

CHAPTER 5

RECORDS MANAGEMENT POLICY

BACKGROUND

DEFENCE RECORDS MANAGEMENT POLICY MANUAL (RECMAN)

6.5.1 The Defence Records Management Policy Manual ([RECMAN](#)) was first published in 2014 and outlines the requirements that Defence must comply with to fulfil its lawful obligations under the *Archives Act 1983*. The content is consistent with the guidance provided by the National Archives of Australia and incorporates relevant Australian and international standards for records and document management to ensure alignment with recognised best practices.

6.5.2 RECMAN applies to all records created as part of Defence decision-making or business activities. It establishes a clear, decisive and current records management policy for Defence personnel, and supports the transition of records to a digital environment in accordance with the Government's Digital Transition Policy.¹

6.5.3 **Compliance.** All Defence personnel (ADF, APS and contracted personnel) must comply with RECMAN. External service providers must comply with RECMAN where compliance is a condition of their engagement. Members of the Australian Defence Force (ADF) Cadets, including Australian Navy Cadets, Australian Army Cadets and Australian Air Force Cadets, must comply with RECMAN.² Failure to comply may result in the member being subject to criminal penalties as outlined under the *Archives Act 1983*.

ROYAL COMMISSION INTO INSTITUTIONAL RESPONSES INTO CHILD SEXUAL ABUSE

6.5.4 The Royal Commission into Institutional Responses into Child Sexual Abuse was established in 2013 and delivered its final report in December 2017. Volume 8 of the report (*Recordkeeping and information sharing*) examines records and recordkeeping by institutions that care for, or provide services to children.

6.5.5 Specific to Recommendation 8.4 of the report, the Royal Commission recommended that all institutions that engage in child-related work should implement the following five high-level principles for records and recordkeeping, to a level that responds to the risk of child sexual abuse occurring within the institution:

- a. creating and keeping full and accurate records relevant to child safety and wellbeing, including child sexual abuse, is in the best interests of children and should be an integral part of institutional leadership, governance and culture

¹ 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.

² [RECMAN](#) Chapter 3 Paragraph 3.3.

- b. full and accurate records should be created about all incidents, responses and decisions affecting child safety and wellbeing, including child sexual abuse
- c. records relevant to child safety and wellbeing, including child sexual abuse, should be maintained appropriately
- d. records relevant to child safety and wellbeing, including child sexual abuse, should only be disposed of in accordance with law or policy
- e. individuals' existing rights to access, amend or annotate records about themselves should be recognised to the fullest extent.

6.5.6 A key observation from the Royal Commission outlined the need for institutions to dedicate time and resources to creating good records, and managing those records.

POLICY INTENT

6.5.7 The records management policy (refer Section 1 Chapter 2) is intended to meet Defence's obligations to the RECMAN and the Royal Commission report for youth protection, as well as fostering and maintaining best practice records management standards.

6.5.8 The policy outlines the requirements to ensure complete and accurate records of all Defence Youth Program activities and decisions are created, managed, retained or disposed of appropriately, and in accordance with relevant legislation.

6.5.9 Effective records management supports Defence in maintaining authoritative information that has integrity and is accessible, auditable, accurate, reliable, complete, and of a high quality.

6.5.10 YOUTHPOLMAN Part Two contains all ADF Cadets common tri-Service policy. The policies provide leading practice, evidence-based direction on the day to day management of the ADF Cadets enterprise, including unique records management policies where necessary.

POLICY PRINCIPLES

6.5.11 All Defence Youth Programs must be able to demonstrate that due process has been followed in their actions and decision making, including through the existence and maintenance of good record keeping systems.

6.5.12 All Groups and Services responsible for the management of Defence Youth Programs including ADF Cadets must ensure that appropriate arrangements and adequate resourcing are in place to enable implementation of the policies outlined in Section 1 Chapter 2.

POLICY PRACTICES AND MEASURES

RESPONSIBILITIES

6.5.13 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.

6.5.14 Group Heads and Service Chiefs are responsible for ensuring that their respective Group or Service complies with the policy contained in RECMAN and must ensure that procedural guidance and adequate resources are available to support its implementation.

6.5.15 All Defence personnel, contractors, consultants and outsourced service providers, are accountable for their actions and are required to create and retain evidence of their actions and decisions made on behalf of Defence. Such evidence must be managed as records and captured in a Defence compliant Information Management system such as Objective.³ Contractors, consultants and outsourced service providers are responsible for records management tasks where this has been documented in the conditions of their engagement.

6.5.16 [RECMAN Chapter 4](#) provides detailed policy on how to identify, describe and manage records throughout their life, including creation, capture, storage, digitisation, accessibility and disposal.

Accountable Officer: Chief of Joint Capabilities (CJC)

Policy Officer: Head Joint Support Services Division (HJSSD)

³ Compliant Defence Record Management systems include Objective, PMKeyS, the Defence Policing and Security Management System, Sentinel and CadetNet.