# CHAPTER 2

# YOUTH PROTECTION DOCUMENTATION, RECORDS AND PRIVACY

## INTRODUCTION

1.2.1 Having clearly documented youth protection policies and procedures enables Defence to communicate expectations for, and achieve consistent application of child safe practices across Defence. It also enables Defence to examine, through continuous review and improvement processes, adherence to youth health, protection and wellbeing principles and practices.

1.2.2 Defence also has a legal obligation to manage personal information in accordance with the Privacy Act and, specifically in relation to youth, Article 16 of the *United Nations Convention on the Rights of the Child*.

1.2.3 This chapter defines requirements for effective management of youth protection documentation and records, including privacy requirements.

## POLICY INTENT

1.2.4 The intent of this policy is to ensure that:

a. youth protection documentation, including policies, processes, practices, procedures, training packages and guides are documented, fit for purpose and continuously improved

b. youth protection documentation and records are managed and protected in accordance with Defence records management and privacy policy.

1.2.5 Defence youth protection documentation, records and privacy policy is consistent with the following National Principles for Child Safe Organisations:

a. **Principle 1**: *Child safety and wellbeing is embedded in organisational leadership, governance and culture.*

   (1) **Key Action Area 1.6**. *Staff and volunteers understand their obligations on information sharing and record keeping.*

b. **Principle 9**: *Implementation of the national child safe principles is regularly reviewed and improved*

   (1) **Key Action Area 9.1**: *The organisation regularly reviews, evaluates and improves child safe practices*

c. **Principle 10**: *Policies and procedures document how the organisation is safe for children and young people*

   (1) **Key Action Area 10.1**: *Policies and procedures address all national child safe principles*

(2) **Key Action Area 10.2**: *Policies and procedures are documented and easy to understand*

(3) **Key Action Area 10.3**: *Best practice models and stakeholder engagement informs the development of policies and procedures.*

1.2.6 Other Defence publications which may be relevant to this policy include, but are not limited to:

a. Defence Records Management Policy Manual (RECMAN), which prescribes records management requirements applicable to the whole of Defence

b. Defence Privacy Policy, which provides guidance on how Defence collects, stores, uses, discloses personal information, deals with breaches and complaints.

c. Defence Instruction Administrative Policy Annex I, *Disclosure of Certain Personal Information in Relation to Youth Safety Incidents*, which provides the authority and circumstances in which it may be appropriate for Defence personnel to disclose personal information to protect the health, protection and wellbeing of youth

d. Good Decision Making in Defence and the Supplement to the Defence Decision Makers Guide, *Disclosure of Certain Personal Information in Relation to Youth Safety Incidents*.

## DEFINITIONS

1.2.7 **Youth Protection Documentation.** Youth protection documentation comprises all youth protection policies, processes, practices, procedures, training packages/resources and guides, including:

a. Joint Support Services Division (JSSD) sponsored Defence Youth Protection Management System (DYPMS) policy and guidance defined in this manual, Defence youth protection training packages and documentation, and youth protection related guides and other reference material

b. Group/Service and subordinate level youth protection management orders, instructions and publications (OIP), training packages/resources and other guidance material that contextualise implementation of the DYPMS.

1.2.8 **Youth Protection Records.** Youth protection records comprise any electronic or hard copy document, record, data or information generated through implementation of the DYPMS, including records relating to:

a. personnel screening, working with children checks and codes of conduct

b. risk assessments

c. complaints, events, incidents and any associated disclosure of personal information

d. workplace inspections, audits and surveys

e. data analysis

f. meetings, committees, councils and boards

g. training administration

h. feedback, forums and other communication.

1.2.9 Unlike youth protection documentation, youth protection records may contain personal information that is subject to Defence Privacy Policy (refer paragraph 1.2.18).

1.2.10 **Personal Information.** Personal information, as defined in the Privacy Act, is information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is:

a. true or not

b. recorded in a material form or not.

1.2.11 Personal information may also be sensitive information.

1.2.12 **Sensitive Information.** Sensitive information, as defined in the Privacy Act, is personal information that includes information or an opinion about an individual's:

a. racial or ethnic origin

b. political opinions or associations

c. religious or philosophical beliefs

d. trade union membership or association

e. sexual orientation or practices

f. criminal record

g. health or genetic information

h. biometric information.

1.2.13 Generally, sensitive information has a higher level of privacy protection than other personal information.

## POLICY

### YOUTH PROTECTION DOCUMENTATION AND RECORDS

1.2.14 **Compliance with Child Safe Requirements.** Head Joint Support Services Division (HJSSD) must ensure that the DYPMS and associated documentation complies with the requirements of the Commonwealth Child Safe Framework and applicable Commonwealth, state and territory legislation.

1.2.15 **Compliance with DYPMS.** Group Heads and Service Chiefs must ensure that Group/Service youth protection documentation and records comply with the requirements of the DYPMS.

1.2.16 **Documentation and Records Management.** Youth protection documentation and records must be created, stored and managed in the appropriate enterprise system[1] in accordance with relevant enterprise system policy/guidance and RECMAN.

1.2.17 **Documentation Requirements.** Youth protection documentation must be:

a. in a language and format appropriate to the target audience

b. reviewed and/or updated as appropriate:

(1) when relevant Commonwealth, state, territory or Defence legislation, policy and/or guidance changes

(2) when DYPMS policy and/or guidance changes

(3) when deficiencies are identified or suggestions for improvement are received

(4) at least every three years

c. available and accessible to youth, the community, Defence youth program volunteers and participants, and Defence personnel as appropriate.

## PRIVACY AND DISCLOSURE OF PERSONAL INFORMATION

1.2.18 Commanders, managers and supervisors must ensure that personal information and youth protection records containing personal information are managed in accordance with Defence Privacy Policy and paragraph 1.2.19.

1.2.19 **Privacy Statement.** The following Privacy Statement must be used on all documentation, information technology systems and on any other occasion where Defence collects information relating to youth and Defence youth programs:

> *Defence collects your personal information for the purpose of administering, evaluating and reporting on Defence Youth Programs. The personal information you provide is subject to the Privacy Act 1988 and is handled in accordance with the Australian Privacy Principles and the Defence Privacy Policy.*
> *The Defence Privacy Policy explains how Defence (including the Australian Defence Force Cadets) collects, stores, uses and discloses personal information, and is available at www.defence.gov.au/ComplaintResolution/privacy.asp. This policy is supplemented by privacy provisions contained in the Youth Policy Manual available at www.defenceyouth.gov.au.*

[1] Appropriate Defence enterprise systems include Objective, PMKeyS, CadetNet, Sentinel, Defence Policing and Security Management System, and Army Incident Management System

*The information you provide to Defence and any other information Defence collects about you may be used and/or disclosed by Defence to parents, responsible third parties or any law enforcement body, child protection agency or any other organisation where considered necessary to safeguard young people.*

## PERSONAL INFORMATION

1.2.20 **Use of Personal Information.** Personal information must not, without the consent of the person to whom the information relates, be used for any other purpose than that for which it was obtained or disclosed to those for whom it was not collected, except where permitted in in the Privacy Act or paragraphs 1.2.23 and 1.2.24 of this policy.

1.2.21 Individuals can request access to, or correction of their personal information in accordance with the Defence Privacy policy. Copies of the policy can be obtained from the Defence Privacy webpage, or by emailing: defence.privacy@defence.gov.au

1.2.22 **Personnel Authorised to Disclose Personal Information.** Only Defence personnel are permitted to disclose or authorise disclosure of personal information held by Defence about a youth or any other person.

1.2.23 The youth or any other person to whom the personal information relates must be advised of any decision to disclose the information prior to the disclosure occurring to allow them the opportunity to self-disclose or to request a review of the decision.

1.2.24 **Disclosure of Personal Information.** Defence personnel may disclose or authorise disclosure of personal information held by Defence about a youth or any other person to the youth's parents/guardians/specified next of kin, or a responsible third party if:

a. the youth has been involved in a youth protection event/incident (refer Section 3 Chapter 3)

b. they are reasonably satisfied in the circumstances that it is necessary and appropriate for the personal information to be disclosed to protect the health, protection and wellbeing of the youth, having considered:

(1) the youth's age and any wishes expressed by the youth

(2) the nature of the personal information and its relevance to the youth's health, protection and wellbeing

(3) the nature and seriousness of the youth protection event/incident

(4) whether or not the youth or other person to whom the personal information relates is willing and able to self-disclose the information.

1.2.25 Defence personnel must disclose or authorise disclosure of personal information held by Defence about a youth or any other person to a government oversight body if:

a. there is a federal legislative requirement to report certain information to a government oversight body (the reporting requirement)

b. all of the conditions or criteria that trigger the reporting requirement are satisfied.

1.2.26 **Review of decision to disclose personal information.** Following a decision to recommend disclosure of personal information of a youth, a review of the decision can be requested and natural justice will apply. The review is to be conducted by a Defence member other than the decision maker.

1.2.27 Decision makers are responsible for making the youth aware of the review processes available to them when advising of a decision to disclose personal information.

## SENSITIVE INFORMATION

1.2.28 **Non-disclosure of Sensitive Information.** Defence personnel are not authorised to, and **must not** disclose or authorise disclosure of sensitive information to parents/guardians/specified next of kin, responsible third parties or government oversight bodies.

## COMPLAINTS AND BREACHES

1.2.29 **Complaints and Breaches.** Advice about how to make a complaint or raise a potential breach of privacy can be obtained from the Defence Privacy policy.

**Accountable Officer**: Chief of Joint Capabilities (CJC)

**Policy Owner:** Head Joint Support Services Division (HJSSD)