first level in the classification hierarchy is the broad descriptor of what the file will relate to. This could include corporate terms such as Financial Management, or terms specific to environment and planning activities such as Land Management and Development Control, Environmental Management, or Parks Reserves and Public Places.

Activities – The second level in the classification scheme is literally the activity that is being undertaken in relation to the functional term. This is a specific descriptor that is applied to the file. This can include general administrative terms such as Budgeting or Recruitment, or activities that are more specific to EPD's role, such as Territory Lease Administration or Heritage Assessments.

Subject – The third level in the classification are clarifying terms for common administrative activities, such as Accounting. These terms are referred to as "subjects" and are generally made up of words that most closely relate what the record is about.

An accurate functionally classified file must contain both a Function and an Activity keyword term. Subject descriptors should be used for further classification of files if they relate to a common administrative activity.

Learning functional classification will require lateral thinking, as these terms do not always coincide with previously used rules for file titling.

When we classify functionally, we need to ask ourselves:

- What is the overarching purpose of this file? What does it relate to?
- What activity are we undertaking in relation to this file?
- Are there any transactions or topics under this activity to be more specific?

When you have read the contents of your documents the final answers might be:

- We need to manage the agencies financial resources
- We will do this by preparing a budget
- Specifically we are looking at the budget for our capital works program

Using this logic our classification would look like:

- FINANCIAL MANAGEMENT as the function
- Budgeting as the activity
- Capital Works as the subject

We use the function, activity and subject terms from the thesaurus to form part of our file title. Using the example above our file title would appear as below:

Free Text - FINANCIAL MANAGEMENT: Budgeting - Capital Works

How to Title Files

Files are to be titled using a combination of terms (function and activity) from the Territory Whole of Government Thesaurus and additional free text determined by the file creator. Additional free text is used to distinguish the file from other similarly classified files.

Free Text Naming Conventions

A good file title reflects the contents of a file, telling the 'story' of an activity, project, or program. A good file title helps you and others to find relevant information quickly. Free text is used to describe the purpose of the file. Free text file titling should be used in addition to functional thesaurus terms.

Details of the EPD requirements for naming files, folders, and documents can be found in the EPD Best Practice Guide – Accurate Naming of Records. This document, as well as all other recordkeeping guides and work instructions, can be found on the EPD intranet.

EPD Best Practice Guides form a part of the EPD Records Management Program endorsed by the Director-General. These guides must be used to accurately name files and documents that are records of EPD's business activities.

If a specific file or document type requires an exemption to the approved naming conventions, approval must be sought from the Senior Executive in charge of Records Management before that naming convention can be adopted.

Managing Email

Introduction

Email is the principle form of communication within EPD and between EPD, its clients, and business partners. In many cases email has replaced telephone conversations, corridor meetings, and brainstorming sessions.

Due to the nature of email, many staff receive large volumes of email that should not be retained, or saved to a recordkeeping system. For some staff that manage large volumes of routine work, such as assisting with IT or HR, more than 50% of email received daily could potentially be considered normal administrative practice and could be deleted when no longer required.

Making decisions about what emails to retain should be considered in the same way you consider saving any other type of document.

- Does the email evidence advice you have given or received?
- Does the email evidence an action you have given, or a direction you are required to follow?
- Does the email evidence work you are doing on behalf of EPD?

If the answer to any of these questions is yes, then you should be saving the email to an appropriately classified file in an approved recordkeeping system.

Emails that are business records should be added to an approved recordkeeping system as soon as practicable.

Your Outlook account is only available to you. If you are not filing your emails, the information you are managing may be lost forever, and is likely to negatively impact on the work of the Directorate.

Under no circumstances should email records be maintained solely in Outlook.

Maintaining emails for personal reference

Many staff within EPD maintain comprehensive folders of emails within their Outlook accounts. These folders represent an easy to access history of work that is structured in a personal way that makes sense to you as an individual.

It is acceptable for staff to maintain personal reference material, within reason. Holding extremely large Outlook accounts can impact on network performance. Staff should comply with the Shared Services ICT Acceptable Use of ICT Resources Policy when retaining folders within Outlook.

Staff should also ensure that any corporate records are saved to an approved recordkeeping system, even if they have also saved a local reference copy in Outlook.

Responsibilities

All employees are responsible for capturing **external** emails sent directly **to** them. These should be saved as soon as practicable after being received. If the email is sent to multiple EPD recipients, a primary contact, such as the project manager, should be nominated to store any incoming correspondence to avoid duplication.

Employees who send a business message **to** another EPD staff member are responsible for saving the email to an approved recordkeeping system. The recipient of the email should **not** save the email. It is the responsibility of the sender to retain it as evidence of their business activity.

Employees must **not** save emails from external or internal sources that are **CC'd** (courtesy copy) or **BCC'd** (blind courtesy copy) to them. CC copies are for information only to keep someone 'in the loop' they are not to be retained as a record.

When sending internal emails requesting input or action, staff must include a reference to the relevant file in Objective or HP RM so the receiving staff member is aware of where to save relevant records.

Sending Emails

Email is inexpensive and easy to use, so it is often distributed widely and copied indiscriminately to people who don't need to receive it.

Before sending an email, you should carefully consider who needs to receive the message. Where possible only include a single individual, or a small group, and only copy in those staff that legitimately need to be included.

A good rule to follow when using the CC field is to see if you can articulate within the email why you have copied each person. If you aren't able to articulate why an individual has been copied into the email, they probably don't need to receive it.

Email Subject Line

The subject line of an email determines what kind of attention the email will receive from the recipient. The subject line also allows the priority of the message to be reinforced or provide the recipient with an indication of what action they are required to take.

Email subject lines should:

1. Contain enough information that the content can be determined without having to open the message
2. Include the following elements:
    a. The name of the entity to which the email refers i.e. a project, development application, or similar
    b. The purpose of the message i.e. agenda, article, or what action the receiver should take
    c. A reference to any relevant files (if sending internally)
3. Be in plain English
4. Not include abbreviations or acronyms
5. Not be empty or use default subjects such as 'Re', 'Fwd' or the name of an attachment.

Email Threads

An email thread is a multi-part virtual conversation on a given topic.

When replying to an email the subject line of the email should not be changed while the subject remains the same. If the subject of the email changes the subject line of the email should be changed to reflect the new content or a new email should be started to address the change in content.

Email threads must be saved into a recordkeeping system in the same way as any other document. Each reply should be considered as a new version of a single document rather than considered in isolation. Email replies in one thread can be saved as a new version of the original email in Objective, or depending on their importance, saved as individual emails.

Under no circumstances should information be deleted or modified within an email thread, this impacts the integrity and authenticity of the content.

Multiple Subjects

If multiple subjects need to be discussed it is advisable to send each subject in its own email to allow more accurate filing and titling. If multiple subjects need to be addressed in one email clearly define all content within the subject line of the email.

Email Content

The content of the emails should be clearly and concisely presented. A useful technique is to use bullet points, which can be structured to advise the recipient of:

- What the email is about?
- Why it is being sent?
- What needs to be done?
- When does it need to be done by?
- What are the consequences if action is not taken?

Adding Attachments

Large attachments slow down systems particularly if they are sent to many recipients.

If the email is being sent internally, it is not acceptable to send copies of documents. Objective or HP RM references should be utilised and attached to every internal email.

When sending documents externally consider the sensitivity of the documents, whether there are privacy considerations, and whether each of the recipients actually needs to be included in the email.

Always double check the spelling of email addresses for customers and stakeholders to ensure the correct person will be receiving the email.

Sentencing and Disposal of Records

Introduction

Sentencing is the process of appraising records. Appraisal can include:

- Retention, deletion or destruction of records in or from recordkeeping systems
- Migration or transmission of records between recordkeeping systems
- The transfer of custody and ownership of records.

The *Territory Records Act 2002* gives the Director of Territory Records (the Director) the responsibility of authorising the disposal of records made and/or received by EPD as a result of its business activities. There are several ways EPD can legally dispose of its records. The Territory Records Act allows disposal where it is:

- Required by another law
- With the permission of the Director of Territory Records
- A normal administrative practice (NAP) not disapproved by the Director.

The way in which the Director permits the disposal of EPD records is by the use of approved Records Disposal Schedules (RDS). These schedules are issued after a detailed examination and appraisal of the value of records has been completed. The schedules describe classes of records, state how long they are to be retained and recommend where they should be kept when no longer in current use. Disposal schedules can be selected from the Territory Administrative Common Administrative Functions, or from functions more specifically aimed at the responsibilities of EPD.

A full list of Disposal Classes can be found on the Territory Records Office Intranet

Records Disposal Schedule – Land, Planning and Building Records

Land, Planning and Building Records (NI 2004-91) covers the records for the following functions:

- Building Services Control
- Land Management and Development Controls
- Territory Plan and Strategic Planning Policy

Records Disposal Schedule – Environmental Management Records

Environmental Management Records (NI2011-86) includes a range of administrative terms such as committees, as well as specific environmental functions, including:

- Animal Welfare
- Conservation
- Grant Funding
- Horticultural Services
- Inspections

- Licensing
- Mapping Programs
- Research
- Vegetation Management

Records Disposal Schedule – Parks Reserves and Public Places Records

Parks, Reserves and Public Places Records (NI2011-94) includes a range of administrative terms such as committees, as well as specific functions, including:

- Conservation
- Designing
- Fire Management
- Horticultural Services
- Land Data and Mapping
- Mapping Programs
- Research
- Security
- Vegetation Management
- Visits

Records Disposal Schedule – Waste Management Records

Waste Management Records (NI2004-336) includes a range of administrative terms related to waste management.

Sentencing of Records

Sentencing involves the examination of records in order to identify the disposal (retention) class to which they belong and the actions that should be taken based on that class. Records must always be sentenced based on their content, not on the title of the file.

Before any record is sentenced it the disposal class assigned to the record must be reviewed and confirmed. In the event a file contains records that could be determined to belong to more than one disposal class the content should be sentenced in accordance with the disposal class having the longest retention period.

The steps involved in sentencing (reviewing) are:

- Ensure the file is closed so that no further documents can be added
- Examine all documents within the file (regardless of format) and determine the appropriate classification for the content
- Review the Records Disposal Schedule that was applied during file creation and determine that it is still relevant to the content of the file
- Apply the sentence to review, retain, archive, or destroy, based on the requirements of the applied Records Disposal Schedule
- Apply the “action by” date to which the required action must be complete.

When sentencing multiple parts of one file, the complete file must be retained until all parts of the file have reached the end of the period for which they must be retained. In the case of hard copy files the parts which are not required should be sent to off-site storage until the actions can be applied.

Normal Administrative Practice (NAP)

Normal Administrative Practice (NAP) allows destruction of ephemeral, duplicate, or transitory material to be carried out as part of normal agency practices and procedures. NAP is designed to

reduce the need for formal approval for destruction for ephemeral information. It is not intended as a replacement for approved records disposal schedules.

Material that can be destroyed using the NAP provisions:

- ☑ Working papers consisting of rough notes, calculations, or diagrams used for the creation of records
- ☑ Duplicates and copies of documents where the original is safely retained within an approved recordkeeping system. Ensure this is the case before destroying the copy
- ☑ Drafts where the contents have been reproduced in a final document
- ☑ Published materials used as reference only including pamphlets, leaflets, brochures and PowerPoint presentations
- ☑ Information from other organisations that are not essential to EPD's functions
- ☑ Personal material such as invitations, tickets and brochures.

Material that CANNOT be destroyed using the NAP provision:

- ☒ Official records, records that are essential to the ongoing business of an agency. For example, registered files, official minutes, regulations, agreements, legal and financial records which affect or define EPD's functions and activities
- ☒ Records required to be retained by Records Disposal Schedules approved by the Director of Territory Records or information required to be retained for any specific time by an Act or Regulation
- ☒ Records containing essential information of the rights and obligations of the Territory or of any persons
- ☒ Information likely to be required for the determination of any action in any inquiry, court or tribunal
- ☒ Material of significance or public interest relating to political, social and economic affairs and history of the Territory.

Environment and Planning

Records Management Program

Procedures Part 3

Public Access

ACT Government
Environment and Planning

Public Access

Introduction

The Territory Records Act 2002 provides for a general right of access to records to meet the obligations of the government to:

> *"…support accountability and democratic government and to enrich the community through a source of cultural and collective memory".*

The Environment and Planning Directorate (EPD) must manage records in such a way that ensures that the information they contain remains accessible over time. This should include:

- Ensuring that unauthorised destruction of records does not take place
- Providing a secure storage environment to prevent loss or damage
- Undertake conservation surveys and treatments

In June 2011 the Chief Minister made a Ministerial Statement on Open Government which stated that the ACT Government is *"taking a broad approach to enhance the openness of the way we govern, encompassing transparency, participation and collaboration"*. On the issue of transparency the Chief Minister further stated *"as a first principle information available to the Government should be made available for use by the community"*.

These principles of transparency, collaboration and community engagement form the basis for the approach EPD takes in responding to any legislative or legal request for information.

Any staff member responding to a public access request should do so in a way that reflects the principles of open government.

The approach to the release of information is that all information should be made available, unless there is a very clear reason that it should not. Consideration should be given to records that have personal privacy implications, relate to legal/professional privilege, matters between the Commonwealth and States, or commercial in confidence, but should still be approached with a view to transparency and accountability.

Legislation and References

Freedom of Information Act 1989

Territory Records Act 2002

ACT Government Open Government Website

CMTEDD Customer Service Standard

Freedom of Information (FOI)

Within EPD the Information Management Team coordinates and manages requests made under the *Freedom of Information Act 1989*. This includes:

- Receipt and acknowledgement of incoming requests
- Requesting documents from line areas that could be stored in hard copy files, Objective, HP RM, network and local drives, or in a staff members email
- Preparing documents for scheduling and release, including masking content that is outside of the scope of the request, or is exempt from access
- Briefing the appropriate decision maker
- Providing the finalised documents and schedule to the applicant
- Publishing the release to the ACT open government website
- Ensuring the entire process is clearly documented, completed within legislated timeframes and in compliance with recordkeeping requirements

Requests for access

Any person or organisation may make an application, in writing, to the relevant directorate, or minister, to obtain access to records held by the agency or minister.

Under section 14 of the Freedom of Information Act a request for access must provide sufficient information as is reasonably necessary to enable a responsible officer of the agency, or the minister, to identify the document.

This means that the applicant must be as clear as possible in articulating their request to allow the Directorate to identify relevant documents and provide them within a reasonable timeframe.

To ensure that requests are managed via the appropriate process, be it under the Territory Records Act, or the Freedom of Information Act, or the Information Privacy Act, applicants are encouraged to clearly state which Act they are requesting access under.

An “in writing” request can include a request via email, as long as all required criteria are included in the email.

Where a request is not sufficiently specific the Directorate will make all reasonable attempts to contact the applicant to refine the scope of the request.

In the event the scope of a request is too narrow and would result in no records being released, the Directorate will contact the applicant to discuss the scope and the best way to achieve the best outcome for the applicant.

Access

When EPD makes a decision to grant access to documents, that access can be provided in the following ways:

- Provision of a copy of the records
- Inspection of the original records
- If the record contains sound or visual images, arrangements will be made to allow the applicant to see or hear the content of the records
- If the document is an audio recording or one in which words are contained in the form of shorthand or in codified form, provision of a written transcript of the words recorded or contained in the document

The applicant can indicate their preferred method of access.

As a general principle EPD encourages access through digital means, such as providing the applicant with an emailed copy of documents in PDF format, or providing access to large documents via secure cloud transfer. This process results in a significant reduction in the amount of waste paper generated by the Directorate.

If the preferred method of access indicated by the client will have a significant impact on the operational efficiency of the Directorate, has the potential to cause damage to delicate records, or will result in a copyright infringement, the Directorate will negotiate an alternate method of access that meets the needs of the client.

Under Section 16 of the *Freedom of Information Act 1989* an agency is not obligated to respond to a request where the information requested does not exist within a document, for example where the information being requested is held in a financial management database.

In cases where a document would need to be created by EPD to provide a response to a request, consideration should be given to the scope of the request, how the request would divert the resources of EPD, and whether the release of information may or may not benefit the public.

As with all public access requests the main guiding principle should be the ACT Government's Open Government Policy.

If it is possible to easily source the data and provide a response to the client, without having significant consequences on the delivery of Directorate services, every effort should be made to response to the request within the legislated timeframes.

Open Government Policy

EPD is committed to complying with the Open Government Policy and its requirements to publish responses to Freedom of Information Requests on the Open Government website within 14 days of being provided to the applicant.

Exemptions to online publishing will be on the grounds of the FOI exemptions as outlined in the Act.

Special care will be taken to review all FOI responses before they are published online to ensure the privacy of the applicant, and other community members are protected.

The Open Government Online Publishing Policy can be found through this link.

http://sharedservices/ACTgovt/ICTdocs/FOI-Online-Policy.pdf

Processing FOI Requests

Procedures for the processing of Freedom of Information applications, including business rules for specific types of applications commonly received by EPD, can be obtained by contacting Information Management team.

Requests made under the Territory Records Act 2002 (Archives ACT Requests)

Under *Section 26* the *Territory Records Act 2002* a record of an agency is open to public access 20 years after the record came into existence. The Act allows for those records to be released on the next Canberra Day following the 20 year anniversary of the creation of the record.

The Senior Executive Responsible for Recordkeeping may determine it appropriate to release additional records younger than 20 years old, where it would provide additional context or assist in community research.

The majority of requests under the Territory Records Act relate to research for publication or personal history and the Directorate takes an active approach to providing as much information as possible to assist the researcher in completing their request.

Requests for Access

A person who wishes to have access to a record of an agency may apply to the agency. In most cases requests for access under the Territory Records Act are managed by Archives ACT on behalf of the ACT Government. Requests can be made via the Archives ACT website.

As part of their service to the ACT Government, Archives ACT assess the incoming request, determine which agency or agencies should respond and where possible provide a list of relevant file numbers or cartons in which records may be stored. This information is included in the email request to the agency requesting access.

An agency must take reasonable steps to assist a person to make a request in accordance with the Act. This can include assisting the customer in lodging a request via Archives ACT, or responding directly to the client when appropriate.

Regardless of the way in which the request for information is received EPD will respond in a customer focussed and time efficient manner to ensure the client receives assistance in accessing the relevant records.

Access

Where possible, EPD will provide original files to Archives ACT, who maintain a reading room at the Woden public library. Archives ACT supervise public access of customers reviewing records to ensure that the files are not damaged, records are not removed, and assist customers in making copies if required. Records are maintained in a secure environment when not being reviewed by customers.

When it is not possible to provide original records due to the age of the record, the delicate nature of historical records, or the record is held digitally an alternative method will be arranged. This could include prints or photocopies of documents, or scanning extremely delicate records and emailing to Archives ACT who will pass onto the client.

Exempt documents

Any record younger than 20 years old is exempt from access under the Territory Records Act. The Directorate may choose to release records younger than 20 years old if they relate to the request and would assist the customer in their research.

The only exemptions possible under the Territory Records Act are for personal privacy, protection of law and safety, legal professional privilege, protection of relationships with the Commonwealth or states, or records the release of which would be in contempt of the Assembly or a Court.

It is **not** permissible to restrict access to records that are more than 20 years old on the basis of commercial confidentiality.

Review of decisions

The Territory Records Act does not specify the means in which an application made under this Act can be reviewed.

If an applicant would like to review a decision they should contact the Senior Executive responsible for Records Management via email to EPDCorporate@act.gov.au.

If the applicant is not satisfied with the response of the Senior Executive responsible for Records Management they can contact the Director-General for further review.

Search and Retrieval of Documents

Documents that may be requested under the Territory Records Act primarily include hard copy records such as leasing files, building files, maps retained in the plan room and surveyors office, or historical records maintained offsite.

Because of the way in which records have been maintained historically, by location, rather than against a specific architect or planner, in most cases a request must include a block or section to enable it to be progressed.

In most cases the Information Management Team will source all relevant records, however if additional assistance is required staff are required to provide any assistance they can in completing responses to requests under the Territory Records Act.

Processing Territory Records Act Requests

Procedures for the processing requests made under the Territory Records Act, including business rules for specific types of applications commonly received by EPD, can be obtained by contacting the Information Management team. .

Legal Requests –Subpoena or Non-Party Production

Requests for access

A legal access request for information must be lodged at the EPD customer service shop front at Dame Patty Menzies House. Most lodgements will come with a processing fee attached, which must be processed by customer services before the request is forwarded to the Information Management Team for processing.

The request must clearly state if it's a subpoena or non-party production and clearly detail what information is required to be provided, and in what timeframe.

Requests for access to EPD documents can commonly be directed to "the ACT Planning and Land Authority" "ACTPLA" "BEPCON" "DEECEW" or "Environment and Sustainable Development". EPD will accept lodgement of legal requests regardless of whether it is issued correctly, as long as the scope of the request covers documents held by EPD.

In the event the documents requested fall outside of EPD, EPD will notify the applicant of how to obtain the documents.

Timeframe

A minimum of seven days must be allocated to allow the Directorate to respond to a request. If seven days are not allowed, contact the officer listed on the document to advise enough time has not been provided and request an amended due date. Where possible the applicant should email to confirm the new due date in writing.

Search and Retrieval of documents

Search and retrieval of records should commence as soon as practicable after receipt of the request. Records related to a request could be stored in Objective, HP RM, hard copy files, network drives,

local drives, USB devices, or email accounts. If a staff member is asked to assist in responding to a request, that staff member should review all storage options before replying to the coordinating officer.

In order to ascertain the scope of the request the coordinating officer will run a search of both Objective and HP RM before forwarding the request to relevant line areas. A snapshot of each search will be saved to the request file for reference by internal staff responding to the request.

After completing a snapshot search the coordinating Officer will contact internal staff who may hold records relevant to the request. Within EPD this is considered to be any staff member employed by the Directorate.

All legal applications will to be sent to senior managers likely to hold records related to the request. Access to legal requests files are limited to only those staff that are responsible for responding to the request. If additional staff require access authorisation must be provided by the relevant senior manager before access can be provided.

Officers providing records in response to the legal request should interpret the request as broadly as possible to ensure that all relevant documents are provided.

In the event the records are stored in Objective a reference to the records should be forwarded to the coordinating officer as soon as possible. If the relevant records are stored within HP RM, a network or local drive, USB device, or email account, the records should be forwarded to the coordinating officer, where possible. If the volume of items is not practical to send via email all items should be saved directly into the legal request file by the responding officer.

Responses are to be forwarded within one week (five working days) of receipt of the email from the action officer.

Access to sensitive records

The Environment and Planning Directorate maintains historical records that contain links to Aboriginal and Torres Strait Islander (ATSI) history, as well as records that detail land that is significant and sensitive to Aboriginal and Torres Strait Islander people.

EPD will maintain these records in such as a way as to ensure they are available for access by Aboriginal and Torres Strait Islander people now and into the future.

Historical records that connect Aboriginal and Torres Strait Islander people with their history may contain language or concepts that are highly upsetting. On that basis, access to records related to the history of Aboriginal and Torres Strait Islander people will be managed in a sensitive and considered way.

EPD will provide a private space for review of historical records by people of Aboriginal and Torres Strait Islander origin, and will provide access to counselling and support should it be necessary.

The Directorate will maintain a register of sensitive records as part of this Program and will continuously update the register as records are identified.

Records that are historically sensitive to Aboriginal and Torres Strait Islander people will be stored in such as way as to limit unnecessary access and inadvertent release of information that may be sensitive to the Aboriginal and Torres Strait Islander people.

Environment and Planning

Records Management Program

Procedures Part 4

Business Critical Records

ACT Government
Environment and Planning

Disaster Preparedness and Recovery

Introduction

Records Management Programs must establish a regime for the proper care of EPD records particularly records that are vital to the operations of the Directorate. This includes preservation strategies and disaster prevention and recovery processes.

Vital Records

Management of vital records should be considered as an integral part of business planning and preparation for business continuity in the event of a disaster. Understanding what vital records are held by EPD allows the Directorate to prepare for reestablishment of essential business processes in the even a disaster occurs.

Each business unit should develop a list of its vital records that are required to maintain business in the event of an emergency.

Vital records are defined as *"those records that are essential for the ongoing business of the authority, and without which the authority could not continue to function effectively"*. Therefore vital records should be considered those records that would be required to re-establish EPD in the event of a disaster.

Vital records include records that are required for:

- Resumption and/or continuation of operations (including records which are needed to conduct emergency operations during a disaster
- Recreation of the legal and financial status of EPD
- Fulfilment of obligations to local, state and federal governments and outside interests

In the event of a disaster it is critical for re-establishing the operations of EPD that vital records are preserved. Although all measures are taken to prevent accidents and disasters, such as off-site back up of disks, it is worth some preparation to ensure that vital records are preserved.

Currently, actions include a daily back-up of the entire network, including:

- All personal directories and drives (e.g. H drives and Outlook settings)
- Records management systems and other databases (e.g. Objective and HP RM)
- Financial management systems (e.g. Oracle)
- Personnel records (e.g. Chris 21)

Critical business systems, such as Objective and HP RM, have disaster recovery plans based on their criticality to government.

Protecting Vital Records

There are measures which can protect vital records in the event of disaster. These can include:

- Fire proof storage
- Closing compactus at night to limit the spread of fire
- Remote storage and back-up of essential data.

Some of EPD's vital records are already in electronic form and can easily be duplicated and held at a remote location. Assessment of the likelihood of particular types of disaster and most cost effective means of preventing against them must be made. Once the cost of different levels of protection

against the cost of potential loss of records has been made, decisions about protection methods can be made.

Risk Assessment Disaster Planning

One of the key elements to any recovery from a disaster is identifying the possible risks that could cause damage to records. These may include:

- Flood
- Fire
- Earthquake
- Mite or insect damage
- Vermin damage
- Hard disk failure
- Back-up failure
- Storage medium failure

This is not meant to be comprehensive, it is provided to identify possibly risks that could potentially cause damage to EPD records, in whatever format they exist in. The intention of disaster planning is that in the case of an emergency action can be taken in an orderly and effective manner in accordance with a plan.

A critical component of disaster or contingency planning is prevention. Much of the storage and security procedures for buildings and records anticipate the requirements for recovery from a disaster.

The preparation for a disaster includes:

- Assembly and training of a disaster recovery team
- Identification and marking of priority salvage material
- Preparing documentation including local emergency and other service numbers needed in an emergency, lists of staff contact numbers, floor plans, access to keys
- Contact procedures (including out of hours) for the Senior Executive in charge of Records Management and other specialist staff e.g. trained archive personnel, trades people, and equipment and vehicles
- Access to a refrigerator for saving wet documents
- Space organised and equipment for an emergency assembled and maintained
- Test and review the disaster plan regularly.

Disaster Recovery

In the case of a disaster causing significant damage to records such as a flood, fire or explosion, the Senior Executive in charge of Records Management should be contracted. They will assess the situation, recommend a program of action, and upon acceptance of the plan start recovery action at an agreed time. Recovery action should be taken to restore to a usable condition the disaster site and materials. The action should include:

- Immediate assessment of damage.

- A decision about the urgency and type of action required e.g. what action is required on site or off site, is immediate action or gradual conservation program required? This decision will be made in consultation with conservation experts
- Removal of damaged material
- Perform conservation action
- Review performance of the plan and team, and upgrade if necessary.

Disaster Prevention and Recovery Plan

A Disaster Prevention and Recovery Plan sets out the strategies and activities for preventing disaster and preparing an appropriate response to, and recovery from, disaster and resuming normal business.

The purpose of the Disaster Prevention and Recovery Plan is to provide guidelines for identification, storage and protection of EPD's vital records. It also provides a guide for the development of a Disaster Prevention and Recovery Plan to manage these records before and after a disaster and to ensure that the resumption of business can continue through a sound recovery system.

The Disaster Prevention and Recovery Plan is not designed to provide an answer to each and every type of disaster that could happen it is designed to identify the methods on how to recover from a disaster if one was to occur.

This is the documents that will define the roles and responsibilities of staff, what other resources you will require, the location of back-ups, how the plan is to be implemented, and so on. As a guide the following steps are provided and should be documented to formulate your plan.

The Disaster Prevention and Recovery Plan

Steps	Action
Identify what records you manage (electronic and paper)	Conduct a survey of records managed by EPD, develop and maintain a complete file list. A copy of the file list should be retained or backed-up at another location.
Identify your vital records (electronic and paper)	Determine which records are vital to the area and if lost or unusable could result in the area not being able to function or provide its services. This also includes where the records would result in significant costs to restore due to their uniqueness.
Identify the risks	Refer to the risk assessment section above.
Identify any remedial or prevention action.	Refer to the preventative action section above.
Identify alternative storage facilities	Review existing storage facilities and identify if they are secure and will inhibit loss or damage. Identify an alternative location for storage of vital records and computer back-ups.
Define roles and responsibilities	Establish a group of staff contacts to assist with a restoration (also assign the duties of maintaining the plan so that it is up to date at all times). Determine who will be responsible for the various aspects of the plan an who to contact for assistance in restoring an area after disaster. Determine who will be responsible for the various aspects of the plan and who to contact for assistance in restoring after a disaster. Determine who will be responsible for reviewing the disaster plan at least quarterly to ensure it is up to date with contact details, change of locations, etc.
Prepare a disaster bin	Acquire tools and other supplies to be used in small disasters such as leaky pipes, small fires, etc. This may include gloves, masks, fire extinguisher, fire blanket, etc. Ensure disaster bin is easily accessible and all staff are aware of it's location.
Draw up an action plan	Develop a short one page plan that contains details such as contact numbers and step-by-step actions during a disaster or emergency and circulate to every staff member within the work area.

Succession Planning

Introduction

Succession planning is a critical element of employment within the ACT Government. Staff in key positions that are responsible for essential Directorate functions should maintain succession plans that will enable efficient handover of responsibility with limited or no notice.

Where a position is identified as critical, and a succession plan developed, a copy of the succession plan should be lodged to EPDHR@act.gov.au as well as retained in Objective for reference.

EPD commit to developing a succession planning policy and establishing a mechanism for recording succession plans for key organisational positions.

Responsibilities

Supervisors and managers of vital positions must complete a succession plan for the role, including detail of key staff that are capable of moving into the position, and their suitability for the role. If there are no staff internally that are identified as capable an alternative plan for sourcing outside resources should be clearly outlined, including the time frame that is likely to be required to obtain an suitable external replacement.

Staff that hold vital positions within EPD must keep accurate records of their business activities to ensure a smooth handover should the need arise.

Outsourcing

Introduction

EPD may outsource some of its recordkeeping activities, but not the responsibility or accountability for those business activities. Even when EPD outsources records management functions it still retains ultimate responsibility for the provision of the service.

EPD is responsible for ensuring that records that are in someone else's possession are held under arrangements that provide for the safekeeping, proper preservation and return of the records.

Agreements or contracts controlling the outsourcing should check that:

- Contracts specify which party will own each class of records at the end of the contract
- Continuity of service and the rights and entitlements of individuals and Territory are protected in ownership arrangements
- Any restrictions on the contractors use of information in the records is made clear in the contracts
- Contracts specify who owns the intellectual property in any records made as part of the contract
- The contract specifies any particular requirements for records description and control as well as the measures agencies will use to ensure compliance
- The contractor is made aware of the requirements of the *Territory Records Act 2002* and the standards, codes and guidelines produced under it
- Specific instructions or standards are included in the contract to ensure that sufficient contextual documents of the records is available at the end of the contract
- Contracts specify the records to which agencies are entitled to have access during and after the contract period

- The contract puts in place arrangements for providing public access to records under the Freedom of Information Act 1989 and the Territory Records Act 2002 as appropriate
- Where appropriate contracts specify the information technology format that the records are made and maintained in and how this will be managed over time.

Ownership

If relevant the outsourced contract must specify which party will have ownership of each class of records at the end of a contract.

- The agreement or contract stipulates the treatment of record ownership issues upon expiry or termination of the contract or agreement
- How the continuity of service, the rights and entitlements of individuals and the Territory are protected in ownership arrangements must be specified in the outsourced contract
- The outsourced contract must specify who owns the intellectual property in any records made as part of the contract
- The contract or agreements includes any restrictions on the third party entity using information from records for commercial profit and other purposed during or upon completion of the project that EPD feels are required.

Access

- The agreement stipulates that the sentencing of records is in accordance with all approved Records Disposal Schedules
- The agreement or contract stipulates the treatment of record disposal issues upon expiry or termination of the contract or agreement
- The agreement or contract contains provisions for the orderly transfer or disposal of records between entities when one third party entity is replaced by another to person the same outsourced function or activity
- The agreement or contract stipulates the treatment of record transfer issues upon expiry or termination of the contract or agreement.

Managing Records During Administrative Change

Introduction

Most forms of administrative reorganisation within government will require amendment to the intellectual property and/or physical management of records as part of the change. Machinery-of-government changes that can affect the Territory include: the movement of functions from one Directorate to another; the introduction of new or amended legislation; or a change of government after an election. These changes can result in:

- the transfer of a function from one ACT Government administrative unit to another
- the transfer of a function to another government jurisdiction (e.g. from the ACT to the Commonwealth)
- the creation or undertaking of a new function by the ACT government
- the abolition of a function by the ACT Government.

When such administrative changes take place, a key principal is that records relating to the function should always follow the function. This will see administering units of the function having to relinquish control of, and transferring the custody of, records to the inheriting (receiving)

administrative area of the function. As part of this, existing Records Management Programs and will need to be amended reflecting the changes and agreed to i.e. signed by the responsible Principal Officer.

Records for transfer could potentially be in any format, for example:

- registered paper files
- electronic records captured into any system (including unstructured data and records held in shared drives)
- databases and business systems
- maps and plans
- photographs
- microfilm
- obsolete technologies (e.g. DAT tapes).

Relinquishing agency records

The records and any business information systems (e.g. client management databases, project management systems, EDRMS) associated with the function, and therefore affected by the functional transfer will first need to be fully identified. This is best achieved by representatives from both the relinquishing and inheriting administrative units to ensure the understanding of scope (e.g. quantities and formats) involved and to provide completeness of the capture.

A relinquishing administrative unit may choose to use an administrative change process to conduct a sentencing project. This is encouraged but should be conducted in consultation with the administrative unit's Records Manager.

For sentencing and disposal see Records Advice No. 31 – Disposal actions: Preparation of records and Records Advice No. 32 – Utilising a records disposal schedule.

Key processes

- Determine what control records relate to the records to be transferred
- Create an inventory of the records included as part of the transfer - this can be either prepared manually or via generating reports out of an appropriate system (e.g. EDRMS). A copy of the inventories should be provided to the inheriting administrative unit
- Details of any records held within an approved storage provider, including contractual arrangements and costs, should also be made available
- Agree with the inheriting administrative unit on a timeframe for the physical and/or intellectual transfer of records to occur. For physical transfer, ensure all records containers are clearly identified with the contents
- Provide the inheriting administrative unit all Records Management Program details covering the affected records (e.g. nominated functional classification and disposal coverage)
- Once records have been physically moved, update control records indicating the new custodial administrative area and the date of transfer – all other original metadata should not be altered including the original creator of the records i.e. retain all provenance metadata (data that was applied at the creation of the record)
- Document the decisions, and the rationale for the decisions reached, in the transfer file
- Revise the Records Management Program to reflect the loss of the function

- Forward the amended Records Management Program, signed by the responsible Principal Officer (the Director-General) to the TRO

Inheriting agency records

The process of transferring records from one administrative unit to another should be planned by the inheriting administrative unit as well as the relinquishing administrative unit. Failure to appropriately plan for the carriage of inherited records could result in the loss of records necessary to perform the new function effectively.

Key processes:

- Nominate a liaison officer between the two administrative units – discuss the arrangements of the transfer outlined above with the relinquishing administrative unit
- Consider the storage arrangements for the records (not currently held with an approved storage provider) when they are physically transferred. The records should be categorised as:
    - required for immediate business use
    - required for business use in the foreseeable future
    - likely infrequent or non business use
- Use the inventories supplied by the relinquishing administrative unit to review the completeness of the transfer of all records in all formats stated
- Records should be retained in their original context upon receipt i.e. file covers not changed, control symbols/numbers not to be altered or top numbered, and titles to remain the same as received. If necessary, identify records that can be closed and create new files with intellectual links (relationships) to the inherited records within the control system(s)
- Update arrangements with any approved storage providers holding identified inherited records
- Update all control systems indicating the previous controlling administrative unit and the date of transfer
- Do not combine or integrate transferred records into the existing filing systems of the current administrative unit i.e. records should be maintained in their original order
- Revise the Records Management Program to reflect the gaining of the function
- Forward the amended Records Management Program, signed by the responsible Principal Officer to the TRO

Records required by both administrative units

Some records may be identified as necessary for both the relinquishing administrative unit and the inheriting administrative unit in order for them to continue their business. In the case of these records, they should remain with the original administrative unit and arrangements made for appropriate access to, or copying of, the records by the inheriting administrative unit.

Environment and Planning

Records Management Program

Procedures Part 5

Managing & Preserving Records

ACT Government

Environment and Planning

Digitisation and Conversion

Introduction

Digital records, like records in other formats, are evidence of the day-to-day business activities and decisions of the ACT Government. They are subject to legislation such as the *Territory Records Act 2002* and the *Freedom of Information Act 1989* and to legal processes such as discovery and subpoenas. Digital records made or received by the Directorate or its officers in the course of official duties are Territory records.

As well as records that were created in digital format the Directorate may convert records that started life in a non-digital format into digital records. This conversion is known as digitising a record, or digitisation.

When converting a record from one format to another, the source record is the record being converted and the converted record is the result of the conversion, for example, the source record is a hard copy document, the result of the conversion is a digital copy of the document. The requirement to retain the source record is dependent on the value of the source record, and the compliance of the resulting record with the *Territory Records Office Standard for Records Management No. 9 – Records Digitisation and Conversion*.

When undertaking digitisation of records the following should be considered:

- Does the converted record contain the "full and accurate" information contained in the source record?
- Does the converted record meet the Directorates business needs?
- Does the converted record meet legal, financial and other requirements?
- Can the converted record be retained and accessible for as long it is required?
- Can the source record be disposed of?

The answers to these questions will determine whether the converted record can be considered a reliable source of information, allowing the source record to be destroyed.

Another consideration when converting records is whether the conversion is pre or post action conversion.

Pre-action conversion is where conversion is carried out as soon as the record is received, for example a letter is received and scanned immediately upon receipt before any reply has been crafted.

Post action conversion is where conversion is carried out after any action has been taken on the record, for example the digitisation of existing paper based files in which the action has been completed. An action includes any decision on how to deal with the subject of the record.

The official record is the record that the Directorate staff member has based their action upon. Where pre-action conversion is carried out, the official directorate record is the converted record, as that is the record the staff member reviewed in order to make a decision.

In the case of post-action conversion, the source record is the original document (e.g. the hard copy letter) as the original document is what the decision was made on. It may contain annotations, notes, or further information forming part of the record. For this reason there is a stricter control over records converted post action.

Please refer to Guideline for Records Management No.9 – Records Digitisation and Conversion for technical guidelines.

Preservation Strategies

The prime strategies for preserving records are:

- Ensure that all staff treat records carefully
- Implement adequate storage standards and records handling practices
- To use archival quality materials for records expected to have a long life.

Preservation of electronic records requires strategies to migrate records to new systems in such a way that the records can be maintained as reliable, authentic evidence over time.

ESDD and its employees are responsible for preserving Territory records for as long as required by law and business requirements. A major threat to the preservation of records is the risk of disaster, natural or otherwise.

Records that have deteriorated over time or suffered damage by use or through disastrous events may require specific conservation treatments by experts. Advice on suitable treatments and on the availability of experts is available from the Territory Records Office. In some cases conservation may be undertaken by copying records into another medium such as film or electronic formats. Advice on this is also available from the Territory Records Office.

Digital First

EPD is a digital first Directorate. Where possible, staff should request that documents lodged to EPD be done via a digital mechanism, such as email, smartforms, or eDevelopment. If information is received in hard copy via the mail it should be converted to digital as soon as practicable and processed digitally from the point of conversion.