



## POLICY P5.1.6 RECORDS MANAGEMENT

ITEM	DESCRIPTION
Version Number	3.0
SOPs	<ul style="list-style-type: none"><li>➤ SOP P5.1.6-1 Creation and Capture of Records</li><li>➤ SOP P5.1.6-2 Security and Access to Records</li><li>➤ SOP P5.1.6-3 Maintenance and Storage of Records</li><li>➤ SOP P5.1.6-4 Disposal of Physical Records</li><li>➤ SOP P5.1.6-5 Management of Corporate Correspondence</li></ul>
Policy Owner	Executive Director, Executive Services
Policy Contact	Director, Program, Audit & Inquiries
Approved Date	2 December 2016
Effective Date	5 December 2016
Next Review	2 December 2019
Document Control	Electronic - Printed Copies are Uncontrolled

### 1 Purpose

- 1.1 The NSW Government requires that the business of the NSW Public Sector is properly documented and that official records are managed efficiently and effectively to support service delivery, good governance and accountability.
- 1.2 In accordance with the *State Records Act 1998*, the NSW Rural Fire Service (NSW RFS) is committed to adopting and implementing standards and codes of best practice to improve the management of its records and recordkeeping systems so as to protect the interests of the NSW RFS, the rights of its employees and stakeholders.
- 1.3 This policy promotes best practice records management and quality recordkeeping and provides guidance on the management of records, including physical and digital records of all formats so as to provide:
  - a. Evidence of compliance with legislative requirements;
  - b. Improved support for business activities;
  - c. A means for accountability to all NSW Rural Fire Service members and external stakeholders;
  - d. Access to and preservation of information; and
  - e. Guidelines for the receipt, registration and dispatch of mail and other articles.

### 2 Definitions

- 2.1 For the purpose of this Policy Document the following definitions apply:
  - a. **Appraisal:** the process of evaluating business activities to determine which records need to be captured and how long records need to be kept.
  - b. **Designated officer:** the NSW RFS staff member responsible for records management in a District or Regional office, or business unit.

- c. **Disposal:** a range of processes including retention, destruction of records from recordkeeping systems; migration of records between recordkeeping systems, and the transfer of custody of records.
- d. **Disposal Authority:** a schedule issued by the State Records Authority for use by the NSW RFS that identifies the business activities and transactions of the organisation and provides the authority for the disposal of records.
- e. **Dissemination Limiting Markers (DLMs):** Information that does not meet the criteria for security classification but which requires some lower level of protection can be labelled with a dissemination limiting marker (DLM).
- f. **Document (digital & physical):** any source of information of a stand-alone nature including text, images and scanned documents.
- g. **EDRMS:** Electronic Document and Records Management System (currently HP Records Manager).
- h. **Folder:** a cardboard cover or electronic container used to group and store associated documents
- i. **Normal Administrative Practice (NAP):** routine disposal of records that have short term value or are of a facilitative nature as prescribed by the State Records Regulation.
- j. **NSW RFS Recordkeeping Manual (the Manual):** the official document that details the recordkeeping processes for the NSW RFS and is located on the Records intranet page.
- k. **Personal Information:** information or opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.
- l. **Record (digital and physical):** any document or other source of information compiled, captured in audio format or stored in written form or on film, or by electronic process, or in any other manner or by any other means, e.g. letters, emails, photographs, audio and visual recordings, websites, social media, databases etc.
- m. **Recordkeeping system:** any system, paper or digital that captures and stores records.
- n. **Sensitivity labelling:** standard labels to mark sensitive official information for the purpose of protecting confidentiality.
- o. **State Archive:** State records of continuing value that require transfer of custody to the State Records Authority, as identified in disposal schedules.
- p. **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.

## 3 Policy

### Creation and capture of records

- 3.1 All NSW RFS staff and contractors are responsible for ensuring records of business activity they undertake are created and captured in approved recordkeeping systems.
- 3.2 Wherever possible, records that are created digitally should be retained in digital format and paper records should be imaged (e.g. scanned) to improve accessibility. The paper copy may be destroyed if the conditions outlined in SOP P5.1.6-1 Creation and Capture of Records are adhered to.
- 3.3 The procedures outlined in SOP P5.1.6-1 Creation and Capture of Records should be adopted to avoid duplication in the recordkeeping systems and improve the integrity of the records.

### Security and access to records

- 3.4 Where appropriate records are to be assigned a Security Classification and/or Dissemination Limiting Marker (DLM) in accordance with SOP P5.1.6 - 2 Security and Access to Records.
- 3.5 Staff will be provided with the appropriate level of access to records and recordkeeping systems to enable them to undertake their duties in accordance with their position.
- 3.6 Staff should only access or provide access to records in the proper course of business and through the correct channels, and in accordance with Service Standard 1.1.7 NSW RFS Code of Conduct and Ethics.

### **Maintenance and storage of records**

- 3.7 All staff are to ensure records are stored with appropriate levels of preservation, security and accessibility, in particular those that are vital to the function of NSW RFS. This will minimise accidental loss or destruction and the granting of access to unauthorised individuals.
- 3.8 Audits of records and recordkeeping systems may be undertaken to ensure compliance with this Policy and statutory requirements.
- 3.9 Managers are to ensure that each NSW RFS facility has local disaster recovery and business continuity plans for physical records. Refer to Policy P7.1.9 Business Continuity Management.
- 3.10 Physical records are to be stored in an appropriate storage location as described in the NSW RFS Recordkeeping Manual (the Manual).
- 3.11 The designated NSW RFS business owners of ICT systems are to ensure recordkeeping systems, especially those that are vital to the function of NSW RFS, are managed and kept up to date, thus reducing the risk of loss of technology-dependent records.
- 3.12 Removable storage devices (e.g. CD's, flash or portable hard drives) or limited access drives (e.g. C: drive) are not to be used for the storage of official NSW RFS records.
- 3.13 The email system and shared drives (such as G: drive) are not suitable for the storage and management of NSW RFS records, and records created or received in these systems should be transferred to approved recordkeeping systems as soon as practicable.

### **Disposal of records**

- 3.14 Records must not be destroyed or transferred outside the custody of NSW RFS without the prior written consent of the Corporate Records Manager. Certain records may be disposed of under NAP in accordance with SOP5.1.6-4 Disposal of Physical Records, without the approval of the Corporate Records Manager.
- 3.15 Disposal authorities issued by State Records are to be used to determine retention and disposal of records. These are listed in the Manual.

### **Mail services**

- 3.16 The mail system is for official purposes only and must not be used for sending personal articles, cash or valuables. This applies to both internal and external mail.

## **4 Related documents**

- *Evidence Act 1995*
- *Government Information (Public Access) Act 2009*
- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *Public Finance and Audit Act 1983*
- *State Records Act 1998*
- *State Records Regulation 2010*
- NSW Finance and Services - Classification and Labelling Guidelines
- NSW State Records Procedures
- NSW State Records Policies
- NSW State Records Standard: No. 11 - Physical storage of state records
- NSW State Records Standard: No. 12 - Standard on records management
- NSW Premier's Memo M2007-08 Efficient and Cost Effective Management of Records
- NSW Treasurer's Directions (118.01, 240.01)
- Service Standard 1.1.7 Code of Conduct and Ethics
- Service Standard 1.1.14 Personal Information and Privacy
- Service Standard 1.4.5 Social Media
- Service Standard 6.1.3 Training in the NSW RFS

- Policy P5.1.1 ICT Equipment Standards and Security
- Policy P7.1.9 Business Continuity Management
- NSW RFS Records intranet page
- NSW RFS Recordkeeping Manual

## 5 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
31 March 2009	1.0	Initial release
6 November 2012	2.0	<ul style="list-style-type: none"> <li>➤ Repealed v1.0</li> <li>➤ Comprehensive review to reflect current legislative, regulatory and business requirements and organisational alignment</li> </ul>
2 December 2016	3.0	<ul style="list-style-type: none"> <li>➤ Repeals v2.0</li> <li>➤ Comprehensive review to reflect current legislative, regulatory and business requirements and organisational alignment, including aligning processes to HP Records Management</li> </ul>

# SOP P5.1.6-1

## Creation and Capture of Records

### 1 Purpose

- 1.1 All NSW RFS staff members are responsible for capturing evidence of all business activity through the creation of appropriate records in the official recordkeeping systems.
- 1.2 All business unit managers are responsible for ensuring staff remain knowledgeable in how to create appropriate records, and the processes and systems that are in place.
- 1.3 This provides guidance for the effective creation and capture of NSW RFS records into recordkeeping systems, including
  - a. Physical records;
  - b. Digital records of all formats including text documents and images.
- 1.4 This Standard Operation Procedure (SOP) seeks to ensure:
  - a. Records are easily identifiable through consistent naming and titling; and
  - b. Consistent and appropriate access via the use of security classification.

### 2 Procedures

#### Record creation

- 2.1 The *State Records Act 1988* and this Policy require a record to be created whenever a business activity or transaction takes place.
- 2.2 Records that are created electronically should be maintained electronically.
- 2.3 A search for like or existing records is to be conducted prior to creating a new record. This avoids duplication and encourages grouping of like records.
- 2.4 When creating a document, the approved NSW RFS templates are to be used.
- 2.5 Document naming or titling should ensure clear identification of the content of the document.
- 2.6 All documents are to be:
  - a. Named in accordance with the document naming guidelines in the Manual
  - b. Authorised and version controlled, in accordance with the Manual;
  - c. Dated.

Note: Where the document is a contract or agreement, the commencement and end date (or review date) is to be a condition of the agreement. This is required so that disposal schedules can be applied based on the contract end or review date.

#### Record registration

- 2.7 All NSW RFS staff are responsible for the registration of records.
- 2.8 Records are to be registered in the recordkeeping system to assist with identification, tracking and retrieval of NSW RFS records.
- 2.9 The record registration process applies to the creation and capture of:
  - a. Physical records;
  - b. Digital records of all formats in approved recordkeeping systems (e.g. HPRM) or in other business systems (e.g. BRIMS, ICON, SAP, etc) or databases; and
  - c. Folders. Refer to clauses 2.13-2.18 of this SOP for further information.

2.10 Guidelines on what records to capture and what not to capture can be found in the Manual.

### **Avoiding duplication**

2.11 To avoid duplication, only master copies of records are to be registered in recordkeeping systems. For more information refer to the Manual.

2.12 Where a relevant folder exists but is under the control of another NSW RFS section, consideration should be given to sharing this folder, rather than creating a new one.

### **Folders**

2.13 Folders exist for the purpose of filing similar, or “like”, records.

2.14 Folders can be either physical (containing physical records such as documents in paper format); or electronic (containing electronic documents, images etc).

2.15 The creation and management of folders is undertaken by the Records section or the designated officer responsible for records management.

2.16 Requests for the creation of folders should be on the Folder Creation Form and submitted as per guidelines on the form.

2.17 For officers responsible for the creation of folders refer to the Manual for minimum requirements.

2.18 Records Folder numbers are to be referenced on all official outgoing communications including letters, faxes and emails.

### **Imaging (Scanning) of Records**

2.19 Imaging procedures only apply when the paper record is to be disposed of and the imaged copy to be retained as the official record. If these procedures are not applied the paper copy is to be retained.

2.20 Imaging of records is to be undertaken in accordance with State Records guideline – Managing digitisation programs and projects.

2.21 Digital imaging of records (e.g. scanning) is permitted to facilitate efficient business practice. For this purpose, the scanned record is to be captured in the recordkeeping system as an electronic record.

2.22 The use of Optical Character Recognition (OCR) software is recommended to enhance the ability to search the content of records.

2.23 The scanned image must be an authentic and complete reproduction i.e. a true representation of the original document.

2.24 Where colour provides context or is integral to interpretation, the documents are to be scanned in colour e.g. maps, photos, colour coded graphs. If colour is not integral then scanning in black and white is recommended.

2.25 A local document imaging procedure and document imaging checklist is to be implemented to authorise the business unit to dispose of paper records in preference to imaged records. This local procedure is to be developed using the template in the Manual prior to commencing the digitisation process and on replacement of scanner or any major change to the local procedure.

2.26 There are minimum imaging requirements for software and hardware detailed in the Manual that are to be adhered to in order to allow the destruction of the paper record.

2.27 Records to be imaged are to be listed in the local procedure to ensure they are covered by an approved disposal authority.

2.28 Paper copies of scanned documents may be destroyed after 6 months in accordance SOP P5.1.6-4 Disposal of Physical Records.

## **3 Related forms**

➤ Folder Creation Request form

# SOP P5.1.6-2

## Security and Access to Records

### 1 Purpose

- 1.1 This Standard Operating Procedure (SOP) provides guidance for the application of:
- a. Security Classifications and Dissemination Limiting Markers (DLMs) in accordance with whole of government guidelines; and
  - b. Internal access controls to records.

### 2 Procedures

- 2.1 The person responsible for creating or receiving records should ensure appropriate application of protective markings and access controls.

#### Access to records (general)

- 2.2 Owners of business records should ensure appropriate access controls are applied to minimise the misuse of sensitive information for both physical and digital records.
- 2.3 Sensitive records should be stored in secure locations with appropriate restrictions applied.
- 2.4 Access to sensitive information should be provided as required to meet business requirements.

#### Access to records (EDRMS)

- 2.5 Access controls in the EDRMS should be in accordance with the guidelines in the Manual.
- 2.6 Access controls are to be applied to records on creation.

#### Applying Access Controls (EDRMS)

- 2.7 The primary controls for restricting access to records within the EDRMS are the Access Controls.
- 2.8 Access Controls are to be applied at the folder level with the document adopting the same controls.
- 2.9 Access Controls may be amended on a document as required.
- 2.10 Access Controls should be assigned to designated access groups or organisational positions, rather than specific individuals.

#### Security classifications and dissemination limiting markers (DLM's)

- 2.11 Where appropriate, and in accordance with the NSW Government Information – Classification and Labelling Guidelines, protective markings (security classifications & dissemination limiting markers) should be applied to ensure the confidentiality of corporate information.
- 2.12 Protective markings should only be applied where the compromise of the information could damage the National and State interest, organisations or individuals, or requires protection under NSW or Commonwealth legislation.
- 2.13 Classifications should be regularly reviewed to ensure appropriateness over time.
- 2.14 Within the EDRMS, security classifications will restrict access whereas DLMs only provide guidance on handling sensitive information.
- 2.15 The following security classifications may be used where appropriate:
- a. Protected
  - b. Confidential

2.16 The following DLMs may be used when appropriate:

- a. For Official Use Only (FOUO)
- b. Sensitive
- c. Sensitive: Personal
- d. Sensitive: Legal
- e. Sensitive: Cabinet
- f. Sensitive: NSW Government
- g. Sensitive: NSW Cabinet

### **3 Related forms**

- > None



## SOP P5.1.6-3

# Maintenance and Storage of Records

## 1 Purpose

- 1.1 This Standard Operating Procedure (SOP) has been developed to provide guidance on the process for the effective maintenance and storage of NSW RFS records and to ensure:
  - a. That official NSW RFS recordkeeping systems are used to manage appropriate NSW RFS records;
  - b. Consistent procedures are adopted for the storage and retrieval of NSW RFS physical records in approved locations;
  - c. That only authorised persons are granted access to NSW RFS records; and,
  - d. To outline effective procedures for sharing or distributing digital records including suitable short to long term storage locations.

## 2 Procedures

### Tracking of physical records

- 2.1 All users are responsible for ensuring the location of NSW RFS physical records shown in the recordkeeping system is kept up to date to ensure they can be located efficiently. The recordkeeping system is to be updated every time the record changes hands or is put into storage.

### Sharing and distribution of records

- 2.2 Wherever possible, internal distribution of digital records is to be by the use of links and not email attachments. This avoids duplication and enables access to a single source of the record.
- 2.3 Wherever possible and to protect NSW RFS records, all external distribution of official digital records is to be in read-only format such as PDF format.

### Version control

- 2.4 All documents should be version controlled by the author in accordance with the Manual.
- 2.5 Only authorised versions should be captured in an official recordkeeping system.

### Storage of physical records

- 2.6 All storage locations are to be appropriately identified and maintained to minimise the risk of degradation, damage (including pests), and inappropriate access according to the NSW State Records Standard No 11 Physical storage of State records.
- 2.7 Only NSW RFS administrative staff responsible for the management of records within their business unit should be granted access to records in storage in accordance with the Manual.
- 2.8 NSW RFS records more than 12 months old should be submitted to Headquarters Records for storage, unless they are referred to on a regular basis.
- 2.9 Once a retrieved record is no longer required, it should be returned to storage as soon as practical and the location updated in the recordkeeping system.
- 2.10 Each NSW RFS premises that stores records on-site, is to develop and implement a disaster recovery plan in accordance with NSW State Records Standard No 11 Physical storage of State records and Policy P7.1.9 Business Continuity Management.
- 2.11 Depending on the suitability of the premises, records can be stored in boxes or filing cabinets, in accordance with the Manual.

### Off-site storage and retrieval of physical records

- 2.12 Special record storage boxes are used for the storage and added protection of records identified for off-site storage. Only storage boxes recommended or provided by the storage provider are to be used for the storage of NSW RFS records.
- 2.13 The designated officer should create boxes when records are identified for transfer to off-site storage. Storage boxes should contain records of similar type and date range to facilitate timely disposal.
- 2.14 Storage boxes should not be over filled to protect the integrity of the box and its contents and should be able to be firmly closed.
- 2.15 The designated officer responsible for records management is to register the box in the EDRMS.
- 2.16 The process for the retrieval of a storage box should be coordinated by the designated officer responsible for records management and is as follows:
  - a. Ensure sufficient information is provided to identify the appropriate records;
  - b. Conduct a search to identify storage box details;
  - c. Contact supplier and provide their local reference number;
  - d. Arrange delivery;
  - e. Update record location in the EDRMS.

### Storage of digital records

- 2.17 Digital records are to be created and stored in approved NSW RFS recordkeeping systems only in accordance with the Manual.
- 2.18 Microsoft Outlook is **not** a recordkeeping system and emails that are required to be captured as records are to be captured in an approved recordkeeping system, such as the EDRMS.
- 2.19 Network drives are **not** a recordkeeping system and documents that are required to be captured as records are to be captured in an approved recordkeeping system, such as the EDRMS.
- 2.20 The designated NSW RFS business owners of ICT systems are to ensure:
  - a. Recordkeeping systems, especially those that are vital to the function of NSW RFS, are managed and kept up to date, thus reducing the risk of loss of technology dependent records;
  - b. ICT back-ups are used for disaster recovery purposes only and not as recordkeeping systems;
  - c. Monthly ICT back-ups or snapshots of electronic data are kept for a period of 12 months, after which time, these can be destroyed in accordance with normal administrative practice;
  - d. Audit trails of who has accessed, and what operations were performed in recordkeeping systems, are kept for a minimum of 7 years;
  - e. Workflow and record movements are to be kept for a minimum period of 7 years.

## 3 Related forms

- > None

# SOP P5.1.6-4

## Disposal of Physical Records

### 1 Purpose

- 1.1 This Standard Operating Procedure (SOP) provides guidance on the disposal processes for NSW RFS physical records, including destruction and transfer of custody, and to ensure the disposal of NSW RFS records is:
  - a. Authorised by the designated NSW RFS officer and State Records through an approved disposal authority;
  - b. Irreversible, by applying appropriate disposal methods;
  - c. Secure and confidential to prevent unauthorised access;
  - d. Timely to minimise storage costs;
  - e. Documented to provide evidence of what actions have been taken; and,
  - f. Designed to prevent the disposal of records which are required as part of current or pending court cases, legal proceedings, and/or information requests such as those requested under the *Government Information (Public Access) Act 2009*.
- 1.2 This SOP does not apply to the disposal of records of short term value in accordance with the normal administrative practice (NAP) provisions of the *State Records Act 1998* and the *State Records Regulation 2010*.

### 2 Procedures

#### Identification and appraisal of records for disposal

- 2.1 At least once per year, records are to be appraised by the local NSW RFS officer responsible for records management to determine if any are due for destruction, either individually or collectively (e.g. a folder).
- 2.2 Initial assessment may identify records of short term value including local and reference copies or insignificant drafting versions. These can be destroyed locally in accordance with the normal administrative practice (NAP) provisions of the *State Records Act 1998*.
- 2.3 Any record to be disposed of should first be assessed against an approved disposal authority. Refer to the Manual for a listing of all disposal authorities.
- 2.4 Once the correct disposal authority has been identified, it is to be used to classify and determine retention and disposal information for the records marked for disposal in accordance with the Manual.

#### Disposal of imaged record

- 2.5 Records can only be destroyed if they are covered under a current disposal authority as identified in the Manual.
- 2.6 Once scanned, the paper record is to be retained for a minimum of 6 months, after which time it may be disposed of, in accordance with State Records general disposal authority for Imaged records (GA36).

#### Authorisation

- 2.7 The local officer responsible for records management is to complete an Authority to Destroy form and submit to the section manager for endorsement.
- 2.8 If the records are subject to current or pending legal proceedings or an application for access under legislation such as the *Government Information (Public Access) Act 2009*, the *Health Records and Information Privacy Act 2002* or the *Privacy and Personal Information Protection Act 1998*, they should also be considered for exclusion from destruction including after digitisation.
- 2.9 Once endorsed, the form must be submitted to the Records Manager for approval. The only NSW RFS officer with authority to approve the disposal of a record is the NSW RFS Records Manager.

### **Destruction process**

- 2.10 Once the disposal is approved, the designated local officer arranging disposal is to utilise the services of a records destruction service provider approved by NSW Procurement and included on the Integrated Waste Management Government Contract.
- 2.11 Transfers of records to the service provider are to be undertaken using secure transport to avoid accidental loss during transfer.
- 2.12 After the destruction has taken place, the service provider is to provide a certificate of destruction to the local officer coordinating the destruction. This certificate is to be retained together with the approval form.

### **Transfer of custody to State Archives or other organisation**

- 2.13 Some NSW RFS records are required to be transferred to another organisation (e.g. on change of employment to another State authority or on sale of property) or permanently transferred to State Archives (as identified in Disposal Authorities). All transfers are to be undertaken by the Records section only, under the guidance of the Records Manager.
- 2.14 Records held by Regional Offices, District Offices or Headquarters business units that require transfer are to be forwarded to the Records section in accordance with the Manual.

## **3 Related forms**

- Authority to Destroy form

## **SOP P5.1.6-5**

# **Management of Corporate Correspondence**

## **1 Purpose**

- 1.1 This Standard Operating Procedure (SOP) provides guidance to ensure that all incoming and outgoing business correspondence, including that initiated by the NSW RFS (including cheques) is identified and captured in the recordkeeping system.

## **2 Procedures**

### **Receipt and handling of incoming mail**

- 2.1 All mail received by NSW RFS is deemed business correspondence and is to be opened and receipted by the Records Unit or designated NSW RFS section, with the exception of any mail addressed to the Chaplaincy Section and Critical Incident Support Services.
- 2.2 Wherever possible, incoming correspondence should be opened in the company of at least two officers, in accordance with the NSW Treasurer's Directions (s118.01).
- 2.3 Correspondence that is marked "Confidential" should be opened by NSW RFS staff responsible for the management of mail.
- 2.4 All mail that is marked "Private" or "Personal" is to be forwarded unopened to the addressee. Where the addressee identifies this as business correspondence, it is to be registered in the EDRMS.
- 2.5 All mail items, including cheques, are to be receipted with an official stamp, which includes the date of receipt and NSW RFS identification.
- 2.6 Invoices received in the mail should be forwarded directly to the Headquarters Finance Section for processing.
- 2.7 Solicited and unsolicited advertising material, including brochures, catalogues and price lists are not required to be recorded as an official record and can be disposed of at the discretion of the local office.
- 2.8 Any quotations received are to be retained as a record, in accordance with the relevant financial requirements.
- 2.9 All Australia Post notifications of mail articles to be collected from the local post office should be forwarded to the addressee to arrange collection. The Records unit is not responsible for collection of these items as it is an Australia Post requirement that the addressee presents identification upon collection of the item.

### **Registration of correspondence and cheques/cash**

- 2.10 All business correspondence is to be registered in the EDRMS in accordance with the recordkeeping manual.
- 2.11 All cheques received in the mail are to be recorded in a cheque and cash register and forwarded to the Headquarters Finance Section each day. The register is to be created in the EDRMS using the Daily Cheque Register template.
- 2.12 Australia Post and the NSW RFS do not recommend the sending of cash via external or internal mail however should cash be received, it should also be recorded in the cheque and cash register.

### **Dispatch of mail**

- 2.13 Mail services are only to be used for official business correspondence.
- 2.14 All mail items should be securely packaged to avoid accidental loss or damage.
- 2.15 Cash is not to be sent through the mail system.
- 2.16 Where mail is sent via an external service provider on account, a copy of the mail lodgement advice is to be retained in the EDRMS.

- 2.17 One business day's notice should be provided for large or bulk mail outs, international parcels and other special postal services to ensure timely dispatch.

### **3 Related forms**

- None