Records Management Policy

Policy Number	DOC20/179852	Version	2
Authorised by	LLS Senior Executive Team	Authorised date	7 December 2020
Responsible Officer	Director, ICT	Issue date	15 December 2020
Category	Business	Review date	15 December 2023

Policy Statement:

Local Land Services (LLS) is committed to ensuring that complete 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 protects and contributes to LLS important information assets and supports the achievement of overall outcomes.

LLS will implement information and records management practices and systems to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records. LLS will safeguard the protection of all personal and confidential information.

Scope

All employees of LLS are expected to exhibit integrity, service and accountability, and build public trust in our work and organization. This policy is part of a suite of policies that demonstrates ethical conduct in our workplace. This policy applies to all business units, regions and offices of LLS.

This policy applies to:

- all personnel who work for or on behalf of LLS (including contractors and consultants)
- any individuals or organisations to which LLS has outsourced functions or activities, and therefore associated recordkeeping responsibilities
- all aspects of LLS operations and all information and records, in any format, created or received, which provide evidence of business activities or decisions
- all aspects of LLS operations whether performed in a NSW Government office or working remotely including, working in the field or working from home.

Requirements

1. Creation and Capture

a. Section 12(1) of the *State Records Act 1998 (NSW)* requires that LLS make and keep full and accurate records of its activities. All staff must take appropriate measures to create and capture records of activities, decisions and actions made in the course of their work to:

- explain why decisions or actions have been made or taken which impact upon individuals or organisations
- enable current and future staff to take appropriate action and make well-informed decisions
- protect individuals or organisations affected by our decisions or actions
- enable an authorized person to examine the conduct of the organisation's business (such as for an audit, investigation or inquiry)
- protect the financial, legal and other rights of the organization along with everyone who works for the organisation
- preserve the history and heritage of NSW.

This includes but is not limited to; documenting meetings and telephone conversations, capturing web content, 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 (e.g. Facebook, Twitter, LinkedIn, chats, wikis, discussion boards/forums).

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 HPE Content Manager (CM9) to manage electronic or physical documents, or other approved business systems where recordkeeping requirements have been considered and incorporated, such as MyHQ. Important or useful records are not to be kept alone in email folders, shared drives, personal work drives, Microsoft OneDrive, Microsoft Teams, or in any other unapproved location.

c. Operational procedures should be documented and clearly define the records and information to be captured as part of that process.

d. Where possible, records should be captured in an electronic format. This requires records to be captured into LLS official electronic recordkeeping systems rather than printed and placed in a physical file.

2. Storage

a. All work-related records must be stored in conditions appropriate to their format and use to prevent their unauthorised access, use, alteration, disclosure, destruction or removal.

b. LLS must comply with the *PPIP Act* principles as per NSW Information Privacy Commissioner's Office requirements.[1]

c. 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

[1] IPC Fact Sheet – Understanding your privacy obligations – for public sector staff

returned to their appropriate place of storage when not in use. The current location of physical records should be registered and maintained in CM9.

e. Records classified as "Protected" or higher in accordance with the NSW Information, Classification, Labelling and Handling Guidelines cannot be stored electronically and must be physically stored and secured appropriately (with the physical file registered in CM9).

f. 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.

g. Physical records requiring long-term storage will be held in a central location as advised by the Information, Communication and Technology Unit.

3. Retention and Disposal

a. Disposal of records may only be undertaken in accordance with the applicable records retention and disposal authority approved by the NSW State Archives and Records Authority. This applies to physical and electronic records held in any location, system or application.

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 (NSW)* and *State Records Regulations 2015 (NSW).*

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

d. All hard copies of confidential business information used in the course of day to day operations must be shredded or placed in a secure destruction bin and not placed in wastepaper or recycling bins. The definition of confidential business information includes but is not limited to details or information relating to employees, customers, projects, business operations and financial transactions.

e. Records maintained in CM9 are assigned the applicable retention schedule based on the classification terms selected for the Virtual File containing the records. Virtual files containing records relating to completed activities, matters or projects should be closed in order to trigger the archiving process.

f. Records required to be kept as State Archives in a relevant retention and disposal authority will be transferred to State Archives when the record is no longer in use for official purposes.

4. Protection of, and Access to records

a. Records must be accessible to all staff in LLS so that staff who have a legitimate 'need-to-know' can perform their roles effectively and efficiently. Exceptions include where required by law to restrict access, or where there are confidentiality, privacy, sensitivity, legal or other legitimate business reasons for limiting access.

b. Appropriate security and access controls must be maintained for any system, workplace or storage area that stores records and information in any format. Controls must be:

- Proportional to the sensitivity of the stored records and information based on an assessment of business and records management risks;
- Capable of preventing the unauthorized access, removal, use, alteration, concealment, disclosure, or unlawful destruction of deletion of records and information; and
- Prevent the accidental damage or loss of records and information.

c. Unless authorised to do so by legislation, a LLS policy, directive or procedure, staff must not use or disclose any records or information (especially confidential or personal information) that would not normally reasonably be expected to be made available for general public consumption, to any unauthorized individuals or organisations. LLS staff cannot be directed to issue information by an Authority Figure if it is in direct violation of current legislation or any LLS policy or our Code of Ethics and Conduct. Work-related records and information must not be used in any way which would:

   - give an unfair or improper advantage or benefit (either commercial or otherwise) to any external individuals or organisations
   - facilitate a personal benefit (either directly or indirectly) for any individual working for LLS
   - involve the improper or unauthorized use or disclosure or records and information after separation from LLS (such as through retirement or resignation)
   - cause harm (such as financial) or reputational loss to individuals or organisations
   - cause an invasion of an individual's or organisation's privacy
   - prejudice or undermine the effectiveness or integrity of any function, activity or process, including any investigation, enforcement, regulatory, monitoring, audit or review activity
   - be premature (e.g. involving the inappropriate disclosure of working documents prior to a final decisions being made).

d. Restricting access to records maintained in CM9 should be done using CM9's Access Controls functionality. Access and modification to records is monitored in CM9 and able to be audited.

e. Access to the LLS records and information by members of the public is governed by the *Government Information (Public Access) Act 2009 (NSW) (GIPAA)*, the *Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA)*, the Health Records and Information Privacy Act 2002 (NSW)(HRIP) and *the State Records Act 1998 (NSW).* This applies to all records in any format held by the Department and stored in any location.

f. While access to records and information by members of the public is a fundamental right in a democratic society, this must still be balanced between the need on the one hand for LLS to be transparent and accessible to the public, and the need on the other hand to protect the integrity of LLS records and information. All staff must:

   - Have regard to requirements and responsibilities specified within our Code of Ethics and Conduct which encourages the disclosure of a broad range of information, and
   - Must not disclose or handle records and information in any way which would undermine requirements within this policy or the *Code of Ethics and Conduct*.

g. Advice and guidance relating to both the *PPIP* and *GIPA Act* is available via the LLS website.

h. Staff members must refer all requests for information from an external party as part of a subpoena, legal warrant or Standing Order 52 to LLS Risk and Assurance Unit in the first instance (via accesstoinformation@lls.nsw.gov.au).

i. The *NSW Information, Classification, Labelling and Handling Guidelines* define sensitive and classified information, and specify requirements in relation to their labelling and handling. All staff must comply with requirements of this Guideline, along with any supporting LLS guidance, procedure or directive.

5. External Parties

Contracts or agreements with external parties where LLS has outsourced any functions or activities, or with whom LLS has entered into any service arrangements with (including cloud computing arrangements), must include records and information management provisions. These must:

a. comply with our legislative obligations

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

c. ensure that appropriate records of outsourced functions or activities are created and maintained

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 LLS

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

6. Continuous Improvement and Monitoring of Compliance

a. The Information, Communication and Technology 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 Information, Communication and Technology Unit will provide guidance and advice to remediate issues and drive greater efficiency in the management of records.

Procedures

- LLS Records Management Operational Guide
- Department of Regional NSW documents and advice available on the intranet

Roles and responsibilities

1. LLS Chief Executive Officer

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

2. LLS Director ICT Program

a. The LLS Director ICT Program is the Senior Responsible Officer who has responsibility for the oversight of records and information across LLS as per the requirement within the Standard on records management *[Standard: No. 12 issued under the State Records Act 1998 (NSW)]*. This includes establishing, developing and maintaining a records management program.

b. The LLS Director ICT Program is the LLS Policy Steward, whose role is to oversee the effectiveness of the application of the policy across the agency, and report to members of the Senior Executive Team to enable them to monitor policy effectiveness.

3. LLS Information, Communication and Technology Unit

The LLS Information, Communication and Technology Unit is responsible for:

a. providing advice and training in order to enhance the creation, storage, access and use of records and information

b. implementing quality controls to ensure policies, procedures and standards for recordkeeping are maintained across the organisation

c. coordinating and maintaining long term off-site storage

d. liaising with appropriate managers to authorise the appropriate destruction of records

e. ensuring that the migration of records and information through system and service transitions ensures that records are protected and remain accurate, reliable, complete and authentic and that requirements within *the General Retention and Disposal Authority* for original source records that have been migrated have been met.

4. Chief Information Officer[2]

The Chief Information Officer (or equivalent role) is responsible for:

a. ensuring that information management system projects consider records management requirements when acquiring and implementing new systems or databases or decommissioning existing information management systems

b. providing infrastructure and support to ensure records kept in electronic form are managed so that they are accessible, legible, 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

5. Business System / Process Owners

Business System / Process Owners are responsible for:

a. 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
- considering recordkeeping requirements when systems are to be replaced so that requirements continue to be met in the new system
- in conjunction with the LLS Information, Communication and Technology Unit, ensuring that the migration of records and information through system and service transitions ensures that records are protected and remain accurate, reliable, complete and authentic and that requirements within the General Retention and Disposal Authority for original source records that have been migrated have been met.

6. LLS Senior Executive Team

The Senior Executive Team is responsible for:

[2] DPIE CIO

a. fostering and promoting a culture that promotes sound records and information management practice within their business area
b. providing high-level direction and support (including ensuring adequate resourcing) for records and information management
c. considering recordkeeping requirements have been considered within their business area, such as part of any new program of work.

7. LLS Managers

All Managers are responsible for:

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

8. All LLS Staff

All members of staff (including contingents or contractors) are required to:

a. comply with the records management policy and related procedures or guidelines
b. 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
c. ensure that records are saved into the appropriate, approved system
d. ensure that records are accessible (including tracking the location of physical files) and appropriately secured.
e. Complete the following introductory recordkeeping online training that is available to them via the Learning Management System (LMS):
    - Recordkeeping Fundamentals
    - Handling Sensitive Information

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

LLS Senior Executives and above have authority to approve the destruction of records in accordance with the appropriate retention and disposal authority.

Definitions

Term	Definition	Reference (if applicable)
Archives	Those records that are appraised as having continuing value.	
CM9	HPE Content Manager, the official electronic document and records management (EDRMS) system for LLS	
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.	
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.	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.	
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	Recordkeeping systems: Information systems which capture, maintain and provide access to records over time.	
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 NSW State Archives and Records Authority Board 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 Archives and Records 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 *State Records Act 1998 (NSW)*	*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

- *State Records Act 1998 (NSW)*
- *State Records Regulations 2015 (NSW)*
- *Privacy and Personal Information Protection Act 1998 (NSW) [PPIPA)*
- *Government Information (Public Access) Act 2009 (NSW) [GIPA]*
- *Crimes Act 1900 (NSW)*
- *Electronic Transactions Act 2000 (NSW)*
- *Evidence Act 1995 (NSW)*

Health Records and Information Privacy Act 2002 (NSW) (HRIP) Related policies

- *M2012-15 Digital Information Security Policy*

Other related documents

- Department of Regional NSW *Code of Ethics and Conduct*
    - Supporting documents https://intranet.regional.nsw.gov.au/support-and-services/managing-records-and-information
- *AS ISO 15489.1: 2017 Information and documentation - Records management, Part 1: Concepts and principles*
- *Standard on the physical storage of State records (NSW State Archives and Records, Issued 2019)*
- *Standard on records management [Standard: No. 12 issued under the State Records Act 1998 (NSW)].*
- *NSW Government Information Classification, Labelling and Handling Guidelines (August 2020)*
- *Fact Sheet - Information Protection Principles (IPPs) for agencies - Updated May 2020*
- *Fact Sheet - NSW public sector agencies and notifiable data breaches - Updated September 2020*

Superseded documents

This policy replaces:

- LLS Records Management Policy V1

Contact

Director, ICT