Australian Government

NATIONAL ARCHIVES OF AUSTRALIA

Commonwealth Records in Evidence

2012 revision

the archives

naa.gov.au

RkS R774922011

With the exception of the Commonwealth Coat of Arms, *Commonwealth Records in Evidence 2012 revision* by the National Archives of Australia is licenced under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/).
Enquiries regarding the licence and any use of this document should be sent to recordkeeping@naa.gov.au or the Publications Manager, National Archives of Australia, PO Box 7425, Canberra Business Centre ACT 2610, Australia.
This publication should be cited as: *Commonwealth Records in Evidence 2012 revision*, National Archives of Australia, 2012.

CONTENTS

INTRODUCTION TO COMMONWEALTH RECORDS IN EVIDENCE (2012 Revision)

The purpose of *Commonwealth Records in Evidence* is to provide staff in Commonwealth Government agencies with an overview of the legal issues and risks regarding Commonwealth records used in evidence and advice on how to mitigate some of those risks.

The National Archives of Australia (NAA) first published *Records in Evidence* in 1998 in response to the passage of the *Evidence Act 1995*. A second edition was published in 2005.

This third version specifically addresses the records of Commonwealth agencies and incorporates significant legal developments affecting the issue of records as evidence:

- changes to the *Evidence Act 1995* resulting from the *Evidence Amendment Act 2008*;
- evolving practice in the Federal Court of Australia, resulting most recently in *Practice Notes CM 5 - Discovery, 2011* and *CM 6 - Electronic Technology in Litigation, 2011* and amendments to the *Federal Court Rules, 2011*;
- establishment of the Office of the Australian Information Commissioner, 2010; and
- case law concerning records destruction, including *McCabe v British American Tobacco* (2002), *R v Ensbey* (2004) and *R v Selim* (2007).

NAA wishes to acknowledge the contribution of the Attorney-General's Department, the Australian Government Solicitor and the Office of the Australian Information Commissioner in the revision of this advice.

EXECUTIVE SUMMARY

The *Evidence Act 1995* (Cth) (**Commonwealth Evidence Act**) addresses requirements for the admissibility of evidence and has particular implications for records management, including digital records management, in Commonwealth Government agencies.

This document presents guidance, based on current Commonwealth laws, about the legal acceptance of records, including digital records. The major areas addressed are:

- rules of evidence in courts and tribunals;
- compliance with subpoenas, orders for discovery and freedom of information (**FOI**) requests; and
- records management requirements.

Problems can arise with the legal acceptance of records as evidence if appropriate business practices, including standards and procedures, are not followed in creating and maintaining records. To mitigate this risk and to ensure your business information is well managed, your agency should ensure that:

- its records management systems are reliable;
- the records created and maintained in those systems are authentic; and

- its records management systems are supported by documented business practices that will withstand scrutiny in the event that the agency's records are produced as evidence.

In addition, the need to comply with subpoenas, orders for discovery and FOI requests presents significant implications for agencies.

Prudent management of your agency's information compliance obligations therefore also requires the ability to:

- undertake documented searches to identify and produce all potentially relevant documents as evidence, including any associated contextual information (metadata), across an agency's systems, within short timeframes; and
- identify systems that have not been searched as part of an agency's response to a request or an order.

The advice contained in this document is general in nature and your agency should seek legal advice for its specific circumstances.

INTRODUCTION TO EVIDENCE LAW IN AUSTRALIA

Practice relating to documents as evidence in legal proceedings in Australia is complicated and varies according to jurisdiction.

If the legal proceeding is in a federal court (that is, the High Court, Federal Court, Family Court or the Federal Magistrates Court) or an ACT court, the Commonwealth Evidence Act applies.[1] The New South Wales, Tasmanian and Victorian Evidence Acts generally mirror the Commonwealth Evidence Act and its admissibility requirements. In other jurisdictions, the laws of evidence may vary.

Some provisions of the Commonwealth Evidence Act also apply in State and Territory legal proceedings in relation to some documents.

Commonwealth legislation (for example, the *Archives Act 1983* (**Archives Act**), *Freedom of Information Act 1982* (**FOI Act**), *Privacy Act 1988* (**Privacy Act**)) and *Crimes Act 1914* (Crimes Act)), has provisions about documents that may relate to their use in evidence. State or Territory legislation, policies and standards may also apply.

THE COMMONWEALTH EVIDENCE ACT

The Commonwealth Evidence Act provides for documents created and maintained in paper and electronic form to be admitted in evidence before federal courts.

The Commonwealth Evidence Act relaxed and, in some cases, removed restrictions on evidence that can be admitted in proceedings so that a greater range of relevant evidence is available to courts for fact finding purposes.

In relation to documentary evidence, the Commonwealth Evidence Act:

[1] Rules of evidence for the Federal Magistrates Court are contained in Part 15 of the *Federal Magistrates Court Rules 2001*. Certain *Evidence Act* provisions do not usually apply to child-related proceedings (Section 69ZT of the Family Law Act).

- abolishes the original document rule (also referred to as the 'best evidence rule'), replacing it with simple means of giving evidence of the contents of documents, including documents held in electronic and other non-paper forms;
- includes a narrower hearsay rule and wider exceptions to that rule, providing for greater admissibility of hearsay evidence;
- includes provisions for easier proof of, and presumptions about, business and official records, and documents recording an electronic communication; and
- includes pre-trial procedures enabling litigants to test the weight of documentary evidence that might be given in proceedings.

With a greater range of evidence admissible in many Australian courts, agencies must consider the quality of evidence available in a legal proceeding and whether that evidence is likely to persuade a court to accept the Commonwealth's version of the facts.

THE RULES OF EVIDENCE

The laws of evidence prescribe standards to which a fact must be proved:

- in civil proceedings, facts must be proved on the balance of probabilities; and
- in criminal proceedings, facts must be proved beyond reasonable doubt.

The rules of evidence govern what information is able to be placed before a court for determination of an issue. These rules influence how a party goes about proving its case.

Parties seek to persuade the court of a fact by producing evidence. In doing so, a party should consider three issues:

- how to adduce (that is, put to the court) evidence of the fact;
- whether the evidence is admissible (that is, whether the court will permit it to be given); and
- the weight of the evidence (that is, how much importance the court will give to it in reaching its decision).

The rules of evidence are mainly concerned with the first two issues:

- how information, in the form of 'evidence', is given or presented to a court; and
- whether that information can be admitted to the proceeding.

The admissibility of evidence in any proceeding is subject to compliance with the rules of admissibility and the interpretation placed upon them by the presiding judge. Assessment of the quality of evidence, and therefore of the weight to be given to it, is also matter for the presiding judge in each case.

THE DISTINCTION BETWEEN ADMISSIBILITY AND WEIGHT OF EVIDENCE

Although evidence of information about a particular fact may be admissible, the court will not necessarily believe or act on that evidence.

If the information about a fact is the direct observation of a witness, the court may simply disbelieve the witness. This may occur for a number of reasons. For example, it may have been a long time since the events in question happened, the witness may give confused testimony, or may have some physical incapacity (e.g. poor eyesight) or have some personal inclination or motivation that causes the court to disbelieve their evidence (e.g. it may be shown that the witness is inclined to lie, or bears ill-will against someone connected with the proceeding).

More usually, evidence of information given in court will not be 'direct observation' evidence. Instead it will be evidence that suggests, or from which it can be inferred, that a particular fact occurred. In this regard, the weight of evidence of a record can be adversely affected if it is not contemporaneous with the events it documents (i.e. if it is created well after the events it purports to record).

Example: Minute to the Secretary

The Commonwealth, in litigation, seeks to prove that a certain conversation took place. The Commonwealth has located a Minute to the Secretary of the agency which quotes from a file note of the conversation. However the actual file note of the conversation cannot be found.

The Commonwealth produces the Minute in evidence. That document is found to be admissible. The weight given to that evidence however may vary and depend on other evidence e.g. evidence by the author of the file note that the extract is a true extract, evidence that the file note was written at the time of the conversation.

DOCUMENTARY EVIDENCE

The rules of evidence apply to an ordinary document in writing, documents written in braille or shorthand and, importantly for modern records management systems, a document that is in a digital format.

The term 'document' is defined in the dictionary to the Commonwealth Evidence Act to mean any 'record of information', and includes:

- anything on which there is writing;
- anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;
- anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and
- a map, plan, drawing or photograph.

The definition of a 'document' also includes any part, copy, reproduction or duplicate of a document. Metadata, as information embedded or associated with a document, is generally considered part of a 'document'.

Example: Draft Versions of a Record

An agency involved in litigation has been ordered to give discovery of documents related to a particular issue.

The agency performs reasonable searches across their records and identifies a number of records, as documents, that are potentially discoverable. Searches have also identified draft versions of a potentially discoverable record. A draft version of a record falls within the definition of a 'document' under the Commonwealth Evidence Act and can be subject to an order for discovery.

The Commonwealth Evidence Act abolished the 'original document rule', which required the production of the original document in writing. The Commonwealth Evidence Act permits evidence of the contents of a document to be given in one of a number of alternate ways. These ways include tendering:

- the original document, which may be physical or digital;
- a copy (physical or digital) of the document produced by a device (such as a photocopier or a computer) that reproduces the contents of documents;
- a transcript of a document recording words (such as an audio tape or shorthand notes);or
- a business record being a physical or digital extract, summary or copy of the document.

Other ways may be used to give evidence of official documents, and documents that are unavailable to a party in the proceeding, for example, where they have been lost or destroyed.

While it is not necessary that the original document be produced, parties may still be required to authenticate evidence of the contents of documents tendered in one of these ways. For example, in relation to a document in writing that is signed, it remains necessary to lead evidence (if the point is contested) that the signature appearing on the document is the signature of the person who has purported to sign it. In the case of digital records, it may be necessary to give evidence that the digital record is what it purports to be.

While several provisions of the Commonwealth Evidence Act facilitate this authentication process, the Act also set out procedures under which a party may test the authenticity of evidence of the contents of documents led under one of the alternate ways in a proceeding. Usually, these procedures would be used by a party against whom evidence of the contents of a document is, or might be, led in a proceeding.

The procedures, which can be set in motion before the hearing of a proceeding, may result in the making of court orders against the party leading evidence of the contents of the document, including an order that:

- the original document be produced;
- a party be permitted to examine, test or copy a document;
- a person concerned in a records management system be called to give evidence; and/or

- in the case of a records management system, that a party be permitted to examine and test the way in which the document was produced or has been kept.

Example: Systems Reliability

An agency involved in litigation has presented a digital document as evidence from a system. The document is considered relevant to a key issue in the proceeding. However, the system in which the document was identified has not been managed in accordance with the agency's business practices for some time.

Based on an apparent discrepancy in the timestamp metadata (date created, etc.) associated with the document when compared with other documents presented as evidence, the opposing party has scrutinised the reliability of the system where the digital document was stored.

To address issues raised by the opposing party, the agency is required to divert resources from agency business and engage an independent expert to present evidence in relation to the reliability of the system, and authenticity of the presented document.

The ultimate sanction for failure to comply with such an order is that the evidence of the contents of the document is not to be admitted in the proceeding.

Not all jurisdictions have removed the requirement for the original document to be provided. Where the agency needs to provide evidence in a proceeding before a court that does not apply the Commonwealth Evidence Act, they should seek specific legal advice.

HOW DOCUMENTARY EVIDENCE MAY BECOME INADMISSIBLE

A separate issue from how evidence of information in a document can be given is whether the court will permit the evidence to be given (that is, whether the evidence is admissible in the proceeding before the court).

Whether the evidence is admissible depends, initially, on whether it is relevant to a fact in issue in the proceeding. If relevant, evidence may nevertheless be inadmissible if it is excluded by a rule that provides for the exclusion of particular kinds of evidence (for example, the rule against hearsay evidence, the 'similar fact evidence' rule, and the rule against opinion evidence).

The most important exclusionary rule in relation to documents is the hearsay rule. The hearsay rule applies when evidence of what is contained in a document is being used to prove some fact asserted in it.

Example: Note for file

Midway through the proceeding the file note quoted in the Minute to the Secretary is found. It contains the following words:
"Telephone conversation from James at agency X. James said that Alistair told him that he saw Pip taking home a secret work file. He thought that he saw the numbers and letters 'x100 and MOJ' on it. Five days later when news of a leak came through, it became apparent that the document leaked was from file x100908574, the SMOJK file."
Unless an exception to the hearsay rule applies, the document is inadmissible to prove that Pip took home the x100908574 file and that she leaked from it.

The hearsay rule under the Commonwealth Evidence Act applies to any statement made by a person other than while giving evidence that is led or given to prove the existence of a fact that it can be reasonably supposed that the person intended to assert by the statement.

There are many exceptions to the hearsay rule under the Act including:

- evidence admitted for a non-hearsay purpose (where the statement is relevant for a purpose other than to prove the existence of a fact that the person intended to assert, for example, where the fact that the statement was made is relevant). In such a case evidence of the statement can also be used as evidence of what is asserted by the statement;
- first-hand hearsay, the scope of the exceptions depending upon whether the proceeding is civil or criminal and whether the person who made the statement is available or not to give evidence;
- some categories of more remote hearsay (that is, where the evidence is not necessarily first-hand hearsay), such as some statements in business records, some tags and labels or writing attached to, or placed on, objects (including documents) in the course of business and representations in electronic communications regarding the identity of the sender or receiver or time or date the communication was sent; and
- an admission made by a person who is or becomes a party to the proceeding.

Some procedural safeguards apply for some of these categories of hearsay evidence. For example, for notifying the other parties if the person who made a statement admitted under one of the exceptions for first-hand hearsay is not to be called to give evidence in the proceeding, and other procedures under which a party may be required to call as a witness the person who made the statement.

THE RULES OF EVIDENCE IN COMMONWEALTH TRIBUNALS

The admissibility rules in the Commonwealth Evidence Act which determine whether evidence of information can be given in a proceeding, also apply to proceedings before '*a person or body ...that, in performing a function or exercising a power under a law of the Commonwealth, is required to apply the laws of evidence*'.

The majority of Commonwealth tribunals are not required to apply the laws of evidence. Most commonly, the statute under which the tribunal is created includes a provision to the effect that the tribunal is not bound by the rules of evidence, but may inform itself as it thinks appropriate.

This will not necessarily mean that the rules of evidence are irrelevant to tribunal proceedings. Tribunals may, for example, have regard to what would be admissible had the proceeding been before a court, especially when the outcome of the proceeding may be subject to judicial review. In any event, a tribunal (like a court or, indeed, any person or body with decision-making functions or responsibilities) is unlikely to believe and act on records or other documents unless they can be demonstrated as accurate and reliable.

COMPLIANCE WITH SUMMONS, SUBPOENAS AND ORDERS FOR DISCOVERY

Occasionally, agencies need to comply with requirements imposed by courts to produce or disclose documents needed for legal proceedings, including proceedings in which the Commonwealth is not a party. These requirements usually arise following the issue and service of a summons, subpoena or similar document in a proceeding, or by way of an obligation or court order.

Summons

A summons announces that a legal proceeding against the party summonsed has commenced and requires them to appear in court or respond in writing.

Subpoena

A subpoena is a court order requiring the giving of evidence, or the production to the court of documents, or both.

If served with a subpoena, an agency is obliged to either comply with it or apply to the court which issued the subpoena to set it aside.

A court will set aside a subpoena which is too wide or expressed in vague or general terms requiring the agency it is served on to make extensive searches through a huge volume of documents or to make fine judgements about the relevance of documents.

An agency served with a subpoena is entitled to recover reasonable costs of complying with that subpoena.

If the subpoena requires only the production of documents or a thing, an agency can comply by delivering the documents or the thing to the court which issued the subpoena within the time stated on the subpoena.

Discovery

Discovery is the process where parties to a legal proceeding identify and disclose to each other documents that are relevant to the issues in the proceeding. In some courts, an order for discovery may be made against a person or a body who is not a party to the proceeding.

Substantial obligations may be imposed upon agencies to whom an order for discovery is directed. Both processes require the agency to whom an order is directed to make a reasonable search for relevant documents, including documents held in a digital form, in their control. Performing a reasonable search may also require the agency to identify systems that have not been searched and documents that were, but are no longer, in the agency's control. For example, potentially discoverable documents that have been deleted in accordance with a disposal schedule.

In recognition of the burden (including time and cost) that discovery can cause, courts are increasingly reluctant to order discovery of all documents which might relate to the issues in dispute in a court proceeding, but to limit the scope of discovery to only what is necessary or that can be carried out sensibly taking into account all of the

circumstances, including the resources of the parties. *Practice Note CM 5 – Discovery*[2] provides further guidance for discovery in the Federal Court.

Practice Note CM 6 – Electronic Technology in Litigation[3] sets out a framework for managing the discovery of electronic documents in the Federal Court. It includes a checklist for parties to discuss the discovery of electronic documents at a pre-discovery conference and sample protocols to manage the exchange of discoverable documents between parties and the Court.

Depending on the circumstances, failure to comply with an order for discovery (e.g. to produce all documents falling within a stated description) may result in the agency being found in contempt of court.

COMPLIANCE WITH FREEDOM OF INFORMATION REQUESTS

The FOI Act gives every person a legally enforceable right of access to documents held by an agency and official documents of a minister, other than documents which are exempt under the Act. Of relevance to an agency's information compliance obligations, and in accordance with section 24A of the FOI Act, an agency must be able to demonstrate that it has taken all reasonable steps to find a document subject to a request for access before refusing the request.

Further assistance in relation to complying with the FOI Act should be sought from the Office of the Australian Information Commissioner, and/or your legal advisor.

RECORDS DESTRUCTION AND POSSIBLE LEGAL PROCEEDINGS

BAT Cases

The *McCabe v British American Tobacco Australia Services Ltd* (BAT) case signalled a significant change in the management of records required for evidence. In this landmark case, the Supreme Court of Victoria ruled that BAT had destroyed the records that would have helped Rolah McCabe's case. It found that although legal proceedings were not current, BAT's policy of destroying records that they could foresee being used as evidence in a lawsuit – even if it had not yet started – was an illegal action directed specifically at preventing the litigant from having a fair trial.

While this finding was overturned on appeal (*British American Tobacco Australia Services Ltd v Cowell*), it signalled a potential shift in the court's view on records management requirements, and may be taken up in other jurisdictions, including the Commonwealth. Specifically, the court ruled that records documenting actions where it would be reasonable to assume that there may be litigation, should be kept whether or not a legal action has commenced. This replaces the previous requirement that destruction of records cease only after the announcement of litigation.

The issue in the original McCabe ruling was correspondence between BAT and Clayton Utz, BAT's lawyers in Australia, advising BAT to destroy certain records. The

[2] www.fedcourt.gov.au/how/practice_notes_cm5.html
[3] www.fedcourt.gov.au/how/practice_notes_cm6.html

Supreme Court of Victoria ruled that ad hoc destruction of records for the purpose of hampering a case against a company, even though the action had not yet been commenced, was a criminal action.

When BAT appealed the decision, they established that the destruction of records was neither in contempt of the court nor a deliberate attempt to pervert the course of justice by convincing the court that the purpose of advice from Clayton Utz was to use records storage space more economically.

R v Ensbey

In *R v Ensbey (2004); ex parte A-G (Qld)*, the Supreme Court of Queensland Court of Appeal considered the provisions of section 129 of the Queensland Criminal Code which provides for an offence when a person knowing that a document may be required in evidence in a judicial proceeding wilfully renders it illegible or indecipherable with intent to prevent it from being used in evidence. In that case, the court found that it was sufficient to prove the offence if a person believed that the document may be required in evidence in a possible future proceeding, that they rendered them illegible or indecipherable with the intent to prevent them being used for that purpose.

There is a similar offence provision set out in section 39 of the *Crimes Act 1914* (Cth). This provision provides that:

> *Any person who, knowing that any book, document, or other thing of any kind, is or may be required in evidence in a judicial proceeding, intentionally destroys it or renders it illegible or undecipherable or incapable of identification, with intent to prevent it from being used in evidence, shall be guilty of an offence.*

However, the effect of certain provisions of the *Criminal Code 1995* (Cth) is to make the state of knowledge under a Commonwealth offence stricter. The meaning of 'knowledge' is defined in s5.3 of the *Criminal Code 1995* (Cth) as:

> *A person has knowledge of a circumstance or a result if he or she is aware that it exists or will exist in the ordinary course of events.*

R v Selim

These provisions have been considered by the Supreme Court of NSW in *R v Selim (2007)*. In that case, the court distinguished the decision in *Ensbey* on the basis of the differing legislative provisions and found that it must be established, at the time when the document was destroyed that the person was aware, in the sense that they had a reasonable contemplation, that there was a possibility of judicial proceedings being initiated in the future.

Implications for Commonwealth Government agencies

These cases signal a change in judicial consideration of records disposal. In the past, destruction has been permitted if there were no current legal proceedings, but it has become important for agencies to consider the potential legal cases associated with the records that they generate, and whether their destruction might pervert the course of justice.

The Archives Act provides that Commonwealth records are normally not to be destroyed without the permission of the National Archives, in the form of a records authority issued by the National Archives. Records authorities are based on a thorough analysis of the legal delegates, business activities and stakeholder requirements at the time of issue. Destruction of records in accordance with records authorities is systematic, rather than ad hoc, and records authorities take into consideration all foreseeable uses of the records.

As long as there is no change in context, it is unlikely that records destroyed pursuant to a valid records authority would be considered to be destroyed with the intention of spoiling a litigant's case.

Agencies are not required to keep every record just in case they may one day be needed in a future judicial proceeding. However, agencies are advised to retain and maintain records in an accessible form if the agency knows it is reasonably likely that the record may be needed as evidence in a:

- current judicial proceeding (this includes a legal proceeding or inquiry); or
- a future judicial proceeding that will be commenced or will likely be commenced.

A valid records authority does not exempt Commonwealth Government agencies from this obligation.

It is likely that other jurisdictions may have differing provisions. If it is likely that Commonwealth Government agency records will be required as evidence for offences under State legislation or if there are additional questions, agencies should seek legal advice.

IMPLICATIONS OF THE ELECTRONIC TRANSACTIONS ACT FOR EVIDENCE

The rules of evidence are unaffected by the *Electronic Transactions Act 1999* (Cth) (**Electronic Transactions Act**).

The Electronic Transactions Act intends to promote confidence in electronic transactions by confirming that a permission or requirement under a law of the Commonwealth to provide information in writing, a signature, or to retain information can be met by electronic means unless specifically excluded by other Commonwealth legislation, or the *Electronic Transactions Regulations 2000* (Cth). For example, the Electronic Transactions Act provides that where a person is required to provide a document, the provision of that document will not be invalid because it took place in an electronic communication. Similarly, it enables the recording, and retention of information in an electronic form to meet statutory requirements to retain a written record.

The Electronic Transactions Act states that the integrity of information contained in a document is maintained if, and only if, the information has remained complete and unaltered, apart from the addition or endorsement, or any immaterial change which arises in the normal course of communication, storage or display.

There are a number of exclusions from the Electronic Transactions Act, some of which are widely used in evidence, such as Statutory Declarations. In these cases, the original form of the record is still required for evidence.

RECORDS MANAGEMENT REQUIREMENTS

Preliminary

Agency managers must ensure that their business practices and records management systems can stand up to the scrutiny of the courts, parliament, the Information Commissioner, the Ombudsman and relevant auditors. Individuals are also important stakeholders in this process and have rights of redress through a range of institutions, and access to records and other information through the Archives Act, FOI Act and Privacy Act.

In addition, the need to comply with subpoenas, orders for discovery and FOI requests presents significant implications for an agency.

Prudent management of your agency's compliance obligations therefore requires the ability to:

- undertake documented searches to identify and produce all potentially relevant documents as evidence, including any associated metadata, across an agency's systems, within short timeframes; and
- identify systems that have not been searched as part of an agency's response to a request or an order.

Reviewing records management practices

As Commonwealth Government agencies change their business practices and record management systems, records management practices should be reviewed so that agencies continue to adequately address agency risks and meet legal and other obligations to manage and produce records that are full and accurate.

Even in agencies where formal digital records management systems are not in place, it is possible to implement records management strategies and practices to address some risks.

Agencies should take special precautions to ensure that records reasonably likely to be required for legal purposes will be legally acceptable. Establishing the authenticity and reliability of records may depend on the accuracy of the process or system used to produce the record, the source of the information in the record, the method and time of its preparation, and the controls used to manage the record (including metadata about the record). Problems may arise with admissibility if appropriate procedures are not followed in creating and maintaining records.

The primary purpose of keeping records is to support the business of the agency. Records are also used to account for agency actions to government and the community. Decisions about the creation, maintenance and use of records and their management systems must be made in the context of laws and regulations under which the agency operates. They must also conform with established records management, data processing, auditing and related professional practices and standards, and with

applicable administrative rules and policies. This process needs to include an assessment of the risks, costs and benefits associated with current records management and information systems, and any refinements which may be required to improve them.

Establishing a records management and systems management regime

Meeting evidentiary requirements in a complex, changing technological environment is a challenging undertaking that requires cooperation and coordination within agencies. To ensure that records which are reasonably likely to be required as evidence in judicial proceedings are complete and accurate, an agency must maintain a comprehensive, credible information and records management regime. This requires formal organisational arrangements and clarification of the responsibilities of records management. These should be stated in policies and guidelines relating to records management and business information systems.

Agencies must ensure the appropriate number, quality and proficiency of staff responsible for stewardship of an agency's information assets, including records. Agency staff must understand their responsibility to produce and maintain accurate and reliable records, supported by rules, procedures and training.

In summary, corporate managers, records managers, information managers, administrative support staff, and information technology professionals all need to be involved in the records management process to ensure that records are produced by electronic information systems and that they are authentic, accurate and reliable.

To establish an appropriate records management regime, agencies need to:

- undertake a strategic analysis of corporate information and records management requirements, based on legal and customer obligations, government and business requirements, risks and costs;
- produce written policies and procedures to define normal operations for development, maintenance, and use of digital information and records management systems;
- provide training and support to help ensure that policies and procedures are understood and implemented by staff;
- ensure records management requirements are built into electronic information systems that enable the capture and ongoing management of appropriate records; and
- ensure that records in business information systems are only disposed of in accordance with authorisation provided by the National Archives.

FURTHER INFORMATION

National Archives of Australia

The National Archives website includes a number of publications about records management, particularly in the Commonwealth Government environment.

- Digital records advice
- General Records Authority for Source (Including Original) Records after they have been Copied, Converted or Migrated, 2011
- Digitising accumulated physical records
- Check-up 2.0

Legislation

Link to all referenced legislation via ComLaw or Australasian Legal Information Institute (AustLii) website.

Case Law

British American Tobacco Australia Services Ltd v Roxanne Joy Cowell (as representing the estate of Rolah Ann McCabe deceased) (2002 VSCA 197), published on the AustLii website.

Rolah Ann McCabe v British American Tobacco Australia Services Ltd (2002 VSC 172), published on the AustLii website.

R v Ensbey; ex parte A-G (Qld) (2004 QCA 335), published on the AustLii website.

R v James Selim (2007 NSWSC 362), published on the AustLii website.

Standards

Australian standards such as AS ISO 15489 are available for purchase from SAI Global.