



POLICY TITLE:	ELECTRONIC DOCUMENT MANAGEMENT
YEAR OF PUBLICATION:	2008
IDENTIFIER:	
LEGISLATION:	<i>ACSI 33 Australian Government Information & Communication Crimes (Offences Against the Government) Act 1989 Criminal Code 2002 Electronic Transactions Act 2001 Evidence Act 1995 (Commonwealth) Executive Documents Release Act 2001 Freedom of Information Act 1989 Health Records (Privacy and Access) Act 1997 Territory Records Act 2002 Privacy Act 1988 (Commonwealth) Public Sector Management Act 1994 Spam Act 2003 (Commonwealth)</i>

1 Policy Statement

- 1.1 The ACT Department of Education and Training (DET) is committed to the appropriate management of all electronic documents, including emails, as essential to the maintenance of complete, accurate and reliable evidence of business transactions.
- 1.2 Any electronic folders, documents or electronic messages (email) that show evidence of DET business activities are an official record. The management of these electronic records is critical to maintaining sound recordkeeping practices for the Department.
- 1.3 Digitally generated records, such as those produced by electronic office applications, need to be captured and managed in their original format to maintain the content, context and structure of those records for ongoing business use.

2 Rationale

- 2.1 This policy aims to ensure that the Department meets its legislative and best practice recordkeeping requirements applicable to the ACT Government in managing all types of records, including electronic documents and emails, and sets out procedures to be followed in the management of such records.
- 2.2 The policy also aims to identify standards and strategies and set out principles and minimum standards for the effective management of electronic records so that all these records remain accessible and useable for as long as they are required. It also addresses issues concerning the storage and disposal of electronic records as well as issues relating to security.

2.3 Proper management of electronic documents and emails:

- adds to the corporate memory of the Department and results in better quality decision making
- ensures official records created electronically are available and accessible to employees who require access to complete their duties
- provides evidence of decision making and the ability to defend decisions during litigation
- facilitates identification and accessibility of electronic records requested by legal processes such as subpoenas, Freedom of Information and by other government agencies
- ensures legislative and accountability requirements are met and penalties for non compliance avoided
- prevents the illegal or arbitrary destruction of departmental records
- promotes sharing of information throughout the Department.

2.4 The policy acknowledges that, as the Department's current approved record keeping system is paper based, electronic documents and emails deemed as records should be printed and attached to the relevant paper file.

3 Definitions

Capture:

To fix a record so that it cannot be altered or deleted. This can be done either manually such as printing the document out and placing it on a paper file. Alternatively, when working with an electronic system the record may be captured automatically or a choice given to save the record in to the system.

Digital Record:

Is a record that is communicated and maintained by means of electronic equipment. They include but are not limited to:

- documents created from office applications e.g. word processed documents, spreadsheets
- records in online and web based environments e.g. internets, intranets
- electronic messages from communication systems e.g. email, instant messaging
- records that have been converted into digital form from their original format. e.g. digital scans of paper documents.

Electronic Document and Records Management System (EDRMS):

An Electronic Document and Records Management System enables the capture and management of electronic records.

Electronic Folder:

Electronic folder refers to a Windows operating system folder.

Electronic Message:

Electronic messaging is defined as the transmission of messages over computer networks. This includes email, short message service (SMS), multimedia message service (MMS) or instant messages (IM), but not voice over internet protocol (VOIP) telephones.

Electronic Record:

Electronic record refers to any digital object found in the agency networks. e.g. word documents, spreadsheets, databases, images and presentations.

Ephemeral Records:

Information messages that may have a business context but are not part of a business transaction – for example, notification of a meeting or a message containing an attached document, and personal or social messages.

Records:

Information made, received, and maintained as evidence and information by an agency or person, in pursuance of legal obligations or in the transaction of business. Records can be written, electronic or any other form.

Records Management System:

An information system that captures, maintains and provides access to records. This system may be paper based, electronic or a hybrid of both.

4 Responsibilities

4.1 All departmental officers must be aware of their responsibilities in relation to managing the records they create and receive electronically.

4.2 Email

4.2.1 All agency staff members are required to ensure that all emails deemed as records are captured. The table provided in the [Electronic Messages \(Email\) Handling Guidelines](#) will assist in determining capturing responsibilities.

4.3 Electronic Folders and Documents

4.3.1 Departmental officers should ensure electronic folders and documents that are deemed, as records are kept manageable. This responsibility extends to following the correct naming and storage procedures of electronic folders and documents on the agency G:\drive. Further information on naming standards and storage procedures is available in the [Electronic Folder and Document Naming Guidelines](#).

4.3.2 Departmental officers should ensure electronic documents that are deemed as records are printed and placed on the relevant paper file. These records are not to be permanently saved to hard drives such as G:\drive, H:\drive or C:\drive as they are not fully integrated records management systems and provide no guarantee of lasting access or accuracy.

5 Procedures

5.1 Electronic Message (Email) Handling

5.1.1 Due to the increased risk of information disclosure, emails should not be used to provide any sensitive information.

Deciding whether an email is a record

5.1.2 If an email meets any of the criteria available within the [Electronic Messages \(Email\) Handling Guidelines](#) it is a departmental record and should be printed out and placed on the relevant paper file.

- 5.1.3 Emails identified as records are to be treated no differently from agency records in other formats in relation to their creation, capture, management, retention, disposal and preservation.
- 5.1.4 Emails are required to be accessible, readable and available for as long as they are required for legislative, business, evidential or historical purposes.

Emails with attachments

- 5.1.5 To ensure a full and accurate record of the email is kept, any associated records such as attachments should also be printed with the original email and placed on the appropriate paper file.

Email threads

- 5.1.6 Each email sent or received in an email thread, that relates to agency business and is deemed to be a record, should be placed on the appropriate paper file. As it is possible to modify previous email messages in a thread, each message in a thread should be placed on the appropriate paper file to ensure that every communication of the thread is captured.

Ephemeral records

- 5.1.7 If an email does not meet any of the criteria available within the [Electronic Messages \(Email\) Handling Guidelines](#) it is an ephemeral record and does not need to be captured as a record. Ephemeral records may be deleted once reference to these records has ceased.

5.2 Electronic Functional Directories

Establishing folder structures

- 5.2.1 To consistently manage electronic folders and the documents they contain, the DET Thesaurus should be utilised to provide the framework for the titling of electronic directories, e.g. Function – Activity – Subject. This will establish a relationship between electronic folders on the agency's G:\ drive and the contents of related agency paper based files. Information currently stored in subject/organisational directories should be moved or migrated into a functionally structured directory, as they are being re-saved.

Creating Thesaurus based electronic folders

- 5.2.2 An explanation of the relationship between the Function, Activity and Subject thesaurus based folders, and information on creating the titling framework for thesaurus based functional directories, is available in the [Electronic Folder and Document Naming Guidelines](#).

5.2.3 Scope Notes

The DET Thesaurus provides clearly defined scope notes for each function and activity. This information aids in describing what records can be contained within each folder. Advice on the creation of new folders utilising the DET Thesaurus and the adding of relative scope notes for Windows 2000 is available in the [Electronic Folder and Document Naming Guidelines](#).

5.3 Electronic Document Naming

5.3.1 To effectively manage electronic documents that are deemed as records, the naming standards enclosed in the [Electronic Folder and Document Naming Guidelines](#) should be followed.

5.4 Storage Procedures

Storage of emails

5.4.1 Emails and any attachments that are deemed as records should be printed out and placed on the appropriate paper file. For current business use they can be temporarily saved to an appropriately named electronic folder on the agency G:\ drive. This action facilitates access by other departmental officers who require access to these records for FOI requests or for quick access to corporate memory on decisions made by the Department. Instructions for saving emails to the agency G:\drive are enclosed in the [Electronic Messages \(Email\) Handling Guidelines](#)

5.4.2 Emails and any attachments that are deemed as records should not be permanently stored on the agency G:\ drive as it is not fully integrated records management system and provides no guarantee of lasting access or accuracy. More information is enclosed in the [Electronic Messages \(Email\) Handling Guidelines](#).

5.4.3 Emails and any attachments that are deemed to be records should not be stored on individual hard drives such as H:\ drives or C:\ drives or .pst files as they are not fully integrated records management systems. The C:\ drive is not backed up and therefore deleted records cannot be restored and only the creator or owner of emails stored on H:\drive and .pst files has access to these folders or drives.

Storage of Electronic folders and documents

5.4.4 Electronic documents that are deemed to be records should to be printed and placed on the relevant paper file. For current business use they can be temporarily saved to an appropriately named electronic folder on the agency G:\ drive. This action facilitates access by other departmental officers who require access to these records for FOI requests or for quick access to corporate memory on decisions made by the Department.

5.4.5 Electronic documents that are deemed to be records should not be stored on individual hard drives such as H:\ drives or C:\ drives as they are not fully integrated records management systems. The C:\ drive is not backed up and therefore deleted records cannot be restored and only the creator or owner of documents stored on H:\drive and .pst files has access to these folders or drives.

5.4.6 In order to effectively control different versions of documents, version control should be used for documents which have a number of contributors and which are likely to be in various stages of development before the final version is complete. More information on naming protocols is available in the [Electronic Folder and Document Naming Guidelines](#).

Available electronic storage space

5.4.7 Excess storage of electronic documents places a significant cost burden on the Department. Current storage space is at a premium due to the volume of emails and electronic documents. All departmental officers are to be aware the departmental guidelines on the management of electronic records provided in: [Electronic Messages \(Email\) Handling Guidelines](#) [Electronic Folder and Document Naming Guidelines](#).

6 Security Issues

6.1 Email

6.1.1 Emails should not be used, either within or outside the Department, to provide any sensitive information unless the sensitive information is sent with approved encryption software. Advice on approved encryption software may be obtained from the ICT Services, IT Security Team on 620 72038. Further advice on handling sensitive information is also available from the [Sensitive Information Handling policy](#).

6.1.2 Other potential security issues may include:

- incorrect addressing
- auto-forwarding of messages from the intended recipient's mailbox
- disclosure of CC lists without permission from recipients
- copies kept on email server backups
- sender/receiver cannot be validated
- email passing between mail servers may be captured or copied, viewed and modified by an unauthorised party before the message is forwarded to the next mail server
- privacy breaches in relation to email addresses. (the use of the "BCC" field can aid in alleviating this possible privacy breach).

6.2 Electronic Folders and Documents

6.2.1 Confidential electronic documents and folders should not be secured by passwords as they can be forgotten or lost. Passwords on documents also block virus scanning. Confidential electronic documents and folders may be secured by closed group permissions. Further information on securing confidential electronic documents and folders by closed group permissions may be sought by contacting InTACT 75555.

7 Disposal

7.1 Electronic documents and emails that are deemed as records should not be deleted until a copy has been placed on the appropriate departmental paper file.

7.2 Disposal of records must be managed in accordance with the Department's [Records Management Program](#). For further information on the destruction of records please contact the Records Management Section.

8 Further Advice

See the [Territory Records Office](#) *Records Advice No. 3 Email as a record* for further guidance.

Policy Owner: Director, Governance, Regulation and Risk

Related Policies: *DET Records Management Program*
DET Information Technology Security Policy
DET Privacy Statement
DET Sensitive Information Handling Policy
InTACT Access and use of ICT resources policy
InTACT A reference guide to the ACT Government ICT security policy framework
DET Student Record Keeping Policy
DET Acceptable Use of IT Resources Statement
