Department of Culture and the Arts
Government of Western Australia

State Records Office of Western Australia

SRO Guideline

Management of Email Records

A Recordkeeping Guideline for State Organizations

State Records Office of WA
Perth, Western Australia

July 2009

CONTENTS

GLOSSARY

Archiving - in the recordkeeping context refers to the transfer, management and preservation of records, documents or materials designated as archival records in a separate repository where they are to be held permanently.

Archival record - means a record that is to be preserved permanently (ie never to be destroyed) because of its enduring value (ie historical, evidential etc.)

Attachment - means an electronic file or message sent as an addition to an email message.

Authentic record - means a record that can be proven to:
- be what it purports to be;
- have been created or sent by the person purported to have created or sent it; and
- have been created or sent at the time purported.

Business email - means an email that contains information created or received by the organization in the transaction of business. These emails are State records. See also: Record.

Classification - means the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.

Combination email – means an email that contains both business and personal email.

Digital record - means any record within the meaning of Section 3 of the *State Records Act 2000* that exists in binary form and that requires combinations of computer hardware and software to be read and understood. See also: Record.

Digital signature - means a security mechanism included within a digital record that enables the identification of the creator of the digital object and that can also be used to detect and track any changes that have been made to the digital object.

Digital Rights Management (DRM) - means a technology that creates certain conditions about how some digital media files can be used and shared. In email systems, DRM allows the sender to place restrictions on who can view, print, forward, copy or edit messages.

Electronic Document and Records Management System (eDRMS) - means an automated system used to manage the creation, use, management and disposal of physical and electronically created documents and records for the purposes of:
- supporting the creation, revision and management of digital documents
- improving an organization's work-flow and
- providing evidence of business activities.

These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence. eDRMS are a subset of business information systems and recordkeeping systems. Their primary purpose is the capture and management of digital records.

Electronic record - for the purpose of this guideline has the same meaning as Digital record

Email – means an electronic mail message sent or received using an email system. See also Business email.

Email system - means a system which supports the creation and transmission of messages through a computer system. It enables messages to be sent online to general or private directories or electronic mail boxes by the use of a unique system address. Messages may originate from within or outside an organization.

Ephemeral email – means an email which may or may not be used to facilitate the organization's business and which has no continuing value to the organization. See also: Business email.

Integrity - the integrity of a record refers to its being complete and unaltered.

Long term retention - means the act of retaining records, in an accessible, reliable and readable format for the entire retention period which may mean many decades. In these instances the impact of changing technologies and their effect on the accessibility, reliability and readability of the records must be considered.

Metadata - means data describing context, content and structure of records that must be captured to enable the record to be understood and to support its management and use through time.

Migration – means the act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.

Organization - for the purposes of this guideline means a State organization.

Permanent retention - means the act of retaining the records in perpetuity in an accessible, reliable and readable format. See also: Archival record.

Personal email - means an email that relates to a private or personal matter and has no relevance to the business of the organization.

Record - means any record of information however recorded, and includes:

- any thing on which there is writing or Braille;
- a map, plan, diagram or graph;
- a drawing, pictorial or graphic work or photograph;
- any thing on which there are figures, marks, perforations or symbols having a meaning for persons qualified to interpret them;
- anything from which images, sounds or writing can be reproduced with or without the aid of anything else; or
- any thing on which information has been stored or recorded, either mechanically, magnetically or electronically.

A record may have any or all of the following attributes:
- information which is of administrative, legal, fiscal, evidential or historical value and is not recorded elsewhere;
- formal communication and/or a transaction between officers (for example, a memorandum, report or submission) or between an officer and another party; or
- documents the rationale behind organization policy, decisions or directives.

Recordkeeping - means the systematic organization and control of recorded information in any format from the time it is created to its final disposition.

Recordkeeping system - means a system to capture, maintain and provide access to records over time that displays features for ensuring authentic, reliable, complete and usable records that function as evidence of business transactions.

Records disposal authority - lists categories of records and the retention period, disposal sentence and custody arrangements for each category. State records can only be disposed of under a records disposal authority approved by the State Records Commission.

A records disposal authority may take the form of:
- a general disposal authority (published by the State Records Office);
- a retention and disposal schedule;
- an ad hoc disposal schedule; or
- a disposal list.

Reliable record – means a record where the contents can be trusted as a full and accurate representation.

State organization - means a parliamentary department or a government organization (including local government).

State record - means a parliamentary record or a government record. See also: Record.

State Records Commission (SRC) - means the independent body established under the *State Records Act 2000* (the Act). The SRC's functions include:
- monitoring the operation of, and compliance with, the Act;
- monitoring compliance by government organizations with recordkeeping plans;
- inquiring into breaches or possible breaches of the Act; and
- reporting to Parliament.

PURPOSE

The purpose of this guideline is to assist State organizations in ensuring that records created or received in email systems are managed in accordance with SRC Standard 8: *Digital recordkeeping*.

This guideline serves to:

- assist organizations in the effective management of emails that are State records;
- provide guidance for determining what emails are State records; and
- provide general guidance on aspects of email administrative management processes that may affect recordkeeping compliance.

BACKGROUND

Principle 1 of SRC Standard 8: *Digital recordkeeping* requires that State organizations ensure that all types of digital records are managed appropriately.

State and local government recordkeeping systems must be designed to meet the requirements of efficiency, accountability and the maintenance of State records in accordance with legislative requirements and best practice. Email is increasingly used to conduct business both within and outside State and local government organizations. Email documents created or received by officers in connection with the organization's business activities are the property of the organization, not the individual. They are State records and are subject to the same recordkeeping requirements as State records in other formats.

Most email systems allow senders to attach documents to messages, import text from word processing systems to email systems, forward messages and distribute information to individuals and groups. More sophisticated email systems include workflow software that manages the movement of messages through a defined work group or organization.

All email systems create records, however, there is a danger that important State records may be lost if they are not properly managed. The capture and registration of business email records in the organization's official recordkeeping system is crucial to the organization's accountability and future decision-making process.

Email archiving processes may benefit the organization in terms of managing storage, but they are not a substitute for capturing email into a recordkeeping system. Records management systems provide total frameworks for capturing, maintaining and providing access to evidence of transactions over time.

For email records to be maintained over time, a number of specific management requirements must be implemented to ensure the integrity and functionality of the record. Organizations must ensure that policies and procedures are in place to control the creation, editing, capture, maintenance, storage and authorised disposal of business email records.

Digital records may provide the organization with evidence of its business activities and must be kept as proof of such activities. To be considered as evidence, a digital record must possess:

- **content** – that which conveys information, for example, the text, data, symbols, numerals, images, sound or vision;
- **context** – the background information which enhances understanding of technical and business environments to which the records relate, for example, metadata, application software, logical business models, and the provenance (for example, recipient's name, address, title, link to function or activity, organization, program or section); and
- **structure** – the appearance and arrangement of the content, for example, the relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices.

SCOPE

This guideline applies to all State government organizations as defined in the *State Records Act 2000*.

This guideline supersedes:

- State Records Standard 4: *Records management standard for the management of electronic mail (e-mail).*

This guideline **must** be read in conjunction with SRO Guideline *Management of digital records* and relevant SRC Standards.

GUIDELINE

RATIONALE

Management of emails that are State records should not occur in isolation from the management of other records. It should form part of an information and records management strategy that encompasses all the information created or received by a State organization.

Implementation of this guideline does not mean that all email should automatically be kept, but rather that requirements for the management of State records should be met by the integration of email systems and electronic records management systems.

The specific management arrangements developed to implement this guideline may differ from organization to organization, depending on their information technology environments and operating systems. However, the broad concepts can be applied to any organization.

See also:
SRC Standard 8: *Digital recordkeeping;* and
State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value.*

1. Shared Approach to Managing Emails

The effective management of emails that are State records requires the coordinated effort, shared responsibility and support of all staff including Chief Executive Officers. Strategic and operational roles and responsibilities should be shared between records managers, Chief Information Officers, information technology personnel, system administrators and individual email users who create, send and receive emails. These roles should be supported with appropriate policies and procedures.

2. Categories of Email

2.1 Business email

A business email contains information created or received by an officer, via an email system, in the course of his/her duties.

A business email may have any or all of the following attributes:

- information which is of evidential and/or historical value and is not recorded elsewhere;
- formal communications and/or a transaction between officers (for example a memorandum, report or submission) or between an officer and another party; or
- documents the rationale behind organization policy, decisions or directives.

These emails are State records and must be captured in the recordkeeping system to provide evidence of business activity and meet legal requirements. Business email must be retained for as long as required, giving consideration to the subject matter of the record, and may only be destroyed in accordance with an approved records disposal authority.

2.2 Ephemeral email

An ephemeral email may or may not be used to facilitate the organization's business and has no continuing value to the organization and is generally only needed for a few hours or a few days.

Examples of ephemeral email include:

- unsolicited advertising material (eg incoming promotional literature, brochures, and leaflets);
- duplicates of circulars;
- duplicates of minutes and other documents where the original record has already been captured;
- email notification of routine or trivial telephone messages; or
- duplicate emails circulated *for information purposes only*.

Ephemeral email may not need to be captured in a recordkeeping system and can be destroyed when reference ceases as authorised in an approved records disposal authority.

2.3 Personal email

Personal email relates to a private or personal matter and has no relevance to the business of the organization.

Examples of personal email include email dealing with topics such as:
- arrangements for lunch;
- personal/family arrangements; or
- jokes or unsolicited information not related to work responsibilities,

where no business related content is included. See also 2.4 - Combination Email.

Personal email may be destroyed when no longer required.

See also: 7. Retention and Disposal.

Each organization should have a policy in place which informs staff of acceptable personal use of email systems. Such a policy should highlight issues such as conflicts of interest and should refer staff to relevant codes of conduct.

2.4 Combination email

a. If the email incorporates **both** personal and business related information, the email is to be considered a State record (or business email) and must be managed accordingly.
b. If the email incorporates **both** ephemeral and business related information, the email is to be considered a State record (or business email) and must be managed accordingly.
c. If the email incorporates personal, ephemeral **and** business information, the email is to be considered a State record (or business email) and must be managed accordingly.

3. Methods for Capturing and Managing Email Messages as Records

All business emails have differing values. Some will be needed for ongoing business and some will have a short lifespan. All business email must be captured in the organization's recordkeeping system. It is the responsibility of all officers, including temporary staff, contractors and Board members to ensure that business emails are captured into a recordkeeping system.

It is **not** appropriate to use email systems or network drives to manage business emails. Backup stores of emails within an email system and the practice of saving email messages to directories or folders are merely forms of storing the emails and are not a means of managing them. Recordkeeping systems are required to manage email records appropriately.

The acceptable methods for the management of business emails are to:

A. capture business emails in to an electronic document and records management system (eDRMS); or

B. print and file the business emails, attachments, header details and other appropriate metadata to the paper based recordkeeping system.

Refer to SRO Guideline *Management of digital records* for detailed information on these methods.

4. Integrity of the Message

The integrity of an email message as a record relies upon the metadata and the content of the message being maintained and available over time to meet the business and accountability requirements of the organization.

It is also important that an access history or log is retained in the recordkeeping system to indicate who has viewed the record, extracted a copy or modified the content. This information is important for evidential purposes.

4.1 Recordkeeping metadata

Recordkeeping metadata describes the context, management, use, preservation and disposal action of records. Attaching recordkeeping metadata to emails that are State records allows them to be located, controlled, accessed and managed appropriately and ensures context is maintained.

Metadata includes descriptive information such as author, recipient and date/time of transmission as well as information about the business context (eg the business function and activity that generated the record), a relevant file or container number, and management information (such as the retention and disposal status).

Depending on a range of factors such as the functionality of the email system and integration with a recordkeeping system, some metadata may be system-generated (eg date and time of transmission), some may be created while authoring the email (eg names of recipient and full details of sender) and some may be manually generated when capturing the record into a recordkeeping system.

In the email environment, the capture and maintenance of recordkeeping metadata is essential to the "completeness" of a State record.

4.2 Email records should be accessible

Emails which form part of the State record should be able to be read by anyone who has sufficient access privileges. That is, authorised staff should be able to access emails which are relevant to their role regardless of which email box the email was sent to or from. Many email systems only allow the recipient or the creator of emails to access those emails. This means that some alternative method of providing access to those email records must be found.

See also: 3. Methods for Capturing and Managing Emails as Records

4.3 Email records should not be altered

It is important that State records can only be altered in an authorised fashion, otherwise they may not be considered reliable evidence. Many email systems allow users to alter emails after they have been sent or received. Use of email systems or network drives for storage of business emails is **not** appropriate as a management technique. In the event of a dispute about the content of a particular

email, the ability to prove that the captured version of the email is identical to the version that was sent or received is paramount. Business emails must be captured in the recordkeeping system to ensure that the records cannot be altered after dispatch or receipt.

See also: 3. Methods for Capturing and Managing Email Messages as Records.

For evidential purposes, it is essential that an access history or log (ie metadata) is retained in the recordkeeping system to indicate who has viewed the record, extracted a copy or modified the content.

4.4 Email records should be classified

An important component of records (and therefore email) management is classification. That is, emails should be arranged so that they are linked to and kept in context with other documents (paper or electronic) on the same subject. Effective classification facilitates a combined retrieval of a complete picture of events, related to a particular business activity, client or project, with related records and emails captured together. If related emails are scattered across the organization, it is very difficult to guarantee that all emails relevant to a matter have been found.

4.5 Email records should be readable for the long term

It is highly likely that email kept in most email systems will be unreadable in as little as five years time due to technological obsolescence unless appropriate actions are taken to ensure their ongoing readability. Irrespective of whether the email records are temporary and required to be retained for a short period or of greater value with long term or permanent retention periods, all email records must be managed appropriately.

Electronic systems must be successfully migrated to ensure viability of the records for the full retention period.

See also:
7.4 Migration, in SRO Guideline *Management of digital records*;
State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*; and
SRC Standard 8: *Digital recordkeeping.*

Encrypted emails must be migrated with the attributes of the public and private keys intact to ensure accessibility over time. See: 8. Digital Signatures and Encryption.

5. Emails with Specific Attributes

5.1 Emails with attachments

Attachments to business emails must also be captured into the organization's recordkeeping system. These documents are an important part of the business record and must be captured with the email message.

5.2 Carbon copy and blind carbon copy (cc and bcc) email

If a cc or bcc business email is received from an external party, the email must be captured in the organization's recordkeeping system by the recipient.

If an email is sent by cc or bcc to other officers in the organization for informational purposes only (ie the officers are not required to action the email), the originator is responsible for capturing the email as a record, if appropriate.

5.3 Email threads

Emails that are State records should be captured in the organization's recordkeeping system as soon as they are sent or received or as soon as possible thereafter. However, emails often involve a thread of communication that can continue for a period of time. Organizations should determine an organization-wide approach for the timing for capturing emails.

Options may include:

- capturing each email as it is sent or received. As capture becomes a routine component of the business process, the risk of non-capture of records is reduced; OR
- capturing at the very end of the communication thread. This may reduce the volume of email records captured but may also increase risk of non-capture of the record into the recordkeeping system, as the end of the thread may not always be apparent; OR
- capturing at significant points throughout the communication thread, where key decisions are made, subjects change, or key issues are addressed.

Each organization must determine at which point emails must be captured to ensure the completeness of the record.

6. Backlogs of Emails

Organizations must develop strategies to address issues relating to backlogs of emails that have been stored either in individual email inboxes or on system backup tapes. Planning should include assigning responsibility for identifying stores of emails that are State records and capturing them into the recordkeeping system. This is a particularly critical process prior to staff leaving the organization, or transferring to another department or business unit and when business functions change due to an organizational restructure.

Procedures should be in place to conduct exit interviews with staff that are leaving the organization, or moving to a different position in the same organization. The exit interview must include identification of business emails within the email system and capture of those records in the recordkeeping system.

7. Retention and Disposal

Under the *State Records Act 2000*, State records may only be destroyed in accordance with an approved records disposal authority.

The retention and disposition of business email should be incorporated into the organization's Retention and Disposal Schedule for approval before destruction or archiving can occur.

There are many email system administration strategies that organizations might utilise to manage their email systems. These strategies may include:

- Regular purging of email boxes when too large or staff members leave;
- Automatically deleting emails that have been on the system for a specified period of time, or to move older emails to offline storage; or
- Software that may block, delete or otherwise alter business related emails received by the organization's email system

The potential risks to the organization should be assessed when determining which strategies will be implemented. Consideration must be given to the implications of these strategies with regard to recordkeeping requirements, especially unauthorised destruction of State records and to the potential harm that malicious emails could cause to computing infrastructure.

Improved staff training and tighter controls and policies for filing of emails are preferable strategies for reducing strain on email systems. Staff should capture business emails in the recordkeeping system as a routine practice rather than only when reaching their mailbox size limit.

See also: 6. Backlogs of Emails

The use of digital rights management systems to enable the automatic deletion of email messages, or to place any other restrictions on emails that may impede recordkeeping practices is not recommended. These restrictions can include the automated self-deletion of email – ie the sender of an email can stipulate the lifespan of a message and force the deletion of the email from the system at a predetermined time. Automatic deletion of emails in this manner may constitute unauthorised disposal. State organizations are advised not to use this functionality.

Backups are created to facilitate restoration of a system or file in case of accidental or unintentional loss. All organizations should have procedures in place for such systems management. However, backup stores on email servers or on backup tapes should not be considered as a method of recordkeeping for business email records.

In order to meet accountability and audit expectations, system log files should be kept. They should record information about all messages deleted from an email system, particularly where messages are not delivered to the recipient. These log files should be managed according to the organization's established recordkeeping practices and retained in accordance with an approved records disposal authority.

Before they can be legally deleted from an email system, business emails must be captured into the organization's recordkeeping system, or meet the requirements of an approved records disposal authority.

7.1 Email archiving

In the context of this guideline, the management of business emails designated as archives is concerned with the creation, capture, and maintenance of those records so that they remain permanently accessible.

Archives embedded in the email system are only a storage mechanism and are not a substitute for capturing business emails into a recordkeeping system. Records management systems provide total frameworks for capturing, maintaining and providing access to evidence of transactions over time.

For further information regarding Retention and Disposal and Archiving, see:
SRO Guideline *Management of digital records* (Section 7 Security and Disposal); and
State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value.*

8. Digital Signatures and Encryption

Technology exists which will allow digital records to be digitally signed, or tagged. Electronic communications may need to be verified so the parties involved are certain of who they are dealing with. Digital signatures can provide this verification. The document can also be encrypted for added security. Digital signatures can be created using cryptography software with public key and private key configurations.

The use of encryption should be managed carefully. As public and private keys are a corporate asset, authorisation must be approved and the organization must ensure that encrypted documents can be accessed when required. A corporate record of all keys should be held under strict access restrictions by designated responsible officers.

A digital signature does not replace the need for the type of security provided by an eDRMS. Digital records that have been encrypted should be decrypted prior to capture in the eDRMS and other security mechanisms should be applied to protect the record from unauthorised access. Metadata relating to the encryption and authentication process should be captured and maintained for as long as required.

9. Emerging Technologies

Email currently represents the dominant electronic message format used in business. But organizations should note the emergence of alternative electronic message formats, such as instant messaging, SMS (short message service) and MMS (multimedia messaging service). These messaging systems are often more flexible than email and have the potential to be used for business purposes.

Personnel with responsibility for digital recordkeeping are advised to be aware of the uptake and usage of electronic message formats and implement mechanisms (policies, procedures and practices) to ensure that any resulting digital records related to business activities are treated as State records.

10. Training

It is the responsibility of all officers, including temporary staff, contractors and Board members, to ensure that State records are captured into a recordkeeping system. Management of email records must be incorporated in an organization's recordkeeping training and staff induction program to ensure that all officers are fully cognisant of their recordkeeping responsibilities.

APPENDIX A - Checklist For Identifying Email That Should Be Saved Into A Recordkeeping System (RKS)

SENDER	
Is this official business correspondence?	Save email into RKS
Am I sending an email which contains business information?	Save email into RKS
Am I sending an email with business information attached, ie copies of minutes, reports etc?	Save email and attachments into RKS
Am I sending a reply to a business email?	Save email into RKS
Does this email record an internal business decision?	Save email into RKS
Am I sending an email to another employee/s authorizing an action?	Save email into RKS
Am I sending an email to another organization employee/s which contains business information or instruction, ie circular, notice etc?	Save email into RKS
RECIPIENT	
Is this official business correspondence?	Save email into RKS
Is the email a reply to a business email I had sent and contains further information?	Save email into RKS
Did I receive an email with business information attached, ie copies of minutes, reports etc from an external party?	Save email an attachments into RKS
Does this email record a decision made by an external party?	Save email into RKS
Does this email record an internal business decision?	No need to save – Email is a business record and should be saved in the RKS by the **originator** of the email
Did I receive an email with business information attached, ie copies of minutes, reports etc from another organization employee?	No need to save – Email is a business record and should be saved in the RKS by the **originator** of the email
Was this email sent by another organization employee, ie circular, notice etc?	No need to save – Email is a business record and should be saved in the RKS by the **originator** of the email
Did I receive a Cc or Bcc of an email from an external party that relates to organization business?	Save email into RKS
Was the email forwarded for information purposes only, ie as a Cc or a Bcc and has no business value?	Email is for information only and can be deleted

APPENDIX B - Checklist for Implementing the Guideline for Management of Email Records

The principles of the SRO Guideline *Management of digital records* have been considered in the development of email management strategies within the organization	
AS ISO 15489:2002 Records management and *AS/NZS 4360:2004 Risk management* have been considered in the development of email management strategies	
The Chief Executive supports the email management strategy and has ensured sufficient resources for its implementation	
The organization's broader information and records management plans include email management	
Procedures for the creation and capture of emails that are State records have been developed and implemented	
Recordkeeping roles and responsibilities have been identified and documented in email management policy and procedures	
All employees and contractors are aware of their responsibilities for creating and capturing full and accurate records of business they conduct by email	
All employees and contractors have the capacity to identify and initiate the capture of email business records	
The recordkeeping system has been designed and implemented in a way that allows the capture of emails that are State records	
Recordkeeping metadata is being created and captured with emails that are State records	
Capture of business email records is monitored and email management strategies revised to address areas of risk	
A migration program for emails captured as digital records has been developed and implemented where necessary	
Emails that are State records are transferred from the email system to the recordkeeping system as they are sent or received	
A strategy for addressing backlogs of emails has been developed and implemented where necessary	
Information security protocols and procedures have been developed, implemented and maintained to ensure business email records remain inviolate	
Approved retention and disposal schedules are applied to manage the disposal of emails that are State records	
A risk assessment has been conducted prior to the development of email management strategies	
The appropriate level of awareness raising and training for staff using email has been identified and undertaken	
All staff using email are aware of and understand the organization's email management policy and procedures	

BIBLIOGRAPHY

Archives Office of Tasmania 2005, *Management and capture of email*, viewed 30 January 2008, <http://www.archives.tas.gov.au/legislative/staterecords/advices_list/advice_04>.

Archives Office of Tasmania 2005, *Managing email as records*, viewed 30 January 2008, <http://www.archives.tas.gov.au/legislative/staterecords/guidelines_list/guideline_07>.

National Archives of Australia (NAA) n.d., *Are email archiving solutions suitable for managing emails as records?,* viewed 30 January 2008, <http://www.naa.gov.au/records-management/systems/email-archiving-solutions.aspx>.

National Archives of Australia (NAA) 2004, *Digital recordkeeping: guidelines for creating, managing and preserving digital records*, viewed 30 January 2008, <http://www.naa.gov.au/records-management/publications/Digital-recordkeeping-guidelines.aspx>.

National Archives of Australia (NAA) n.d., *Managing email*, viewed 30 January 2008, <http://www.naa.gov.au/records-management/systems/email/index.aspx#section4>.

Public Records Office of Victoria (PROV) 2002, *Email as records: advice to Victorian government agencies*, viewed 3 January 2008, <http://www.prov.vic.gov.au/publications/publns/PROVRMadvice3.pdf>.

Queensland State Archives 2007, *Managing emails that are public records: policy and guideline for Queensland public authorities*, viewed 1 February 2008, <http://www.archives.qld.gov.au/downloads/emails_that_are_public_records_policy_and_guideline.pdf>.

Standards Australia International Ltd, *Australian Standard AS ISO 15489 - Records management*. Standards Australia International Ltd, Sydney, 2002.

State Records Authority of New South Wales 2000, *Standard on recordkeeping in the electronic business environment*, viewed 1 February 2008, <http://www.records.nsw.gov.au/recordkeeping/docs/standard%20rk%20electronic%20business%20environment%20revised%20march%202007.pdf>.

State Records of South Australia 2006, *Management of email as official records*, viewed 30 January 2008, <http://www.archives.sa.gov.au/files/management_guidelines_managementemail.pdf>.