Department of Industry

Policy

Records Management

NUMBER **IND-I-177**	VERSION 2
AUTHORISED BY Deputy Secretary Finance, Strategy and Operations	AUTHORISED DATE 27/10/2015
ISSUED BY Finance, Strategy and Operations	EFFECTIVE DATE 27/10/2015

Policy Statement

The NSW Department of Industry, Skills and Regional Development (the "department") is committed to ensuring that full and accurate records of its business activities and decisions are created and managed to support the business and to comply with legislative requirements. It is recognised that good recordkeeping practice contributes to, and protects the department's important information assets and supports the achievement of overall outcomes.

The department will implement fit-for-purpose information and records management practices and systems to enable the creation, maintenance and protection of authentic, reliable and useable records that can easily be accessed when required, by those with authority to do so.

Scope

This policy applies to:

- all personnel who work on behalf of the department (including contractors and consultants);
- any individuals or organisations to which the department has outsourced functions or activities, and therefore associated recordkeeping responsibilities; and
- all aspects of the department's operations and all information and records, in any format, created or received, which provide evidence of business activities or decisions.

Requirements

1. *Creation and Capture*
   a. All staff should ensure that they routinely create records that provide evidence of their work activities and/or decisions. This includes, but is not limited to, documenting meetings and telephone conversations, and keeping copies of documents, emails, and other correspondence, including text and/or instant messages along with records of approved work-related social media usage.
   b. Staff members should ensure that electronic and physical records are captured into the appropriate system for the type of record being managed to ensure that the record can withstand independent scrutiny. This includes using HP Records Manager to manage electronic or physical documents, or other approved business systems, such as SAP ByDesign.
   c. Operational procedures should be documented and clearly set out the records and information to be captured as part of that process.
   d. Where possible, electronic records should be captured in an electronic format. This requires electronic records to be captured into the department's official digital recordkeeping systems rather than printed and placed on a physical file.
2. *Storage*
   a. All work-related records should be stored in conditions appropriate to their format and use to prevent their unauthorised access, use, alteration, disclosure, destruction or removal.

b. Physical records must be stored in accordance with the *Standard on the Physical Storage of State Records.* They should be handled with care to avoid accidental damage or loss and returned to their appropriate place of storage when not in use. The current location of physical records should be maintained in HP Records Manager.

c. Records classified as "Protected" or higher under the department's *Classified Information Policy* cannot be stored electronically and must be physically stored and secured appropriately.

d. The management of physical records that are currently active or in use will be the ultimate responsibility of the business unit that created the record.

e. Physical records requiring long-term storage will be held in a central location as advised by the Knowledge Management and Business Systems Unit.

3. Disposal

a. Disposal of records may only be undertaken in accordance with the department's records retention and disposal guidelines. This applies to physical and electronic records and includes records held in any of the department's business systems.

b. Only authorised, delegated staff members may approve, undertake or arrange for the destruction of records. The exception is for unimportant documents such as some drafts, duplicates, rough working documents and unsolicited promotional material which may be destroyed under the Normal Administrative Practice (NAP) provision of the *State Records Act 1998*.

c. Records authorised for destruction must be destroyed by secure means such as shredding or using secure destruction bins.

d. Records required to be kept as State archives in a relevant retention and disposal authority, issued by NSW State Records, will be transferred to State Records when the record is no longer in use for official purposes.

4. Access / Security

a. Records must be accessible to all staff in the department where required to perform their role. Exceptions include where there are confidentiality, privacy, legal or other legitimate business reasons for limiting access.

b. Unless authorised to do so by legislation, a departmental policy, directive, guideline or procedure, staff must ensure that they do not use or disclose any confidential or personal information. Unauthorised use or disclosure may cause harm or reputational loss to individuals, or give an individual or an organisation an improper advantage. All staff must ensure that confidential information in any form (both physical and electronic) cannot be accessed by unauthorised people and that sensitive information is only shared with people who are authorised to access the information and have a 'need-to-know'.

c. Access to the department's records by members of the public is governed by the *Government Information (Public Access) Act (GIPA) 2009* (NSW) and the *State Records Act 1998* (NSW). Advice and guidance relating to GIPA is available on the department's website.

d. Staff members must seek advice from the department's Legal Services area before responding to requests for information from an external party as part of a subpoena or legal warrant.

e. Records must be classified, labelled and handled in accordance with the *NSW Government Digital Information Security Policy* (M2012-15), the NSW *Information Classification, Labelling and Handling Guidelines* (July 2015) and related departmental policies.

5. External Parties

Contracts or agreements with external parties where the department has outsourced any functions or activities, or with whom the department has entered into any service arrangements with, must include records and information management provisions. These should:

a. ensure compliance with our legislative obligations;

b. minimise risks associated with the external storage of departmental records or information;

c. ensure that appropriate records of outsourced functions or activities are made and kept;

d. ensure that ownership of records is clearly addressed;

e. ensure that records or information are accessible as appropriate and when required;

f. ensure that records of outsourced functions or activities that are required after a contract has ended are returned to the department; and

g. ensure records of outsourced functions or activities are disposed of lawfully.

6. Continuous Improvement / Monitoring of Compliance

a. The Knowledge Management and Business Systems Unit will undertake regular assessments of business unit performance against the records management policy and any supporting procedures or guidelines.

b. Where opportunities for improvement or risks to compliance are identified, the Knowledge Management and Business Systems Unit will provide guidance and advice to remediate issues and drive greater efficiency in the management of records.

Procedures

- Procedures and advice are available on the Intranet.

Roles and responsibilities

The **Secretary** has overall responsibility for ensuring that the department complies with the requirements of the *State Records Act 1998* (NSW) and its supporting regulations.

The **Chief Financial and Knowledge Officer** is the *Senior Responsible Officer* who has responsibility for the oversight of records and information across the department as per the requirement within the *Standard on records management for the NSW public sector*. This includes establishing, developing and maintaining a records management program.

The **Knowledge Management & Business Systems Unit (KM&BS)** is responsible for:
- providing advice and training in order to enhance the creation, storage, access and reuse of records and information;
- implementing quality controls to ensure policies, procedures and standards for recordkeeping are maintained across the organisation;
- maintaining the department's Vital Records Register;
- coordinating and maintaining long term off-site storage; and
- liaising with appropriate managers to authorise the appropriate destruction of records.

The **Chief Information Officer** is responsible for:
- ensuring that information management system projects consider records management requirements when acquiring and implementing new systems or databases or decommissioning existing information management systems; and
- providing infrastructure and support to ensure records kept in electronic form are managed so that they are accessible, readable, complete, inviolate and authentic for as long as they are required to be kept. This includes security measures applied to data backups and audit logs

Business System / Process Owners are responsible for:
- ensuring records and information management is considered and included in systems and processes used. This includes:
  - assessing their systems for appropriate recordkeeping functionality;
  - considering recordkeeping requirements during the development phase and re-assessing recordkeeping functionality when systems undergo major upgrades or changes in functionality; and
  - considering recordkeeping requirements when systems are to be replaced so that requirements continue to be met in the new system.

Senior Executives are responsible for:
- fostering and promoting a culture that promotes sound records and information management practice within their business area;
- providing high-level direction and support (including ensuring adequate resourcing) for records and information management; and
- considering recordkeeping requirements for their business, especially as a part of new programmes of work.

All **Managers** are responsible for:

- ensuring that records are created within their business unit and managed in accordance with policy and procedures;
- ensuring staff are trained in how to create and manage records;
- ensuring operational procedures and processes adequately describe recordkeeping to ensure records are captured efficiently and to support their business outcomes;
- identifying vital or key records in their business unit and assisting in planning for disaster recovery and business continuity;
- participating in planning and managing projects to sentence legacy records and reduce hard copy files;
- ensuring that work-related records are only destroyed after appropriate authorisation has been provided; and
- ensuring that records storage areas under the control of their business unit are secure and protect records from accidental damage or loss or unauthorised access.

All **Staff** are required to:

- comply with the Records Management Policy and related procedures or guidelines;
- create full and accurate records of their work activities, including records of all substantive decisions and actions made in the course of their work – the more significant the decision or action, the more detailed the record should be;
- ensure that records are saved into the appropriate system; and
- ensure that records are accessible (including tracking the location of physical files) and appropriately secured.

Safety considerations

Reduce manual handling requirements by encouraging electronic records management over physical files. Staff should consider safe manual handling process when working with physical records.

Delegations

Level 4 Managers and above (as defined by the department's financial delegations), in conjunction with the Director of Knowledge Management and Business Systems, have authority to approve the destruction of records in accordance with the appropriate retention and disposal authority.

Definitions

- *Archives*: Those records that are appraised as having continuing value. [AS 4390-1996-1: 4.5]
- *Disposal*: A range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from recordkeeping systems. They may also include the migration or transmission of records between recordkeeping systems, and the transfer of custody or ownership of records. [AS 4390-1996-1: 4.9]
- *Personal Information*: Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. [Adapted from *Privacy and Personal Information Protection Act 1998 (*NSW), Part 1, s4]
- *Recordkeeping*: Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information. [AS 4390-1996-1: 4.19]
- *Recordkeeping requirements*: Requirements arising from regulatory sources, business needs and community expectations that identify the types of records that should be created and the management framework needed in order to have, and accountably manage, all the business information that is necessary for an organisation. [NSW State Records, Glossary of Recordkeeping Terms, available at http://www.records. nsw.gov.au]
- *Recordkeeping systems*: Information systems which capture, maintain and provide access to records over time. [AS ISO 15489.1-2002: 3.17]
- *Record*: Any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means. [*State Records Act 1998 (*NSW) s3] (Also see definition of a State Record)

- *Records management program*: A records management program encompasses the management framework, the people and the systems required within an organisation to manage full and accurate records over time. This includes the identification and protection of records with longer-term value that may be required as State archives. [NSW State Records, Glossary of Recordkeeping Terms, available at http://www.records.nsw.gov.au]
- *Retention and Disposal Authority*: Documents authorised by the Board of State Records NSW that set out appropriate retention periods for classes of records. There are two main types: Functional retention and disposal authorities authorising the retention and disposal of records unique to a specific organisation; and General retention and disposal authorities authorising the retention and disposal of records common to more than one organisation. [NSW State Records, Glossary of Recordkeeping Terms, available at http://www.records.nsw.gov.au]
- *State archive*: A State record that the State Records Authority of New South Wales has control of under the NSW State Records Act [State Records Act 1998 (NSW) s3]
- *State record*: Any record made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office or for any purpose of a public office, or for the use of a public office. [*State Records Act 1998 (*NSW) s3] (Also see definition of a Record)
- *Vital records*: Those records that are essential for the ongoing business of an agency, and without which the agency could not continue to function effectively. The identification and protection of such records is a primary object of records management and counter disaster planning. [Acland, Glenda. 'Glossary' in Judith Ellis (ed.) *Keeping Archives*. 2nd Edition, Australian Society of Archivists Inc, Thorpe Publishing, Port Melbourne, 1993, p. 480]

Legislation and Standards

- *State Records Act 1998* (NSW)
- *State Records Regulations 2010* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Crimes Act 1900* (NSW)
- *Electronic Transactions Act 2000* (NSW)
- *Evidence Act 1995* (NSW)
- *Government Sector Employment Act 2013* (NSW)
- *Independent Commission Against Corruption Act 1998* (NSW)
- *Limitations Act 1969* (NSW)
- *Public Finance and Audit Act 1994* (NSW)
- *Public Interest Disclosure Act 1994* (NSW)

- Standard on Records Management for the New South Wales Public Sector (NSW State Records, March 2015)
- Standard on the Physical Storage of State Records (NSW State Records, 2012)
- Australian and International Standard AS ISO 15489-2002, Records Management
- Australian Standard AS 4390-1996, Records Management

Related policies

- TI-G-124 Social Media Policy
- TI-A-130 Code of Conduct
- TI-G-147 Standing order 52 – responses
- TI-A-154 Classified Information Policy
- TI-A-155 Privacy Management Plan
- TI-O-159 Accessing and using the Department's TRIM system remotely from Ministers' offices policy

Other related documents

- NSW State Records "Useful Resources" available at http://www.records.nsw.gov.au
- NSW Government Cloud Services Policy and Guidelines (August 2015)
- NSW Government Digital Information Security Policy (Department of Premier and Cabinet, M2012-15)
- NSW Government Information Classification, Labelling and Handling Guidelines (July 2015)
- NSW Government ICT Strategy (May 2012)
- DIGITAL+ - NSW Government ICT Strategy Update 2014-15

- NSW Ombudsman's Good Conduct and Administrative Practice Guidelines for Public Authorities and Officials (May 2006)

Superseded documents

This policy replaces:
- A-043 Records Management
- TI-A 153 Records Management

Revision history

Version	Date issued	Notes	By
1.00	19-12-2013	Creation of original policy (TI-A 153).	Group Manager, Knowledge Management and Business Systems
1.01	20-08-2015	Updated policy after internal review.	Ross Sanson / Randi Birkin - Knowledge Management and Business Systems
1.02	16-09-2015	Updated policy after review by: • Director Knowledge Management and Business Systems • Chief Financial and Knowledge Officer	Randi Birkin, Knowledge Management and Business Systems
1.03	21-09-2015	Updated to reflect allocation of new policy number (IND-1-177).	Randi Birkin, Knowledge Management and Business Systems
2.00	27-10-2015	Updated policy approved.	Deputy Secretary – Finance, Strategy and Operations Division

Review date

30/06/2017

Contact

Knowledge Management and Business Systems