information and privacy commission
new south wales

IPC Records Management Policy

October 2022

Contents

1. Purpose

The records management program for the Information and Privacy Commission (IPC) has been established in accordance with section 12(2) of the *State Records Act 1998* (SR Act). This policy outlines the roles, responsibilities and operations of the program.

2. Objectives

The objectives of this Policy are:

- ensure that records of all activities and decisions within the IPC are created, captured, managed and retained in the EDRM system
- ensure the efficient and effective management of the records is in support of business objectives
- clarify records management responsibilities within IPC.

3. Records Management Principles

The IPC has adopted the following principles for its records management program:

- Records are a vital asset for information accessibility, which underpin government transparency and trust
- Good records management, enhances the provision of services and operations by supporting program delivery, management and administration
- Full and accurate records enable the delivery of services in an efficient and equitable manner and provide evidence of actions and decisions, thus providing precedents for future decision-making
- As a vital asset, records protect the rights and interests of Government, the IPC, its customers and New South Wales (NSW) citizens
- Records management including retention and disposal authorities, must reflect the categories/classifications of records kept by the IPC and reflect legislated requirements of both the SR Act and any other relevant legislation e.g., the *Government Information (Public Access) Act 2009*
- The application of records management enables the effective control of, access to, and security of IPC records
- When a business function changes, the new function retains stewardship of the record assets that were created before the change
- This policy provides a means for the authorised destruction or transfer of records that are no longer in use
- Over time a portion of IPC records will become State archives, contributing to the cultural resources of NSW.

4. Authorising Environment

The IPC relies on the Department of Customer Service (DCS) for the provision of IT infrastructure and network services including access to IPC's EDRM system. However, as a client of these services and in the context of the IPC as a separate agency with its overarching records management responsibilities, IPC staff will demonstrate subject matter expertise and actively engage with DCS in relation to systems issues. IPC staff will liaise with DCS EDRMS System Administrators to fulfill its record management responsibilities with relation to user access controls, reporting and retention and disposal of records.

The IPC's record holdings include information access and privacy records relating to advice, codes of practice, directions and guidelines, complaints, education, monitoring and reviews as well as general administrative records.

The IPC manages its record holdings in accordance with the following Retention and Disposal Authorities made pursuant to the SR Act:

- Functional Retention and Disposal Authority (FA 406) – Approved November 2019, to be Reviewed: December 2024. (D20/015593/DJ)
- General Retention and Disposal Authority: administrative records (GA 28) – Revised 2021.

5. Roles and Responsibilities

Each of the following roles has specific assigned responsibilities under this policy:

Role	Responsibilities
All staff, contractors and consultants	• Create and capture records of their work in accordance with this policy and IPC procedures. This includes making records of work where records are not automatically created. • Understand conventions applied for creation of containers and their delegations/authorisations in respect of records access • Capture records electronically into TRIM • Describe and classify records in accordance with IPC procedures • Store and handle records with care in accordance with IPC policy and procedures • Protect sensitive records from unauthorised access • Release information to those authorised to have access and ensure that those authorised have access to the information they need to meet business needs • Ensure that contractors and consultants act responsibly and in accordance with IPC retension and disposal authorities including ensuring that records created while doing their work for the IPC remain the property of IPC.

Managers	• Develop ways to continuously improve records and information management performance by:
	  ○ integrating records and information management into work processes, systems and services
	  ○ 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
	• Ensure provisions for records capture and management are included in new system design and in contracts with service providers of outsourced functions. See design and review of Business Systems for additional requirements
	• Ensure that staff and contractors comply with this policy.

Senior Responsible Officer*	• Provide oversight and monitor records and information management including developing a policy and governance framework, in collaboration with stakeholders • Provide high-level direction and support (including ensuring adequate resourcing) for records and information management, including training for staff and contractors in use of Business Systems for recordkeeping • Regularly review use of recordkeeping systems • Take a risk-based approach to managing records and information • Identify when the IPC will require new authorities or review of existing authorities • Coordinate responses to mandatory reporting requirements to NSW State Records • Ensure user controls, reports on record holdings and retention and disposal authorities are operational • Apply IPC destruction rules when authorising the destruction of records (see Destruction of records). • 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 • Approve local records business rules and procedures, ensuring they are consistent with this policy and meet organisational needs • approve records storage facilities in accordance with the State Archives and Records Authority of NSW (NSW State Archives and Records) Standard on the Physical Storage of State Records • Reporting to SARA on issues of noncompliance in consultation with the CEO • Escalate to the CEO any issues on non compliance and any issues relevant to the outsourced model of records management by DCS which compromise the IPC's compliance with records management requirements.
Chief Executive Officer	• Responsible for compliance with the SR Act and other records legislation • Ultimately responsible for records and information management in accordance with business requirements and relevant legislation • Responsible for authorising a Senior Responsible Officer.

* The Senior Responsible Officer for records management at the IPC is the Manager Systems and Corporate Services.

6. Records capture and description

Records of all activities and decisions within the IPC must be captured into the EDRM System or other business systems certified for recordkeeping. All records captured are to be described and classified in accordance with the IPC business classification system. IPC's Records Procedures provides guidance to staff on the capture and classification of records.

Classification of records is undertaken in accordance with the State Archive and Record's Keyword AAA, a keyword thesaurus covering terminology common to most NSW Government organisations and common functions and activities. Systems and Corporate Services staff are responsible for managing, providing advice and implementation of the classification of records in the EDRM System.

7. Information Security and Privacy requirements

Information about individuals must also be managed in accordance with IPC's Privacy Management Plan and the Information Protection and the Health Privacy Principles. These define how the IPC will manage the collection, storage, access, accuracy, use and disclosure of personal information in accordance with the:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*

With reference to the above, records security must be implemented to ensure that information is accessible only to those authorised to have access, and that those authorised have access to the information they need to meet business needs.

8. Access to Records

Access to records registered in the EDRM System is determined by user access controls set by the IPC. The IPC's Records Management Procedures outlines the categories of user controls applicable to staff. These user access controls determine what access to records are granted to IPC staff. As the IPC relies on DCS to provide System Administration of its EDRM system, DCS System Administrators have access to IPC's records in order to apply the Retention and Disposal Authorities and create destruction requests in accordance with these authorities. The IPC is able to acquire audit logs to ensure appropriate access and disposal by DCS.

Hard copy records are stored at external storage facilities and can only be accessed by a request to the IPC Systems and Corporate Services Team. Authorisations to the EDRMS system are documented in the Record's Management Procedures. However, the IPC adopts a hierarchal 'need to know' approach to ensure records security.

9. Storage of records

Records created or received in a digital format must be managed digitally, minimising the need to create and store physical records, in accordance with the requirements in the section Records capture and description.

Physical records, when no longer in active use, will be transferred to a pre-approved external storage facility and managed in accordance with this policy and IPC procedures in order to:

- minimise storage and retrieval costs
- ensure external storage facilities are of an acceptable standard to protect records
- dispose of records in accordance with the requirements in the following section Destruction of records.

Records should only be sent to external storage if they have been sentenced.

10. Destruction of records

Systems and Corporate Services staff will undertake an annual review of hard copy and digital record holdings to determine if any records need to be archived, destroyed or sent to State Archives. Retention and disposal of records is undertaken in accordance with the IPC retention and disposal authorities. Future authorities will be subject to consultation with DCS prior to submission to SARA for approval.

Destruction of records includes, for example, shredding or pulping of physical records and the deletion of digital records. In all cases, the following destruction rules must be followed:

- Records must not be destroyed if they are required for ongoing business needs or subject to current or pending audit, legal action or any other information access requests.
- Physical and digital records designated as State archives must be transferred to the NSW State Archives and Records.
- Records destruction must be authorised by the Senior Responsible Officer. The destruction process must:
    a. involve secure destruction relevant to the sensitivity of the records (secure destruction bins are kept within the utilities room in the IPC office)
    b. be carried out in a secure environment when destroying physical records
    c. have evidence of the destruction kept as a record including a description of what was destroyed, who authorised destruction, date of approval for destruction, the retention and disposal authority class the destruction was carried out under and when the destruction was carried out
    d. have evidence of the destruction by way of a certificate of destruction when destruction is carried out by a service provider.

11. System migration and decommissioning

Digital records in systems designated for migration or de-commissioning, must be retained in accordance with the appropriate records retention and disposal authorities and taking into account the protection of records required for long term or archival retention.

Migration of digital records to new systems is acceptable where the new system meets the requirements of digital recordkeeping and has been approved by the Chief Executive Officer.

12. Risk assessment

Risk must be managed in accordance with IPC Enterprise Risk Management Framework. The Manager Systems and Corporate Services is responsible for overseeing the risk assessment and reporting risks related to IPC's records management responsibilities and the EDRM System All risks are to be reported to the Director Business Improvement for consideration for inclusion in IPC's Risk Register.

13. Definitions

Term	Definition
Business Systems	Automated systems that create, process and manage data to support business processes.
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, e.g., NSW State Archives and Records archives.
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 HP Content Manager, TRIM.
Information security	The preservation of the confidentiality, integrity and availability of information.
Physical records	Physical records include records in files, folders, paper documents, magnetic tape, optical disc, maps, and plans.
Records	Any source of information created, received, and maintained as evidence of the transaction of business. Examples include email approvals, outward correspondence, financial transactions in SAP. This information can be structured in Business Systems or can reside in unstructured repositories.
Retention and Disposal Authority	A retention and disposal authority is a formal instrument approved by the Board of the State Archives and Records Authority of New South Wales, that identifies the records which an organisation creates and maintains, and for how long they should be kept to meet regulatory, business and community requirements.
Sentencing	Applying a disposal authorisation to a record.

14. References

State Records Act 1998

State Records Regulation 2015

Government Information (Public Access) Act 2009

Privacy and Personal Information Protection Act 1998

Health Records and Information Privacy Act 2002

IPC Records Management Procedures

Guidelines on Collaboration Tools and Recordkeeping

Document Information

Identifier / Title:	IPC Records Management Policy
Business Unit:	Systems and Corporate Services
Author:	Director Business Improvement
Owner:	Director Business Improvement
Approver:	Chief Executive Officer
Date of Effect:	October 2022
Next Review Date:	October 2024
EDRMS File Reference:	D21/044592/DJ
Key Words:	Records Management Program, Records Capture, Classification, Roles and Responsibilities, Access to Records, Retention and Disposal

Document History

Version	Date	Reason for Amendment
1.0	October 2022	First publication