

CHAPTER 3

ADF CADETS RECORDS MANAGEMENT

INTRODUCTION

4.3.1. The Defence Records Management Policy (DRMP) outlines the requirements that Defence must comply with as a Commonwealth agency to fulfil its lawful obligations under the [Archives Act 1983](#). The DRMP establishes clear principles for records management within Defence and applies to all records created as part of Defence decision-making and business activities.

4.3.2. The content of the DRMP is consistent with the guidance provided by the National Archives of Australia (NAA) and incorporates relevant Australian and international standards for records and document management to ensure alignment with recognised best practices.

4.3.3. The legal instrument issued by the NAA which outlines the mandatory requirements of Australian Government agencies for retaining, transferring or disposing of records is called a 'Records Authority'. A 'Records Authority' contains information about the classes of records that must be retained, how long they must be retained and other conditions for the disposal of records. To meet the NAA's records disposal requirements and to ensure there is adequate coverage for the records created during the conduct of Defence business, several subject-based Records Authorities have been established within the Defence organisation, including a subject-based records authority for Defence Youth and Cadets.¹

4.3.4. The Defence Youth and Cadets Records Authority focuses on the core business of Defence when managing contact, engagement and interaction with youth in a variety of ways, both in Australia and overseas. This involvement with youth is acknowledged as a unique arrangement within Defence and accordingly in the context of the administration of all related records. Not only are ADF and APS personnel directly involved, but also other stakeholders are considered to hold direct involvement, such as approved volunteer non-Defence adults and youths who participate in ADF Cadets programs.

4.3.5. In addition to the requirements of the [Archives Act 1983](#), the [Royal Commission into Institutional Responses to Child Sexual Abuse](#) delivered its final report in December 2017 and recommended that all institutions that engage in child-related work should implement high-level recordkeeping principles in response to the risk of child sexual abuse occurring within the institution.

4.3.6. The Royal Commission recommended, amongst other things, that full and accurate records should be created and maintained for all incidents, responses and decisions affecting child safety and wellbeing, including child sexual abuse and that records should only be disposed of in accordance with law or policy.

¹ NAA Records Authority 2019/00457762 (Defence Youth and Cadets)

4.3.7. Key observations from the Royal Commission were that the rights of individuals to access records about themselves should be recognised to the fullest extent and that institutions must dedicate time and resources to creating and managing records.

4.3.8. Defence has a requirement to manage its records in a way that complies with legislation, standards and government policy, provides for public accountability, supports decision-making and which preserves corporate memory and historical information. To meet this requirement, all Defence records must be created, captured and controlled, made accessible and disclosed when required and be retained and disposed of in accordance with the principles in the DRMP.

4.3.9. The DRMP sets the standards for Defence to achieve compliance with the *Archives Act 1983* and the recommendations of the Royal Commission and directs Defence personnel, including those involved with ADF Cadets programs, to manage their obligations when creating, capturing, controlling, accessing and disposing of Defence records.

POLICY INTENT

4.3.10. The purpose of this policy is to outline the records management practices required to ensure that complete and accurate records of all ADF Cadets activities and decisions are created, captured, controlled, accessed and disposed of appropriately and in accordance with the DRMP.

POLICY PRACTICES AND MEASURES

DEFENCE RECORDS

4.3.11. A Defence record is any document or object, in any form, that contains information relating to Defence activities that is created, captured, managed or stored by Defence personnel or external service providers in order to provide evidence of that activity.

4.3.12. Records are not restricted by format and include structured and semi-structured data, raw and processed data, documents, images, audio and visual digital media, handheld imagery and motion imagery, emails, web pages, social media posts, medical documentation and imagery, technical drawings and physical objects (such as art work and artefacts).

4.3.13. Records constitute the 'memory' of Defence by documenting decisions, actions, events, policies and processes. As such, records strengthen current and future decision making capability, inform stakeholders and support litigation and regulatory compliance. To achieve these outcomes, records must be created, managed, retained, accessible and appropriately preserved and/or destroyed.

MATERIAL WHICH IS NOT A RECORD

4.3.14. A document or object is not a record if it does not relate to Defence activities, has no unique content or is only momentarily useful. Documents or objects relating to Defence activity are not records if they are:

- a. copies of blank forms, templates or form letters
- b. copies of material retained for convenience or reference purposes only
- c. facilitative, transitory or short-term items
- d. rough working papers
- e. drafts not intended for further use or reference whether in paper or electronic form, including documents that have minor edits for grammar and spelling and do not contain significant or substantial changes or annotations.

CREATION OF RECORDS

4.3.15. Records are created to preserve the corporate memory and historical information related to Defence events, activities, decisions and personnel. Records are required to be complete, reliable and fit for purpose enabling Defence to:

- a. meet operational, legal and legislative obligations
- b. provide accurate and adequate evidence of Defence functions, policies, procedures, decisions and transactions
- c. support lessons learnt and better decision-making in the future.

CAPTURING AND DESCRIBING RECORDS

4.3.16. Defence records are to be captured in systems that ensure they are adequately described, organised and preserved for as long as they need to be kept. When records are adequately described, users will have confidence in the integrity of the records and will be able to discover and retrieve records more readily.

4.3.17. Systems that hold records need to have an information structure that enables Defence personnel to store their records and find information when they need it. Information structures should be fit for purpose and organise records in a way that:

- a. uses recognisable and understood terminology
- b. enables Defence personnel to know where they need to store records

- c. enables Defence personnel to navigate to the records they need
- d. enables specialist records management activities including disposal.

4.3.18. Where possible, records must be captured in digital format to support the systematic and consistent application of records management practices. Physical processes should only be used to store records where digital systems are not available.²

4.3.19. Descriptive information in digital records (called metadata) can be used to identify, authenticate and contextualise records, making them easier to find, retrieve and use. Appropriate preservation techniques ensure the records remain accessible and usable for as long as required.

ACCESSING AND DISCLOSING RECORDS

4.3.20. Access to Defence records is to be managed in a way that ensures they are available when needed to conduct Defence business and are protected from unauthorised access when necessary.

4.3.21. Defence has an obligation under the *Archives Act 1983*, *Freedom of Information Act 1982* and *Privacy Act 1988* to enable public access to Defence records. However, the *Archives Act 1983* provides some exemptions for Defence Intelligence agencies.

4.3.22. Defence security policy for the Classification and Protection of Official Information must be applied to Defence records in accordance with the Defence Security Principles Framework. Access to records will only be restricted when required by Defence security policy, legislation or business requirements.

4.3.23. Where Defence holds personal information about an individual that was collected for a particular purpose, Defence must not use or disclose that information for another purpose. Prior to considering disclosing personal information about a young person or another individual, all other courses of action must be considered. This includes encouraging the young person or other individual to self-disclose the relevant personal information to the parents, a responsible third party or government oversight body.

RETENTION AND DISPOSAL OF RECORDS

4.3.24. The legal requirement to retain records is mandated by Commonwealth legislation. Defence records are to be disposed of when all legal requirements for the

² In 2011, the Australian Government released the Commonwealth 'Digital Transition Policy' which requires agencies to move to digital information and records management, and away from paper-based records management. This means that the majority of Defence's records must be created, stored and managed digitally, and where practicable, paper records should also be digitised.

retention of records have been met and when the records are no longer required for business or historical purposes. Records that are no longer required should be disposed of to enable the efficient and effective use of current records and to reduce the cost of records management practices.

KEY ROLES AND RESPONSIBILITIES

4.3.25. All Defence records are owned by the Department of Defence. The Secretary and the Chief of Defence Force are ultimately accountable for all Defence records although everyone has a responsibility towards Defence records.

4.3.26. **Group Heads and Service Chiefs** serve as the sponsor for records management within their Group or Service. They are responsible for ensuring that their respective Group or Service complies with the policy contained in the DRMP.

4.3.27. **Functional Commanders and Division Heads** are responsible for allocating adequate resources and approving local records management guidelines that meet business and functional requirements.

4.3.28. **Records Management Advisors** are responsible for providing specialist advice, leadership and coordination in relation to records management. They are required to:

- a. assist Group Heads and Service Chiefs and the Functional Commanders and Division Heads to make records management related decisions
- b. develop local records management guidelines to meet business and functional requirements.

4.3.29. The Records Management Advisor role must be identified on the employee's performance agreement and the relevant specialised training must be completed.

4.3.30. **Records Management Specialists** are responsible for managing and maintaining the day-to-day records management activities including system administration and the provision of records management training. The Records Management Specialist role must also be identified on the employee's performance agreement and the relevant specialised training must be completed.

4.3.31. **Managers and supervisors** are responsible for identifying where specialist records management resources are required and for ensuring that Records Management Specialists are given support to complete day-to-day records management activities.

4.3.32. **All Defence personnel** are responsible for following the approved local records management guidelines and completing training to understand their role and responsibilities.

ADF CADETS RECORDS

4.3.33. A record in the ADF Cadets context is any artefact (physical or digital) that preserves the memory or knowledge of facts from which information can be obtained in relation to ADF Cadets events, activities, decisions, personnel and processes, regardless of format including:

- a. emails, documents, reports, assessments and forms
- b. presentations, plans and spreadsheets
- c. photographs, videos and graphics
- d. social media posts and images from websites.

CORE FUNCTIONS

4.3.34. The core functions and business activities associated with ADF Cadets programs which require appropriate records management processes include, but are not limited to:

- a. developing and implementing agreements policies, directives, strategies, procedures and other guidance material such as handbooks and manuals
- b. accepting and managing adult volunteers and youth
- c. planning, evaluating, approving and reporting on events and activities
- d. conducting risk assessments and managing risks
- e. delegating authority and approving actions
- f. providing and receiving advice
- g. receiving and handling complaints of unacceptable behaviour
- h. managing youth protection and safety incidents
- i. providing care or welfare services to youth
- j. conducting training for adult volunteers and youth
- k. undertaking compliance and monitoring functions
- l. conducting and facilitating audits
- m. liaison with other Cadet programs.

4-3-7

4.3.35. With regard to the recommendations of the Royal Commission into Institutional Responses into Child Sexual Abuse, appropriate records management processes must be undertaken by ADF Cadets programs in relation to:

- a. receiving and managing disclosures, allegations and complaints of child sexual abuse or neglect
- b. referring matters to other bodies (for example, referrals to the Australian Federal Police)
- c. conducting investigations and inquiries into actual or alleged incidents of child sexual abuse or neglect
- d. collecting and managing supporting documents and other evidence
- e. conducting interviews with witnesses
- f. preparing investigation briefs
- g. imposing sanctions, penalties and disciplinary actions
- h. provide remedial action for individuals who have made allegations of child sexual abuse or neglect.

4.3.36. Full and accurate records about all incidents, responses and decisions affecting child safety and wellbeing, including child sexual abuse and neglect, should be created, captured and maintained in accordance with the DRMP.

CAPTURING AND DESCRIBING ADF CADETS RECORDS

4.3.37. ADF Cadets programs are required to create and retain evidence of their actions and decisions made on behalf of Defence. Such evidence must be managed as Defence records and captured in a Defence compliant information management system such as Objective, PMKeyS, the Defence Policing and Security Management System, Sentinel and/or CadetNet whenever possible. When capturing ADF Cadets records in Defence information management system such as CadetNet, care should be taken to ensure records are classified and described appropriately to assist with future access and retrieval.

4.3.38. Any Electronic Document and Records Management System (EDRMS) with advanced recordkeeping functionality that enables the capture, description, and organisation of records, such as those used at school based Cadet units, is considered to be compliant with Defence requirements. Where practicable, all paper records should be digitised and captured on EDRMS of this nature.

4.3.39. In cases where it is not possible to capture ADF Cadets records in Defence compliant information management systems, ADF Cadets records should be:

- a. captured and maintained in suitable secured premises and containers
- b. monitored for environmental conditions appropriate to the record materials and retention periods.

ACCESSING AND DISCLOSING ADF CADETS RECORDS

4.3.40. ADF Cadets records need to be available, accessible and retrievable whenever required for Defence business or whenever individuals require access to records about themselves, as recognised by the Royal Commission. However, ADF Cadets records must also be protected from unauthorised access, tampering or alteration and from accidental or intended damage or destruction.

RETENTION AND DISPOSAL OF ADF CADETS RECORDS

4.3.41. Guidance on the retention and disposal of ADF Cadets records is contained in NAA Records Authority 2019/00457762 (Defence Youth and Cadets). This Records Authority sets out those records that need to be retained and transferred to the NAA as national archives and specifies the minimum length of time that other temporary records need to be kept. It gives Defence members permission under the *Archives Act 1983*, for the destruction of the temporary records described, after the minimum retention period has expired.

4.3.42. Disposal of ADF Cadets records is to be undertaken by authorised Defence members only, and is to occur in a planned, systematic manner, to include records in all formats, in all business environments and in all types of information management systems.

ROLES AND RESPONSIBILITIES FOR ADF CADET PROGRAMS

4.3.43. All Groups and Services responsible for the management of Defence youth programs, including ADF Cadets, must ensure that appropriate arrangements are in place to enable the policies outlined in the DRMP to be implemented.

4.3.44. Head of Reserve and Cadet Support Division is responsible for approving local records management guidelines that meet business and functional requirements.

4.3.45. The Director General Australian Navy Cadets (DGANC), Commander Australian Army Cadets (COMD AAC) and Director General Cadets - Air Force (DGCADETS-AF) must ensure that respective ADF Cadets programs implement records management processes and procedures that are compliant with this policy.

PRIVACY

4.3.46. ADF Cadets records that contain personal information are to be managed in accordance with [Part 1, Section 1, Chapter 2](#) and the [Defence Privacy Policy](#).

Accountable Officer: Chief of Personnel

Policy Owner: Head Reserve and Cadet Support Division