NSW Police Force

# Records and Information Management policy statement

## 1. INTRODUCTION

Under the State Records Act, 1998, all public offices are required to establish and maintain a records and information management program that conforms to the standards and codes of best practice approved by the State Records Authority of New South Wales.

The Australian Standard AS ISO 15489 Records Management has been adopted as a code of best practice for the management of records by the NSW Public Sector.

The legislation and standard applies to both physical and electronic records and requires the New South Wales Police Force (NSWPF) to document business transactions fully and accurately in a compliant recordkeeping system.

## 2. AUTHORITY OF THIS POLICY

This policy is issued as corporate policy under the authority of the Commissioner's Executive Team (CET) and will be reviewed and amended as required, in consultation with business unit managers, local area managers and other members of staff.

Ownership of this policy rests with the Manager, Process and Records Services.

## 3. COMPLIANCE WITH THIS POLICY

Under Section 10 of the *State Records Act 1998*, the Commissioner has a duty to ensure that the NSWPF complies with the requirements of this Act and any associated regulations. Therefore all staff, consultants, contractors and volunteers must comply with this policy, and the procedures issued in accordance with it.

This policy applies to records of work done by, or on behalf of, the NSWPF, and therefore it applies to sworn and unsworn officers of the NSWPF, consultants, contractors and volunteers.

## 4. PURPOSE OF THIS POLICY

The purpose of this policy is to define and specify records and information management principles that all staff must comply with to ensure that NSWPF effectively fulfils its obligations and statutory requirements. This policy applies to all personnel who create records, across all NSWPF locations.

The aim of this policy is to ensure that:

- Principles and procedures of good records and information management are consistent across all commands and units of the NSWPF.
- Records are created and maintained as an integral component of, and support to, NSWPF business processes.
- Accepted standards of accountability are maintained.
- Guidelines on security, privacy and disposal of records are observed.

Records are essential parts of the NSWPF's information resources and corporate memory. They are an asset crucial in meeting business, accountability and audit requirements, and like any asset, they need to be managed efficiently and effectively. The creation, transmission, maintenance, use and retention/disposal of records must be in accordance with this policy.

## 5. SCOPE OF THIS POLICY

This scope of this policy covers:

- All administrative, functional and investigative information and the records they form, as created and managed by the NSWPF to ensure that they are protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.

- All information managed within the corporate recordkeeping system, RMS, or other NSWPF corporate information management systems, covering all operating environments, including diverse system environments and physical locations.

- All records and information managed and maintained on behalf of the NSWPF, in all outsourced, cloud and similar service arrangements, plus systems that hold high-risk and/or high value records.

## 6. RECORDS AND INFORMATION MANAGEMENT PROGRAM

The records and information management program is a planned, coordinated set of policies, procedures and activities that are required to manage NSWPF's records.

The objectives of this program are that:

1. NSWPF has the records it needs to support ongoing business activities and customer services, meet accountability requirements and community expectations.

2. These records are managed efficiently and effectively.

3. These records can be readily retrieved when required.

4. Records relating to critical NSWPF activities are preserved for historical and research reasons.

Section 12(2) of the *State Records Act 1998* requires the following principles be implemented for establishing and maintaining a records and information management program:

**The program is directed by policy**

- Records management is directed by policy adopted at the corporate level.
- Policy statements direct that records are made, captured, maintained and disposed of in accordance with the legal, regulatory and business needs of the public office.
- Policy defines the responsibilities of all personnel who manage records and information.

**The program is planned**

- Long and short term records management goals are identified and documented in the planning mechanisms of the public office.
- Adequate resources are allocated to achieve long and short term records management goals.

**The program is staffed with skilled people**

- Overall responsibility for the records management program is assigned to a Nominated Senior Officer.
- Specialist records management skills required to implement the records management program and its component recordkeeping systems are available to the organisation.
- Staff undertaking records management have appropriate skills for their positions and responsibilities and these are kept up to date.

**The program is implemented**

- Records are made, captured and maintained in official recordkeeping systems in accordance with legal, regulatory and business needs.
- Business systems meet identified requirements for making and maintaining records.

- Current retention and disposal authorisation is in place for all records, regardless of format, of the public office.
- Records are disposed of in accordance with authorised retention and disposal authorities and appropriate processes.
- Staff are trained in recordkeeping practices and procedures, and training is appropriate to their positions.
- Staff use official recordkeeping systems and services and have access to appropriate advice.

**The program is monitored and reviewed**

- All aspects of the records management program are regularly reviewed against performance objectives.
- Opportunities are identified for improving the effectiveness, efficiency and quality of records management systems, processes and tools through regular monitoring and review.
- Areas for improvement are addressed in records management planning.

## 7. RECORDKEEPING RESPONSIBILITIES

The State Records Act requires all public officials to 'make and keep full and accurate records' of their business activities.

The NSW Public Sector Code of Conduct requires all public officials to maintain adequate documentation to support any decisions made of their business activities.

The Ombudsman's Good Conduct and Administrative Practice Guideline 2006 – 2nd Edition for Public Authorities states that public official must make and create records to support accountability and corporate memory.

Under Parts 2 – 8 of the State Records Act, 1998, the Commissioner is responsible for ensuring that the NSWPF complies with the regulations and requirements of the Act.

The Process and Records Services Unit develops, and has overall responsibility for the NSWPF records and information management program covering policies, procedures, training and advice, records classification and disposal tools, management of RMS - the corporate records management system, management of corporate archives including provision of reference and access services, records storage and life-cycle management solutions, and quality assurance of records.

All records captured and maintained at the local level must comply with the procedures for, and concepts of, records management, as outlined in this and other Records Services' policies and procedures.

## 8. THE IMPORTANCE OF RECORDKEEPING

A record is defined as:

"Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business" (Source: ISO 15489 - International Standard on Records Management).

All records created by NSWPF personnel in the course of their duties are considered public records of the NSW Government. The NSWPF therefore has an obligation to the people of New South Wales to ensure that the principles of records management are implemented. This ensures that:

1. Business communications and decisions are captured as official records.
2. The evidentiary chain is kept intact.
3. Information is available for ongoing business purposes.
4. Storage costs are minimised through accountable records disposal.
5. An historical record of the NSWPF is maintained.

Under the NSWPF Code of Conduct, all NSWPF personnel are required to "make sure confidential information cannot be accessed by unauthorised people and sensitive information is released only to people inside and outside of the NSWPF who have a lawful access need".

Records generated by NSWPF document the organisation's past activities and may be required for internal and external investigations, litigation, and public access reasons. It is therefore essential that records are properly created and can be retrieved when needed.

## 9. DIGITAL INFORMATION AND RECORDKEEPING

Activities and business transacted electronically must be managed in accordance with this policy. The medium of the record is immaterial to how it is managed; the critical factor is the subject matter and its content, rather than the format.

The preferred method for managing information within NSWPF is to capture, distribute and dispose of records in electronic format throughout their life-cycle. This is the most efficient and cost-effective method of managing information and NSWPF is moving to minimise the creation of hardcopy records as a corporate priority.

Electronic records fall into two main categories – unstructured documents saved to network drives and emails, and information held in databases.

Unstructured information, such as documents and emails, that are evidence of business transactions must be registered in RMS and attached electronically to an appropriate file also registered in the corporate recordkeeping system RMS.

Digitisation processes must ensure that the images created are full and accurate and that they are also:

- Authentic - i.e. the product of routine, authorised digitisation and registration processes.
- Complete - i.e. an accurate, legible reproduction of the original, without substantive changes or deletions of content.
- Accessible – i.e. available and readable to all with a right to access them for as long as required.

Digital images also need to be stored, backed up and managed effectively for as long they are as required. When digital images replace original paper records as evidence of business, it is particularly important to store master versions in a way that promotes and ensures their security and longevity.

Images stored in a digital recordkeeping system must comply with the following requirements:

- Secure – i.e. unable to be altered or tampered with or accessed by unauthorised users. Digital images must remain accurate and reliable reproductions of the original paper records that were created or received, so that they can be trusted as reliable evidence. Unauthorised attempts to access them must be able to be detected by the system and images and their associated metadata must also be backed up and protected from disaster.
- Accessible – i.e. stored in a way that allows anyone with sufficient access privileges to access and view the digital images and their metadata.
- In context with related records – i.e. related to other records thate document the same business processes. Digital images will also inherit the metadata and classifications associated with the business process they document or relate to.
- Able to be managed long term (when required) – i.e. protected, accessible and useable for as long as required, as defined by existing retention and disposal authorities.

If a digital image is linked to a business system, the system should have recordkeeping functionality or be integrated with RMS. This will enable the image to comply with the requirements detailed above and inherit metadata associated with the business processes it forms part of.

Removable media must not be used to store State Records as they are subject to a number of risks including being easily damaged, stolen or lost. Additionally they are not backed up as part of a regular backup cycle.

When using a NSWPF mobile device, NSWPF information should only be transmitted via email and should not be transmitted via SMS or MMS including between NSWPF mobile devices, as these communication methods do not comply with this policy.

The Manager, Process and Records Services should be consulted whenever new databases and automated systems are being implemented, to determine the recordkeeping requirements and ensure compliance with legislative requirements

**General Authority 45 (GA45) – Original or source records that have been copied**

GA45 provides the authority to the NSWPF to securely dispose of hard-copy records and digital records that have been registered and attached to the NSWPF Records Management System (RMS), subject to meeting the specified criteria in section 1.4 of GA45.

It is recommended that any hard-copy or digital record added to RMS as an electronic record is securely destroyed at the first available opportunity, once the digital records has been checked and verified.

## 10. SECURITY OF RECORDS AND INFORMATION

### 10.1. Security Classification of Information

To ensure the protection of corporate information produced and managed by NSWPF, security classifications based on national standards have been developed and implemented. Details of the various security levels and associated Dissemination Limiting Markers (DLMs) used by NSWPF and guidelines on managing information classified in terms of these security levels, are available on the Classification and Security Classifications Intranet page.

### 10.2. Circulation and Tracking of Records

All official records of the NSWPF must be accessible at any point in time, subject to appropriate access and security controls being in place.

The electronic management of records registered within RMS provides a secure and auditable method of tracking and circulating information, whilst minimising the risk of their loss.

Electronic records registered in RMS are immediately available subject to any access restrictions placed upon them.

Managing records in hardcopy format is subject to the receipt and actioning of the record, with subsequent delays imposed by the delivery of mail, increasing the risk of the record becoming lost. The records can also only be actioned on an individual basis.

### 10.3. Confidentiality of records

NSWPF personnel must take particular care to ensure that any information that relates to sensitive reports, investigations, or other protected matters, is appropriately classified and managed in terms of the information security classification.

### 10.4. Security of Records

All members of the NSWPF have a statutory obligation to ensure that any official record that comes into their possession or that they have access to is used only by authorised personnel for official purposes.

NSWPF personnel must make themselves familiar with provisions regarding the secrecy and confidentiality of police business as outlined in Part 4, Clause 75 of the Police Regulation 2008.

Users of RMS have been assigned appropriate levels of security clearance that restrict the information that they can access on a need-to-know basis.

### 10.5. Access to Records

Records must be available to all authorised staff that require access to them for business purposes. Reasons for restricting access must be justifiable.

Members of the public are entitled to access to records of the NSWPF, subject only to the exemptions and exceptions provided for in the *Government Information (Public Access) Act 2009*.

There are other legislative instruments which allow other agencies or members of the public to access to records held by the NSWPF. NSWPF will assess and make a decision to grant or refuse all requests for access to its records which are properly lodged in accordance with the relevant governing legislation.

### 10.6. Safe Handling

Only records secured as 'Secret' require safe handling. For information on the management, handling and transmission of Secret information within the NSWPF please refer to Appendix 1 of the NSWPF Information Classification, Protective Marking and Handling Guidelines.

## 11. DESTRUCTION OF RECORDS

The destruction of NSWPF records, whether in hard-copy or electronic format, is regulated by section 21 of the *State Records Act 1998*. Functional Disposal Authorities are approved by the NSW State Records Authority and specify set retention periods and disposal actions relating to records specific to NSWPF. NSWPF records must be sentenced in accordance with an approved disposal authorities; advice and guidance on the use of the Disposal Authorities used within the NSWPF can be found on the Records Services' intranet site.

Commands and Business units that create records are the Owners of the records and as such have responsibility for ensuring that records are appropriately sentenced with an approved Disposal Authority. The ownership of any record is maintained even after records have been transferred to the custody of Records Services.

The Director, Shared Services has delegation to approve the destruction of all records in the custody of Records Services. However, prior to any records being destroyed, commands and business units will be given 4 weeks to reply and request an extension to the retention period for any records that they are responsible for.

Extensions will only be approved if one, or more, of the following conditions are met:

1. The records are required for current or pending legal action.
2. The records may be required as evidence in a court case.
3. The records are the subject of a current or pending access request or application, such as under the Government Information (Public Access) Act (GIPA) or a privacy request.
4. The records are subject of any other statutory access request.
5. The records relate to an unsolved serious crime.

Records that don't provide evidence of a business transaction or a decision can be destroyed without specific reference to a disposal authority, under Normal Administrative Practice (NAP). The destruction of records under NAP is intended to have a narrow use, with most records having to be disposed of in accordance with approved disposal authorities. Under NAP, drafts, working papers, duplicates, computer support records, facilitating instructions and stationery can be destroyed without the need to refer to disposal authorities.

When digital images are managed as records, their disposal must also be authorised. They must be retained for the same retention period that the original paper records were subject to.

Records must not be destroyed if they are subject to a disposal freeze or an embargo.

For audit and reference purposes, the NSWPF Manager, Corporate Records & Logistics should be informed when any official records are destroyed. The advice of the NSWPF Manager, Corporate Records & Logistics should be sought if there is any doubt as to whether records should be destroyed.

## 12. STORAGE & TRANSFER OF INFORMATION AND RECORDS

Active hardcopy records should be stored locally by Commands and Business Units for a minimum of 2 years or until such time as they are no longer frequently accessed. Records held by Commands and Business Units must be appropriately secured.

Inactive records can be transferred into the custody of Corporate Records & Logistics in accordance with established transfer protocols.

For advice and guidance on transferring records, please refer to the Transfers, Storage and Disposal Procedures section of the Records Intranet Site.

Records identified as a State Archive, as detailed in disposal authorities, will be transferred to the State Records Authority of NSW by Corporate Records & Logistics.

## Appendix A – Relevant legislation, standards, procedures and disposal authorities

**Legislation**

- State Records Act, 1998
- Government Information (Public Access) Act, 2009
- Privacy and Protection of Personal Information Act, 1998

**Standards**

AS ISO 15489 (International Standard on Records Management)
Government Recordkeeping Manual, 1999 – prepared by State Records Authority of NSW. Includes the following standards:

- Standard on the physical storage of State records
- Standard on records management

**Disposal Authorities**:

- DA220 – NSW Police Force Functional Retention and Disposal Authority
- DA221 – NSW Police Force Investigation Case File Disposal Authority
- GA28 – General Retention & Disposal Authority
- GA45 – Original or source records that have been copied
- State Records Guideline No 8 – Normal Administrative Practice

**Procedural Guides**

- Records Services Intranet site – Policies and Procedures
- Information Security Classification