Records and Information Management Policy

Purpose of this policy

The Department of Planning and Environment (department) is committed to implementing and maintaining records and information management behaviours and practices that meet our work needs, accountability requirements along with government and community expectations for sound recordkeeping. It is recognised that our records, information and data are valuable assets which support the delivery of quality services for the community.

As part of meeting our overall commitments, records and information management requirements are a mandatory component of business process, operational activity and systems design or acquisition.

Guidelines, procedures and directives supporting this policy are located on the records and information management intranet pages.

To whom this policy applies

- all employees, consultants and contractors of all department Cluster entities that have people employed in or though the department. Including Environment Protection Agency.
- any individuals, consultants or organisations to which the department has outsourced functions or activities, and therefore associated recordkeeping responsibilities
- all aspects of the department's operations and all records and information in any format and in any location, created or received, which provide evidence of work-related activities, decisions or actions.

Related entities that are not employees of the department may opt to use this policy or establish an equivalent policy in accordance with section 12(2) of the State Records Act 1998. Exemptions from the provisions of this policy may be obtained by approval from the Secretary.

Policy requirements

Creation and capture

Section 12(1) of the State Records Act 1998 (NSW) requires the department to make and keep full and accurate records of our work. Records created or received must be captured into Business Systems certified for recordkeeping and described and classified in accordance with the department's standards, procedures and local business rules developed according to assessment of risk.

All employees 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 employees to take appropriate action and make well-informed decisions
- protect individuals or organisations affected by our decisions or actions

- enable an authorised person to examine the conduct of the department's business
- protect the financial, legal and other rights of the department along with everyone who works for the department
- preserve the history and heritage of NSW

Use of business systems

Digital records and paper files, created and received, must be captured and stored in Business Systems that are compliant with the State Archives and Records Authority's Standard on Records Management as per section Managing physical records of this policy.

Records must be captured into dedicated recordkeeping systems (EDRM Systems) when a Business System certified for recordkeeping is not available. Records are not to be kept alone in email folders, shared drives, personal work drives; Microsoft OneDrive, Microsoft Teams, or in any other uncertified location

Personal (or private) email, Google or Microsoft accounts (i.e. an account not issued by the department) must not be used for the purpose of transacting work-related business or storing work-related records and information. This requirement applies to any cloud-based services involving the use of a personal or private account (such as Dropbox, iCloud, Smartsheets, Facebook, Messenger and so on).

See Where should I store my digital records for more details

Design and review of business systems

Before issuing a tender for a new system, upgrading a system or moving to software-as-a-service (SaaS), specification requirements must consider the creation and capture of records of the business activity that the system controls.

Deletion of records in Business Systems, migration of records and decommissioning of Business Systems must be carried out in accordance with section Retention and disposal.

Records Management can provide advice on the use of Business Systems for recordkeeping. This includes advice on assessing systems against the State Archives and Records Authority of NSW's Standard on Records Management and certifying that Business Systems meet the requirements of this policy.

Digital recordkeeping

The principle of 'what is born digital stays digital' must underpin the record capture process.

Furthermore, the practice of capturing physical records must be re-designed to capture these as digital records for the purpose of increasing accessibility and efficiency in storage and retrieval and improving security. This principle aligns with the NSW Digital Government Strategy.

Managing physical records

Business areas continuing to capture and manage physical records must review their processes and consider how they can re-design those to instead capture records digitally.

Where they do exist, physical records must be:

1. stored in accordance with requirements within the Standard on the physical storage of State records
2. captured on an official physical file that has been registered in an official recordkeeping system (such as CM9)
3. updated in the recordkeeping system to reflect each change of location or assignee (so that this is always current)
4. 'sentenced' correctly against relevant records retention and disposal authorities (where Normal Administrative Practice (NAP) does not apply) before being transferred to off-site storage or being considered for disposal. Business unit owners are responsible for resourcing and managing any sentencing projects or activities and preparing records for transfer to off-site storage in accordance with any procedures or directions issued by the department's Records Management Team
5. transferred only to an off-site storage arrangement coordinated by the department's Records Management Team.

Retention and disposal

Disposal of records and information, in any format or held in any location, system or application, must be:

- undertaken in accordance with authorised disposal actions in relevant records retention and disposal authorities and supporting departmental procedures or directions
- approved by an authorised (delegated) employee in conjunction with the department's Records Management Team.
- Exceptions are for those records that may be:
- disposed of under the Normal Administrative Practice (NAP) provision of the State Records Act 1998 (NSW) and State Records Regulations 2015 (NSW); or where
- retention periods specified in legislation other than the State Records Act 1998 (NSW), that is specific to a function or activity, need to be satisfied.

Records that must be retained, even if the authorised disposal action in a relevant records retention and disposal authority has been satisfied, are those:

- reasonably likely to be required for a pending or anticipated investigation, inquiry or legal proceeding
- relating to an access request submitted under legislation or Order of Parliament.

In each situation, relevant records may only be considered for disposal if all action associated with the event or request, and any subsequent action or reviews arising, have been completed.

All system migration, and/or decommissioning of systems or applications, must ensure that authorised disposal actions are satisfied for any stored records. This includes a requirement to ensure records that have long-term value (something to be retained greater than 30 years but not permanently) or those of continuing value (something to be retained permanently as a State archive) are safeguarded, managed, protected and preserved in appropriate storage.

Records authorised for destruction must be destroyed by secure means.

Protection of, and access to records

General

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, information, and data based on an assessment of business risks and records management risks. See NSW Information, Classification, Labelling and Handling Guidelines
- capable of preventing the unauthorised access, removal, use, alteration, concealment, disclosure, or unlawful destruction or deletion of records, information, and data
- prevent the accidental damage or loss of records, information, and data.

When collecting, storing, accessing, maintaining, using or disclosing personal information about individuals, all employees:

- must have regard to the department's Privacy Management Plan, Information Protection Principles within the Privacy and Personal Information Protection Act 1998 (NSW) and Health Privacy Principles within the Health Records and Information Privacy Act 2002 (NSW)
- ensure anything of this nature is only shared with individuals authorised to access the record or information and who have a legitimate 'need-to-know'.

The NSW Information, Classification, Labelling and Handling Guidelines define sensitive and classified information, and specify requirements in relation to their labelling and handling. All employees must comply with requirements of this Guideline, along with any supporting departmental guidance, procedures or directions.

Unless authorised to do so by legislation, a departmental policy, directive, or procedure, employees must not use or disclose any records, information or data, that would not normally reasonably be expected to be made available for general public consumption, to any unauthorised individuals or organisations. Work-related records, information and data 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 the department
- involve the improper or unauthorised use or disclosure of records, information and data after separation from the department (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 privacy
- prejudice or undermine the effectiveness or integrity of any function, activity or process undertaken within the department, 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 departmental decision being made).

Working away from the workplace

Care must be taken when working away from the workplace, such as public places or at home. Each employee is responsible for protecting records, information and data in their possession and must:

- take reasonable measures to prevent any loss or damage, or unauthorised access to, or inappropriate disclosure of records, information and data
- ensure confidential, sensitive or personal information is not read or discussed openly in public places, and devices with any associated records, information and data are not left or placed where unauthorised individuals may be able to view any content
- ensure records, regardless of their nature, content or format, are not left unattended in public places (they must only be left with individuals authorised to access)
- ensure records (and any device/s that may contain work-related records, information and data) are locked when not in use, not left unattended in unsecured vehicles, or for extended periods of time (such as overnight).

Sharing within the department

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

Release of records and information

Members of the public

Access to the department's records, information and data by members of the public is governed by the Government Information (Public Access) Act 2009 (NSW)(GIPA), 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.

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 the department to be transparent and accessible to the public, and the need on the other hand to protect the integrity of the department's records and information. All employees must:

- have regard to requirements and responsibilities specified within the department's Code of Ethics and Conduct which encourages the disclosure of a broad range of information
- not disclose or handle records and information in any way which would undermine requirements within this policy or the Code of Ethics and Conduct.

Subpoenas or Legal Warrants

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

Standing Order 52

The Legislative Council can pass a motion under Standing Order 52 requiring the department to produce documents to the Council.

Arrangements with external parties

Contracts or agreements with external parties where the department has outsourced any function or activities, or with whom the department has entered into any service arrangements with (including cloud computing arrangements) must include records and information management provisions. These must ensure compliance with our legislative obligations relating to the management of our records and information and minimise risks associated with the external storage of records and information, and departments right to access information held by the contractors.

Risk assessment

Risk should be managed in accordance with relevant departmental risk and compliance policies and frameworks. All business areas are to conduct a risk assessment of records management in their business processes and the systems that manage them.

The senior NRO is responsible for overseeing the risk assessment and reporting risks in accordance with department policy and frameworks.

Continuous improvement and monitoring

The Records Compliance Team, within Digital Information Office, will undertake regular performance monitoring against the Records Management Policy.

Delegations

Destruction of records

A Group C (Director) role or above as defined by the department's financial delegations has authority to approve the destruction of records (where NAP does not apply) in conjunction with the department's Records Management Team and in accordance with:

- authorised disposal actions specified in a relevant records retention and disposal authority
- any related records retention and disposal guidelines, procedures or directions supporting this policy.

Where an appropriate Group C Director (or role above) cannot be identified, the Senior Responsible Officer for records management in the department (as identified within this policy) has authority to approve the destruction of records in accordance with authorised disposal actions in the relevant records retention and disposal authority.

Any entity that has adopted this policy, may choose to adopt the above delegations, or alternatively, specify their own.

Access directions

The Senior Responsible Officer, or their nominee, has authority for authorising access directions in relation to records open for public access after 30 years under provisions within the State Records Act 1998 (NSW).

Failure to comply with this policy

Reporting wrongdoing or improvement opportunities

The Speak Up hotline allows employees or members of the public to lodge reports about suspected fraud and other serious misconduct. If any employee suspects any serious misconduct in relation to the department's records, information, and data, they are encouraged to make a report. If preferred, reports can be made anonymously.

Other breaches of this policy, or other concerns or improvement suggestions relating to the management and handling of the department's records, information, and data can be reported by raising a ticket via your relevant service desk.

Responding to breaches

Behaviour that is contrary to requirements within this policy will be managed in a manner that is proportionate to the seriousness of the matter. This may involve a discussion with an employee to clarify requirements and responsibilities. More serious breaches may result in disciplinary action in accordance with relevant provisions (in particular Part 8) of the Government Sector Employment Act 2013 (NSW) and the Government Sector Employment Rules.

Review timeframe

The Records Compliance Team will review this policy no later than 3 years from the date the document is approved. The document may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary.

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	December 2020
Approver	Deputy Secretary Corporate Services
Group	Corporate Services
Division	Information, Spatial and Data
Policy owner	Chief Digital and Information Officer
Branch	Records Management
Document location	DPE Intranet and/or Internet
Next review date	December 2023
Associated procedure	
Any additional applicability	
Superseded document	Records Management Policy- SOPA Records Management Policy- DSFI Records Management Policy- FACS Records Management Policy- DPE Records Access Policy - OEH
Further information	records.management@dpie.nsw.gov.au
Document Reference	DOC20/1044166

Version control

Table 2. Version Control

Version	Date issued	Change
1	22 Feb 2020	New document Approval CM9 (Doc 21/101835)1
2	08 Dec 2021	Updated several, broken links in the document. (DOC20/1044166-Rev31)
2.1	3 May 2022	Updated to reflect new branding and name change.

Appendices

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Archives	Those records that are appraised as having continuing value. [AS 4390-1996- 1:4.5]
Data	Data are the building blocks ie. the raw words, numbers, etc. that are recorded, stored, and ready to process and from which information is derived.
Digital Records	A digital record is digital information, captured at a specific point in time that is kept as evidence of business activity. A digital record can be 'born' digital (such as an email message) or a scanned digital image of a paper source record.
Disposal	The destruction of records or their transfer to another organisation, for example, State Archives and Records Authority of NSW archives.
Disposition	A range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments. [AS ISO 15489.1:2017:3.8]. Within the department disposition is generally referred to as disposal, and disposition authorities are referred to as retention and disposal authorities.
EDRM System	An electronic document and records management system specifically designed to manage records in accordance with records management standards that includes the combined technologies of document management and records management systems as an integrated system. Examples include Content Manager (CM9 or TRIM), Objective.
Information	When data is processed and assembled, it becomes information that can be used or analysed. Information management is, in general terms, the discipline of managing information in its many forms. Information is a broader concept than records. It may include published or unpublished material, records, or raw data.

Term	Definition
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]
Physical records	Physical records include records in files, folders, paper documents, magnetic tape, optical disc, maps and plans.
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 below) Note that records include data assets
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 Archives and Records, Glossary of Recordkeeping Terms, available at http://www.records.nsw.gov.au/]
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 Archives and Records, Glossary of Recordkeeping Terms, http://www.records.nsw.gov.au/]
Records System	An information system which captures, manages and provides access to records over time. A records system can consist of technical elements such as software, which may be designed specifically for managing records or for some other business purpose, and non-technical elements including policy, procedures, people and other agents, and assigned responsibilities. [AS ISO 15489.1:2017: 3.16]

Term	Definition
Retention and Disposal Authority	Documents authorised by the Board of the State Archives and Records Authority of 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 Archives and Records, Glossary of Recordkeeping Terms, available at http://www.records.nsw.gov.au/]
Sensitive Information	Any information displaying the protective dissemination limiting markings (DLM's) of Sensitive: NSW Cabinet, Sensitive: NSW Government, Sensitive: Legal, Sensitive: Personal, Sensitive: Health Information, Sensitive: Law Enforcement, Sensitive, or that is assessed to warrant the application of that protective marking in accordance with the NSW Government Information Classification, Labelling and Handling Guidelines. For further guidance read the How to identify and label sensitive information guideline on the intranet.
Sentencing (sentenced)	Applying a disposal authorisation to a record.
State archive	A State record that NSW State Archives and Records has control of under the State Records Act [State Records Act 1998 (NSW) s3] and is part of the State Archives Collection
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) Note: State records are format neutral. They can be digital or physical hardcopy records.
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]

Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

Role	Responsibility
Secretary	The **Secretary** has overall responsibility for ensuring that the department complies with requirements of the *State Records Act 1998* (NSW) and its supporting regulations, as per the requirement within Section 10 of the Act. Where a related public service executive agency, statutory body or other entity within the cluster has chosen to adopt this policy, and they are considered a NSW public office for the purpose of the *State Records Act 1998* (NSW), this responsibility is assumed by the Chief Executive Officer with responsibility for that entity.
Senior Responsible Officer	The person occupying the role of Chief Digital and Information 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 NSW Standard on Records Management. The Senior Responsible Officer is also responsible for: • overseeing liaison with the NSW State Archives and Records Authority in relation to monitoring compliance against the *State Records Act 1998* (NSW) by the department; and • authorising secondary storage locations used by any business area for storing physical records (whether department owned or those of a service provider). Where a related public service executive agency, statutory body or other entity within the cluster has chosen to adopt this policy, and they are considered a NSW public office for the purpose of the *State Records Act 1998* (NSW), they must nominate the role within their entity that assumes this responsibility.

Role	Responsibility
Chief Information and Digital Officer	The **Chief Digital and Information Officer** is responsible for: • ensuring that information management system projects consider records management requirements when acquiring and implementing new systems or applications, or when decommissioning existing systems or applications; • ensuring appropriate infrastructure and support to ensure records kept in electronic form are managed so that they remain secure, accessible, readable, complete, inviolate, reliable and authentic for as long as they are required to be kept in accordance with disposal actions specified in current records retention and disposal authorities. This includes security measures applied to data backups and audit logs; and • 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 source records that have been migrated (GA48) have been met.
Nominated Responsible Officer	**Nominated Responsible Officers (NRO**) are senior managers with decision-making authority who are responsible for: • providing oversight and monitoring of records and information management within the division/business unit, including Records Management assessments • providing high-level direction and support (including ensuring adequate resourcing) for records and information management, including training for employee and contractors in use of Business Systems for recordkeeping • taking a risk-based approach to managing records and information, in accordance with relevant departmental risk and compliance policies and framework • overseeing information risk assessments and reporting information risks in accordance with department risk and compliance policies and frameworks. • seeking advice on records management from records and information specialists in division and business units and/or the Corporate Records Manager • allocating responsibility to business system owners to: — identify business processes and systems that contain, generate or use high-risk and high-value records and information — ensure records and information management is integrated into work processes, systems and services — ensure provisions for records capture and management are included in new system design and in contracts with service providers • approving local records business rules and procedures, ensuring they are consistent with this policy and meet organisational needs

Role	Responsibility
	• identifying business custodians of information sets, systems owners and operational data stewards • approving local records storage facilities in accordance with State Archives and • Records Authority's Standard on the Physical Storage of State Records.
Senior Executives	**Senior Executives** are responsible for: • fostering and promoting a culture of that promotes sound records and information management practices across their business area • providing high-level direction and support for records and information management • ensuring recordkeeping requirements have been considered within their business area, especially as part of new programs of work • including the requirement to meet recordkeepingresponsibilities in employee performance and development plans.
Business System Owners	All owners of any business system or application that stores records and information must: • fully understand the recordkeeping requirements and responsibilities relating to their system or application and associated business processes that they interact with ormanage • ensure that records are not disposed of without the correct disposal action from a relevant records retention and disposal authority being applied and documented • assess the system or application for appropriaterecordkeeping functionality when acquiring or building. This includes ensuring an appropriate risk assessment has been completed that considers risks associated with the storage of records and information in the system or environment being considered • re-assess recordkeeping functionality when a system undergoes major upgrades or changes in functionality • consider recordkeeping requirements when a system is to be replaced so that requirements continue to be met in the new system; • assess any system or application already in use, and which has not yet been assessed for recordkeeping functionality; and • in coordination with the CDIO ensure that the migration of digital records or digital control records/metadata is conducted in line with conditions specified in the General Retention and Disposal Authority for source records that have been migrated (GA48).
Records Team (EDRMS and Archiving)	The Records Team, or equivalent team or role responsible for similar functions or activities in any entity adopting this policy, is responsible for:

Role	Responsibility
	• managing the day-to-day technical operations of the department's electronic document and records management systems (EDRMS) • providing day-to-day EDRMS support and advice • managing EDRMS enhancements and developing associated strategy • managing archiving processes relating to both physical and electronic records • liaising with appropriate managers to authorise the disposal of records • coordinating and/or managing off-site storage arrangements for physical records.
Records Compliance Team	The Records Compliance Team, or equivalent team or role responsible for similar functions or activities in any entity adopting this policy, is responsible for: • providing advice in order to enhance the creation, storage, access and use of records and information • developing and maintaining records management and CM9 resources and training programmes • implementing the Records Management Policy and any supporting guidelines, procedures or directions • undertaking performance monitoring against requirements within this policy and any supporting guidance, procedures or directions. This also includes monitoring the identification of systems holding high risk and/or high value records and information, and that they are protected in business continuity strategies and plans • maintaining the department's Vital Records Register • ensuring overall records and information management risks are identified, managed and mitigated.
People Leaders	People leaders are responsible for: • developing ways to continuously improve records and information management performance by: — understanding what information is used in the business or program — integrating records and information management into work processes, systems and services, and establishing local business rules and procedures in accordance with this policy — ensuring records are created and captured in the course of business and are managed in accordance with this policy — ensuring assurance checks are periodically scheduled to ensure completeness and accuracy of records and information according to level of risk

Role	Responsibility
	• ensuring provisions for records capture and management are included in new system design and in contracts with service providers of outsourced functions • ensuring that employees and contractors comply with this policy and understand their records management responsibilities • assessing the level of risk to the business or program in managing information and taking a risk-based approach to mitigating identified issues in accordance with relevant departmental risk and compliance policies and frameworks • advising the senior NRO that records, and information management risks have been considered for new or existing programs and systems, or when: — developing a new process — moving to a new service environment, system, service or agreement — improving existing work processes, systems or services • ensuring that their business units and programs have an approved offsite storage account or local storage facility for the storage of physical records. • ensuring that the records of their business units and programs are regularly reviewed via the Records Management Self- Assessment tool • for destruction or archiving. This should be performed annually at a minimum. • Making records available for inspection by the CDIO or delegate.
Records and information specialists in divisions and business units	Where business units or divisions have a specific records or information specialist role, the records or information specialist for that division / business unit is responsible for: • providing advice on records management to the business system owners, business unit managers and program managers of that division or business and the senior NRO and divisional head when required • developing local recordkeeping business rules and procedures for that division or business in accordance with this policy and in consultation with divisional business units and programs • reviewing business processes and systems in the division to ensure appropriate records are captured • monitoring records and information performance • facilitating training for employees and contractors in recordkeeping responsibilities and certain Business Systems used for creating and capturing records • providing input into and assisting with Records Management Self-Assessment.
All Employees	All employees (including contingents or contractors) are required to: • understand the recordkeeping requirements and responsibilities specified within this policy and how they apply to their role;

Role	Responsibility
	• complete relevant introductory recordkeeping training that applies to them: — Former Industry – Recordkeeping Fundamentals and Handling Sensitive Information eLearning modules available at learning@industry. — Former Planning – An introduction to Recordkeeping — Former Property – Recordkeeping and you • routinely create full and accurate records of their work activities, including records of all substantive decisions and actions made in the course of their work, such as minutes of meetings and notes of telephone conversations; • ensure records are captured into the appropriate system so that they are accessible and appropriately secured; and • ensure records are disposed of in accordance with disposal actions in relevant records retention and disposal authorities, and after approved by those authorised to do so (where NAP does not apply).

Appendix 3 – Legislation and Standards

Legislation

- Crimes Act 1900 (NSW)
- Electronic Transactions Act 2000 (NSW)
- Evidence Act 1995 (NSW)
- Government Information (Public Access) Act 2009 (NSW) (GIPA)
- Government Sector Employment Act 2013 (NSW)
- Health Records and Information Privacy Act 2002 (NSW) (HRIP)
- Independent Commission Against Corruption Act 1998 (NSW)
- Limitations Act 1969 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW) (PIPPA)
- Public Finance and Audit Act 1983 (NSW)
- Public Interest Disclosure Act 1994 (NSW)
- State Records Act 1998 (NSW)
- State Records Regulations 2015 (NSW)

Standards

- Australian Standard AS 4390-1996, Records Management [though superseded by AS ISO 15489, contains definitions that are still relevant].
- Australian Standard AS ISO 15489.1:2017, Information and documentation – Records Management. AS ISO 15489.1:2017 has been issued as a **Code of Best Practice** for records management by NSW State Records. [Australian and international standards are available online via the Australian and International Standards page on the department's Records and Information Management intranet pages].
- *Standard on Records Management* for the NSW Public Sector (NSW State Archives and Records, Issued March 2015)
- *Standard on the Physical Storage of State records* (NSW State Archives and Records, 2012)

Useful resources

- Records and Information Management pages available on the department's intranet.
- NSW State Archives and Records "Government Recordkeeping Resources" available at http://www.records.nsw.gov.au/recordkeeping
- NSW Government Information Classification, Labelling and Handling Guidelines (NSW Department of Finance, July 2015)

- NSW Ombudsman's Good Conduct and Administrative Practice Guidelines for state and local government (March 2017)
- NSW Public Sector Commission, Behaving Ethically: a guide for NSW public sector employees
- NSW Government Digital Strategy
- NSW Government Cyber Security Policy
- NSW Government Cloud Policy