Information Management: Business Unit Information and Records Management Procedures - PNHQ and RNZPC

Table of Contents

All Police employees, contractors and volunteers are information and record stewards. For information and records management at PNHQ and RNZPC this means employees are responsible for ensuring their business-related records are created, maintained and stored so as to be accessible within the business unit and elsewhere, as authorised.

The Police Information Management Policy outlines the records and information management responsibilities for all employees.

At an individual level we may understand our responsibilities for creating, managing, preserving and storing information, but in order to meet all our business and legislative obligations, we also need to recognise how business units operate to support Police-wide information management.

Following these best practice protocols, you and your business unit will contribute to ensuring Police are compliant with our legislative responsibilities.

Person/s responsible for certain information and records management tasks in each business unit

Every individual employee is accountable for creating, maintaining and storing their records, whether physical or digital. Each business unit at PNHQ and RNZPC must also ensure that a person or persons within each unit is responsible for the tasks identified in this document in relation to the management of the unit's digital and physical information and records.

These tasks apply to:

- all physical and digital information and records created and received by PNHQ or RNZPC including all files existing in the PNHQ or RNZPC records systems,
- all Police employees, contractors and volunteers based at PNHQ or RNZPC.

Managing digital information and records in Shared Drives

Classifying and organising records is crucial for effective digital information and records management.

It is important that each business unit actively maintains and manages its part of the shared drive. The shared drive should reflect the business unit's functions and the tasks and activities the business unit carries out to meet their functions.

Folder structure and content

This includes applying:

- **Access controls -** Information should be accessible to those who need access to it and appropriately secured when required.
- **Folder structure controls -** The upper levels of the business unit's folder structure should be controlled to ensure changes do not occur at this functional level (usually a business unit's top 2 folder levels).
- **Folder level controls -** Creating too many layers of folder levels is not advisable. In addition to inhibiting discovery, shared drives only permit a limited number of characters when naming folders - creating too many layers will impede naming.
- **Metadata -** Ensure enough valuable and informative metadata is created for ongoing discoverability and re-use of the information.
- **Naming conventions -** Use consistent naming conventions understood by all.

Naming conventions

Consistency in record and document naming assists in the efficient retrieval of information. Effective naming can decrease the time spent searching for information and increase the number of relevant search results generated.

- Use a name that clearly describes the record and is helpful to others without further context.
- As shared drives do not have unique identifiers Police use a combination of the name, date and file path, as its identifier.

Version control for documents

Use the following guide for recording document versions.

Draft/Final	Description	File Name
Minor draft	Minor changes	Report v0.2 DRAFT, v2.3 DRAFT
Major draft	Draft distributed for comment internally or externally	Report v2.0 DRAFT
Final	Final authoritative version	Report FINAL

Managing digital information and records in other operational and business systems

In addition to shared drives, many business units manage information and records within core business applications and systems. In these systems, digital content should be managed in accordance with that application's individual characteristics and protocols and capture metadata per the metadata requirements noted below. Access controls should also be applied as required. Care should be taken to ensure that whatever system is being used, it is also the allocated system for final documentation.

Managing physical information and records in business units

The vast majority of our information and records are created digitally - while historical volumes of physical information and records are reducing, the processes relating to the management of physical information and records focus on storage, retrieval and disposal.

Each business unit proactively manages their on-site storage and refers boxes for off-site storage toPNHQ File Management staff (Ground floor, 180 Molesworth Street) to arrange transfer to the Police's off-site storage provider. Referral to File Management staff includes:

- a complete list of all contents emailed to this address; and
- a physical list of the contents of each box, included with the box contents.

For more details on management of physical information and records see 'Storage and retrieval of physical files'.

Physical records management support for business units

Records management support for business units in PNHQ and RNZPC is provided by File Management staff. In addition to the provision of general recordkeeping advice, they:

- provide business units with a content listing template and guidance on its completion
- apply box barcodes and a review date for each box and arrange transfer to off-site storage
- confirm with the business unit, the specific disposal authority classes applicable for each box before sending material to off-site storage
- arrange retrieval of records in off-site storage
- work with business units to ensure physical files are not retained in off-site storage beyond their retention period.

Contact

To obtain advice about day-to-day recordkeeping, contact PNHQ File Management staff at this email address.

Capturing metadata

Records management metadata is information about the context, content and structure of records and their management through time. Assigning metadata to records enables the creation and maintenance of trustworthy evidence of business activity. It also aids in locating the information and provides an auditable trail of actions that have occurred over the records.

Business owners of systems are responsible for ensuring that complete metadata is captured.

The intranet page Metadata provides in-depth, comprehensive information, guidance and further resources for creating and using metadata to more efficiently manage information and records.

Ceasing employment with Police

When ceasing employment with Police, employees are required to:

- save their material in the appropriate operational and business systems in accessible formats,
- provide their manager with the passwords if using password protection on any documentation.

For further information management best practice, guidance and support, please view the Information Management intranet pages on Ten One.