

OFFICIAL

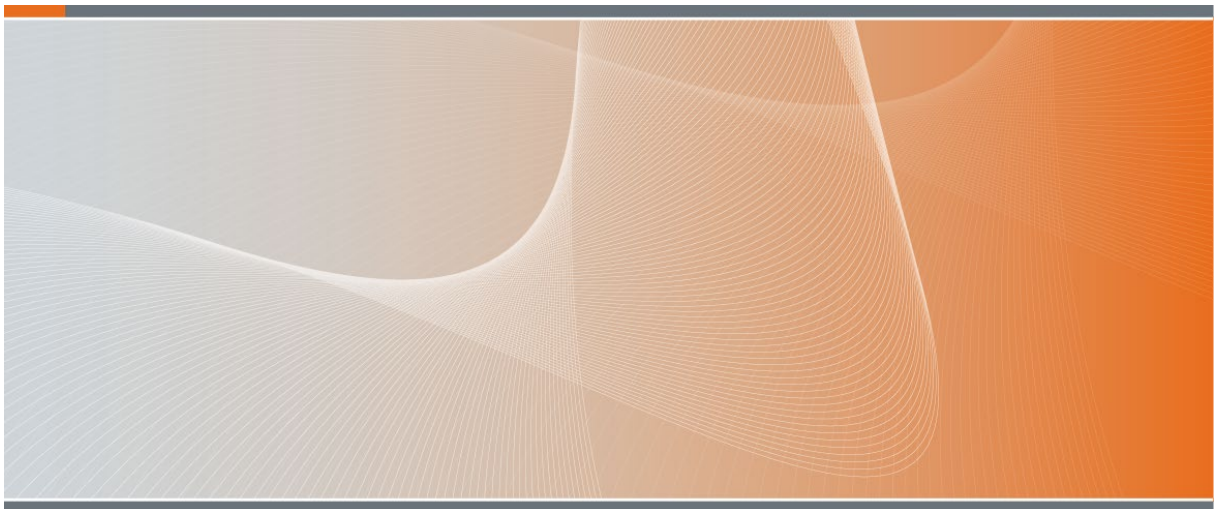


Australian Government

Defence

DEFENCE INSTRUCTION

ADMINISTRATIVE POLICY



A handwritten signature in black ink, appearing to read 'G Moriarty'.

Greg Moriarty
Secretary

Department of Defence
CANBERRA ACT 2600

01 July 2022

A handwritten signature in black ink, appearing to read 'A Campbell'.

Angus J Campbell
General
Chief of the Defence Force

Department of Defence
CANBERRA ACT 2600

04 July 2022

OFFICIAL

AMENDMENT CERTIFICATE

Amendment number	Amendment description	Effective date
AL1	Minor editorial amendments, and inclusion of annexes B to I, including two new military enabling provisions at Annex H.	2 May 2018
AL2	Minor editorial amendments. Addition of one new administration and governance domain provision, one new military enabling provision and five new people domain provisions.	2 July 2018
AL3	- Minor editorial amendments - Main body - six principles of policy development have been included - Main body - references to 'consultant' and 'outsourced service provider' have been replaced with 'a person/s engaged under a contract' and the scope of the framework has been revised to exclude Group and Service specific documents. - Annex A - the definitions of a 'contractor' has been replaced with a definition of 'a person/s engaged under a contract' and the definition of 'administrative policy' have been amended. - Annex A - the definition of 'technical authority' has been added. - Annex C – addition of five new provisions in administration and governance domain (AG2, AG3, AG4, AG5 and AG6) - Annex E – estate management domain changed title to estate domain - Annex H – addition of military command support domain - Annex I – military enabling domain changed title to military joint enabling domain. The accountable officer changed from Vice Chief of the Defence Force to Chief of Joint Capabilities. - Annex J – addition of three new provisions in people domain (PPL6, PPL7 and PPL8) - Addition of Annex K – administrative policy domain structure	8 August 2019
AL4	- Minor editorial amendments to the main body of this Instruction - Annex A – the addition of three definitions: 'administrative policy framework', 'personal	25 July 2020

	information' and 'sensitive information' - Annex C AG1 – deletion of paragraph AG1.3 - Annex C AG2 – Cancelled - Annex C AG3 – Cancelled - Annex C AG5 – Amendment to paragraphs 5.1b to include obligation for Star Ranked personnel, 5.6 removed to correct duplication, 5.8 amended - Annex C AG6 – Cancelled - Annex C AG7 – Addition of new provision - Annex D – title changed from Strategic policy and intelligence domain to Strategy, policy, and industry domain (to align with impending organisational change with effect 1 September 2020) - Annex J PPL3 – language relating requirements for maintaining a zero blood alcohol concentration amended - Annex J PPL4 – amended to allow for cancellation of Interim Defence Instruction 15-6 - Annex J PPL5 - paragraphs 5.1 and 5.2 amended to make exception for people with a protected identity status. Paragraph 5.6 added to include reference to the Defence Security Principles Framework. - Annex J PPL9 – Addition of new provision - Annex K – 'the policy domain structure' is now Annex L - Annex K is now reserved for the new Intelligence policy domain (to align with impending organisational change with effect 1 September 2020)	
AL5	- Annexes MSC1 and MJE1 – administrative amendment to correct issued date and period of effect date	17 December 2020
AL6	- Minor editorial corrections in the main body of this Instruction - Amended front matter to reflect change in policy owner title, First Assistant Secretary Governance and Reform to First Assistant Secretary Enterprise Transformation and Governance - All Annexes – removal of issue date and period of effect. Annex C AG1 – minor editorial amendments - Annex C AG4 – inclusion of definition for 'Defence Investigative Authority' and amended	5 July 2021

	the definition of 'Notifiable incident' - Annex C AG5 – clarification of reporting arrangements for conflicts of interest. Added 'Defence Values and Behaviours' in paragraph 5.1(d). Change of title from Directorate of Fraud Control to First Assistant Secretary Audit and Fraud Control in paragraph 5.7 - Annex C AG7 – added requirement to engage Defence Legal in relation to 'intellectual policy and practice' in paragraph 7.6(a) vi. Amended requirement to engage Defence Legal on matters relating to legislative amendments in paragraph 7.6(d) - Annex I MJE1 – amended terminology regarding youth protection incidents. Amended the object of MJE1 to reflect the same - Annex J PPL2 – amended title of policy contact - Annex J PPL3 – deleted repetitious paragraph 3.4. - Annex J PPL9 – addition of Maritime Spiritual Wellbeing Officer (MSWO). Amended terminology to describe the appointment of honorary rank for chaplains and MSWO. Amended terminology describing duties and obligations of chaplains and MSWO. - Annex J PPL10 – addition of new provision – Notification of Protection Order or Weapons Prohibition Order - Annex L – Insert new Innovation, Science and Technology domain - Annex M – the policy domain structure moved from Annex L to Annex M and there has been business functions added to Intelligence domain and a change in wording of joint military enabling domain business functions	
AL7	- Front matter – Estate policy domain renamed Security and Estate policy domain to align with organisational change; minor amendment to 'availability section' - Main body – minor amendments to increase clarity; para 2 principles amended to align with Transformation Strategy initiatives 1.1, 1.2 and 1.3; inclusion of new para 13 recommending policy owners/accountable officers consider further implications from provisions in the DI; minor editorial amendments to increase clarity - Annexes B, D, F, G, K and L – Wording amended to clarify that there are no provisions for this policy domain currently in force - Annex C – AG1 has been moved to Annex E to	04 July 2022

	align with organisational change – it has been renamed SE1; AG4 policy owner title amended; AG5 policy owner title amended, paras 5.1 a and b amended to include non-star ranked personnel and requirement to disclose when identified and in a particular manner, paras 5.5 and 5.6 impose obligations on person/s engaged under a contract, paras 15 and 16 add clarity around declaration management; AG7 para 7.6 d now includes requirement to engage Defence Legal in relation to new legislation and proposals to develop Defence administered legislation and engaging the Office of Parliamentary Counsel - Annex E – now includes the former AG1 which has been renamed SE1 - Annex H – MSC1 addition of paras 1.5 and 1.6 to appoint Head of Navy Engineering as the Defence Seaworthiness Regulator and impose requirement to act as the regulator of the Defence Seaworthiness Management System; Inclusion of new provision MCS2 appointing the Defence Landworthiness Authority - Annex I – MJE1 minor amendments to improve clarity, para 1.4b extends the authorisation to disclose to include in accordance with a court order or tribunal, para 1.5 includes an exception to the circumstances for not being authorised to disclose - Annex J – PPL7 amendments to increase clarity, para 7.3 the word 'will' has been replaced with 'may' and the definition of 'unacceptable behaviour' has been amended to increase clarity; inclusion of new provision PPL11 appointing a technical authority for Defence Transition. - Annex M – Amendments to reflect organisation change	
--	---	--

DEFENCE INSTRUCTION ADMINISTRATIVE POLICY

Review due: 04 July 2023

Purpose: This Instruction is an administrative policy framework document. It establishes the [administrative policy framework](#) (the framework) that supports the Secretary of Defence (the Secretary) to administer Defence, and the Secretary and the Chief of the Defence Force (the CDF) to jointly administer the Australian Defence Force. Defence personnel **must not** depart from provisions contained in Annexes B to L to this Instruction. The provisions are grouped by [policy domain](#) as follows:

Annexes: [Annex A](#) – Definitions that apply to this Instruction
[Annex B](#) – Acquisition and sustainment policy domain
[Annex C](#) – Administration and governance policy domain
[Annex D](#) – Strategy, policy, and industry policy domain
[Annex E](#) – Security and estate policy domain
[Annex F](#) – Finance policy domain
[Annex G](#) – Information and communications technology policy domain
[Annex H](#) – Military command support policy domain
[Annex I](#) – Military joint enabling policy domain
[Annex J](#) – People policy domain
[Annex K](#) – Intelligence policy domain
[Annex L](#) – Innovation, science and technology domain
[Annex M](#) – Administrative policy domain structure

Document management: This Instruction will be reviewed annually. The review will be coordinated and governed by First Assistant Secretary Enterprise Transformation and Governance. A review may occur sooner to ensure this Instruction continues to align with transformation strategy initiatives.

Availability: This Instruction is current at the date of issue. The issuing of this Instruction may necessitate the updating of subordinate documentation. This Instruction is available from [http://intranet.defence.gov.au/home/documents/data/ADFPUBS/DI G/DI Administrative policy.pdf](http://intranet.defence.gov.au/home/documents/data/ADFPUBS/DI%20G/DI_Administrative_policy.pdf). Its currency cannot be guaranteed if sourced from other locations. It is available for public release.

Policy domain: [Administration and governance](#)

Accountable officer: [Associate Secretary](#)

Policy owner: First Assistant Secretary Enterprise Transformation and Governance

DI ADMINPOL

vii

Policy contact: [Administrative policy team](#)

Cancellations: Cancellations relating to the provisions in this Instruction are detailed at Annexes B to L.

POLICY STATEMENT

1. Efficient and effective administrative policy arrangements support the Secretary of Defence (the Secretary) and the Chief of the Defence Force (the CDF) to jointly administer the Australian Defence Force and the Secretary to administer Defence.
2. Assessing and developing administrative policy favours an agreed Enterprise approach that:
 - a. is principles based and outcomes focussed wherever possible
 - b. empowers our people to be agile, adaptive, ethical and high performing
 - c. is strategy led and data informed
 - d. promotes personal accountability and a culture of continuous improvement
 - e. is easy to understand and apply.

COMPLYING WITH FRAMEWORK DOCUMENTS

3. The Secretary and the CDF expect Defence personnel to comply with, and consistently apply, administrative policies contained in [framework documents](#).
4. Failure to adhere to administrative policy may result in a breach of legislation or other legal obligations.
5. The terms of a contract may extend the application of framework documents to a person/s engaged under a contract.

COMPLYING WITH THIS DEFENCE INSTRUCTION

6. This Defence Instruction (Instruction) is issued by the Secretary and the CDF under section 11 of the [Defence Act 1903](#).
7. This Instruction includes provisions that:
 - a. prescribe or proscribe particular conduct
 - b. impose obligations, functions or duties
 - c. confer powers, authority or rights.
8. This Instruction is not intended to duplicate requirements that already exist in legislation nor does it describe guidelines or provide discretionary procedures.
9. A mandatory requirement of this Instruction is identified by the use of the word '**must**' or the words '**must not**'.

10. This Instruction is a 'general order' for the purposes of the [Defence Force Discipline Act 1982](#). Failure to comply with any mandatory or proscriptive requirement of this Instruction that applies to a Defence member may result in administrative or disciplinary action.

11. This Instruction is a lawful and reasonable direction to Defence Australian Public Service employees by the Secretary for the purpose of subsection 13(5) of the [Public Service Act 1999](#) (subsection 13(5) forms part of the Australian Public Service Code of Conduct). Failure to comply with a mandatory or proscriptive requirement of this Instruction that applies to a Defence Australian Public Service employee may result in investigation and possible sanctions as set out in subsection 15(1) of the [Public Service Act 1999](#), ranging from a reprimand to termination of employment.

12. From 17 August 2017, unless otherwise specified (in Annexes B to L of this Instruction), Defence contract managers **must** include in the terms of any contracts the requirement that a person/s engaged under a contract **must** comply with the mandatory provisions of this Instruction, where the provision is directly relevant to the work a person/s engaged under a contract is performing for Defence.

13. This Instruction is current as at the date of issue. It reflects and refers to applicable statutory and policy provisions as at that date. Accountable officers and policy owners should be aware of, consult and be in a position to advise on any changes, policy or legal implications which may affect their respective Domain provision(s) following the publication of this Instruction.

COMPLYING WITH ACCOUNTABLE AUTHORITY INSTRUCTIONS

14. All Defence personnel **must** comply with [accountable authority instructions](#). Accountable authority instructions draw their authority from the [Public Governance, Performance and Accountability Act 2013](#) and form part of finance law as defined in that Act.

COMPLYING WITH INTERIM DEFENCE INSTRUCTIONS

15. Interim Defence Instructions (interim Instructions) are a means by which the Secretary and the CDF can issue, amend or cancel policy quickly. Provisions in interim Instructions may be appropriate for subsequent inclusion in this Instruction or a manual or policy. Interim Instructions will be reviewed during an annual review of this Instruction and relevant provisions may be incorporated into the most appropriate document types after which the interim Instruction will be cancelled.

16. If an interim Instruction amends a provision included in this Instruction, the provision in the interim Instruction will take precedence over the provision in this Instruction until either the interim Instruction expires or its content is incorporated into this Instruction.

COMPLYING WITH ADMINISTRATIVE POLICIES (INCLUDING THOSE PREVIOUSLY KNOWN AS MANUALS)

17. The Secretary and the CDF expect Defence personnel to comply with administrative policies unless particular circumstances warrant departure.

18. Some administrative policies support Defence personnel to comply with obligations that exist in:

- a. applicable laws
- b. the *Defence Enterprise Agreement*
- c. directives and determinations issued under the [Public Service Act 1999](#) and the [Defence Act 1903](#)
- d. Defence Instructions.

19. Defence personnel **must** not depart from an administrative policy in a way that would result in any breach of the obligations outlined in paragraph 17 above.

20. When considering a possible departure from an administrative policy, the Secretary and the CDF require Defence personnel to:

- a. consider whether a proposed departure is reasonable and justified in the circumstances and whether it will produce a better outcome for Defence
- b. consult their supervisor, wherever practicable, about a proposed departure – a properly informed decision also involves consulting the policy owner
- c. be responsible and accountable for the consequences of departing from, or not adhering to, the content of an administrative policy including where such departure or non-adherence results in a breach of applicable laws or leads to adverse outcomes for Defence.

21. Defence personnel may be subject to performance management, administrative action or, in some circumstances, disciplinary action where their decision to depart from an administrative policy involves serious errors of judgement.

UNINTENDED CONSEQUENCES FROM USING FRAMEWORK DOCUMENTS

22. Where Defence personnel consider the application of a particular [framework document](#) would produce an unintended or undesirable consequence, they should inform their supervisor about the issue to have the matter resolved with the policy owner.

23. Framework documents should not contain material that duplicates or is in conflict with material contained in another framework document. Mandatory provisions in this Instruction, an interim Instruction or an [accountable authority instruction](#) will prevail over provisions in a manual or policy.

KEY ROLES, FUNCTIONS AND RESPONSIBILITIES

SECRETARY OF DEFENCE AND THE CHIEF OF THE DEFENCE FORCE

24. The Secretary and the CDF:

- a. provide the highest level of authority for framework documents and
- b. appoint [accountable officers](#) who are members of the Enterprise Business Committee.

ACCOUNTABLE OFFICERS

25. [Accountable officers](#) are authorised to issue policies their domain. They are accountable to the Secretary and the CDF for ensuring that the policies in their [policy domain](#):
- a. remain coherent, integrated and current
 - b. are effectively implemented across Defence
 - c. provide appropriate policy coverage and guidance.
26. [Accountable officers](#) **must** ensure there are consultation and endorsement arrangements in place for developing, implementing, maintaining and reviewing administrative policies in their [policy domain](#).
27. The arrangements are to be appropriate for the purpose and context of each policy to ensure the intended policy outcomes can be achieved.
28. [Accountable officers](#) may appoint [policy owners](#) for each of the business functions in their respective [policy domain](#).

POLICY OWNERS

29. [Policy owners](#) are responsible to their [accountable officer](#) for:
- a. developing and maintaining [framework documents](#) that enable administrative objectives to be effectively implemented across Defence. This includes ensuring that appropriate consultation is undertaken and capability, resources, Group or Service management and any other policy implications, are considered
 - b. implementing administrative policies contained in framework documents on particular business functions
 - c. issuing administrative policies that relate to their particular business function, if authorised by their accountable officer to do so
 - d. monitoring and, where necessary, reporting on the implementation of administrative policies contained in framework documents.
30. Policy owners are not necessarily subject to the line management of the accountable officer of the [policy domain](#) to which their business function belongs.

FIRST ASSISTANT SECRETARY ENTERPRISE TRANSFORMATION AND GOVERNANCE

31. First Assistant Secretary Enterprise Transformation and Governance:
- a. is accountable to the Associate Secretary for managing the framework and its associated business processes
 - b. will assist [accountable officers](#) in ensuring administrative policies are fit for purpose and maintain the integrity of the framework
 - c. will monitor and report to accountable officers on the currency of framework documents according to their period of effect and the performance of the framework
 - d. will report to the Enterprise Business Committee as required on the performance of the administrative policy framework and seek approval for updated provisions in this Instruction.

GROUP HEADS AND SERVICE CHIEFS

32. Group Heads and Service Chiefs are responsible for:
- a. implementing administrative policies contained in [framework documents](#) within their relevant Group/Service
 - b. ensuring that arrangements (including adequate resourcing) are in place to enable Defence personnel to comply with the provisions specified in this Instruction and to enable Defence personnel to comply with administrative policy contained in other framework documents.

DEFINITIONS

Accountable officer. Is a member of the Enterprise Business Committee, appointed by, and accountable to, the Secretary and the Chief of the Defence Force for policies residing in their policy domain and the administrative policy framework documents that articulate those policies.

Administrative policy. Is a deliberate system of principles and rules to guide decisions and achieve rational outcomes. It is established to align corporate operations, set behavioural expectations, mitigate corporate risk and communicate policy roles and responsibilities beyond those attached to a job description or duty statement. Administrative policy:

- a. has long-term application to the organisation
- b. assists the organisation to reach its strategic goals and priorities
- c. promotes operational efficiency
- d. is consistent with applicable external legal requirements and policy

The implementation of administrative policy may be supported by a range of other material, including systems, procedures, guidance and information.

Administrative policy framework. It sets out the approach for developing, implementing and maintaining policies in Defence.

A person/s engaged under a contract. Is a contractor, consultant or outsourced service provider as defined in the Financial Delegations Glossary of Terms.

Australian Public Service employee. Is a person employed under the Public Service Act 1999.

Commander. Is an Australian Defence Force officer who, by virtue of a delegation or instrument of appointment, exercises authority and has responsibility for assigned Defence personnel and includes an administrative Commanding Officer.

Defence. Is the Department of Defence and the Australian Defence Force.

Defence civilian. As defined in section 3 of the Defence Force Discipline Act 1982, is a person (other than a Defence member) who:

- a. with the authority of an authorised officer as defined in the Defence Force Discipline Act 1982, accompanies a part of the Australian Defence Force that is outside Australia, or on operations against the enemy
- b. has consented, in writing, to subject themselves to Australian Defence Force discipline while so accompanying that part of the Australian Defence Force.

Defence locally engaged employee. Is any person engaged overseas by contract or under section 74 of the Public Service Act 1999.

DEFINITIONS

Defence member. As defined in the [Defence Force Discipline Act 1982](#), is a person who is:

- a. a member of the Permanent Navy, the Regular Army or the Permanent Air Force
- or
- b. a member of the Reserves who:
 - i. is rendering continuous full-time service
 - or
 - ii. is on duty or in uniform.

Defence personnel. Means all Australian Public Service employees in the Department of Defence, Defence locally engaged employees, Defence civilians, Defence members and the equivalents from other Defence organisations on exchange to Defence.

Defence-wide document. Is an administrative policy [framework document](#) that applies to Defence personnel in more than one Group or Service.

Framework documents. Are administrative policy documents that are part of the [administrative policy framework](#). They are: *Defence Instruction – Administrative policy*, [accountable authority instructions](#), interim Defence Instructions, and policies (including those known as manuals).

Manager. Means Defence personnel or a person/s engaged under a contract who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or perform the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Personal information. Is defined in the [Privacy Act 1988](#).

[Policy domain.](#) Means administrative policies that have been grouped together under one accountable officer due to their related content or business function.

[Policy owner.](#) Is a person appointed by an accountable officer to be responsible to that [accountable officer](#) for achieving effective policy outcomes for their particular business function and for effectively implementing policies contained in framework documents.

Provision. Is a condition or stipulation formally incorporated in a framework document.

DEFINITIONS

Sensitive information. Is defined in the [Privacy Act 1988](#)

Supervisor. Means Defence personnel or a person/s engaged under a contract who have direct or line supervisory responsibilities for Defence personnel.

Technical authority: Person or entity responsible for making arrangements and issuing policy for the technical regulation and management of a specified technical environment within Defence.

ACQUISITION AND SUSTAINMENT
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Capability Acquisition and Sustainment

THERE ARE NO PROVISIONS BELONGING TO THIS POLICY DOMAIN
CURRENTLY IN FORCE

SUBMISSIONS MEETING PARTICULAR CRITERIA OUTLINED ON [FACT SHEET 1](#)
CAN BE SUBMITTED TO THE [ADMINISTRATIVE POLICY TEAM](#) FOR
CONSIDERATION AND POSSIBLE INCLUSION IN
THE NEXT EDITION OF THIS INSTRUCTION

[VIEW POLICIES](#) BELONGING TO THIS DOMAIN

ADMINISTRATION AND GOVERNANCE
POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

Title:	AG4 – <i>Incident reporting and management</i> (AG4).
Object:	Incidents that impact on effectiveness and capability are to be reported, recorded and managed. AG4 prescribes and proscribes particular conduct relating to reporting, recording and managing incidents in Defence.
Policy owner:	First Assistant Secretary Defence Integrity
Policy contact:	Director Fraud Control
Cancellations:	NIL

AG4.1 Defence personnel who have a reasonable suspicion that an incident has occurred **must**, as soon as practicable but within 24 hours of commencement of duty, report the incident to their manager or commander.

AG4.2 The following exceptions apply to this mandatory reporting obligation:

- a. the incident is a notifiable incident and is reported directly to a Defence Investigative Authority
- b. a notifiable incident is reported directly to civilian police
- c. a disclosure of information about an incident is made under the [Public Interest Disclosure Act 2013](#)
- d. an incident that might affect a person's suitability to hold a security clearance is reported directly to the Australian Government Security Vetting Agency
- e. a complaint of unacceptable behaviour has already been made to the complainant's or respondent's manager
- f. disclosures made to chaplains that do not relate to serious criminal activity, imminent threat of self-harm or imminent harm to others.

AG4.3 A victim of physical violence or emotional trauma arising from a criminal act is exempt from the mandatory reporting requirements of AG4. However, the Secretary and the Chief of the Defence Force encourage them to report the incident.

AG4.4 In relation to incidents reported to them, managers and commanders **must**:

- a. as soon as practicable, but within 24 hours of commencement of duty, report all required information through their line management or chain of command
- b. report any notifiable incident immediately to a Defence investigative authority
- c. manage any incident until all actions are complete or responsibility for managing the incident has passed to an appropriate internal or external investigative authority

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

- d. record details of the reporting and management of incidents in the authorised case management system using a [Defence Incident Record](#).

AG4.5 The [Incident reporting and management manual](#) is a framework document. It outlines roles and responsibilities, procedural material and definitions. It is intended to be read in conjunction with AG4 as if it is part of AG4.

AG4.6 Subject to Australian law, AG4 is not intended to override or affect:

- a. potential legal privileges (including the privilege against self-incrimination)
- b. confidences (including restricted disclosures made in accordance with AG4 or any other Defence Instruction)
- c. disclosures of information made under the [Public Interest Disclosure Act 2013](#).

Defence Investigative Authority. Means the Directorate of Investigations and Recovery within the Fraud Control and Investigations Branch; the Joint Military Policing Unit; and the Directorate of Security Intelligence and Investigations within the Defence Security and Vetting Service.

Incident. Is any non-routine event or occurrence that may have an effect on Defence, in particular capability, operations, personnel, security, safety, reputation, property, premises, environment, legal and ethical obligations, obligations to minors, and foreign relations. To avoid doubt, it includes all complaints made by Defence personnel, a person/s engaged under a contract, people involved in Australian Defence Force cadets, and members of the public, where the complaint is about Defence (including complaints about Defence Personnel).

Notifiable incident means any incident that:

- a. raises a reasonable suspicion that a criminal offence may have been committed under the criminal law of the Commonwealth, States or Territories, or the criminal law of another country;
- b. raises a reasonable suspicion that a serious offence has been committed under the [Defence Force Discipline Act 1982](#), not including incidents that are regarded as minor (Schedule 1A offences), which would ordinarily be dealt with by a subordinate summary authority or under the [discipline officer scheme](#) (noting that, if found to be more serious than initially determined, it may need to be reported as a notifiable Incident);
- c. involves allegations of fraud, corrupt practices or behaviour, collusive tendering, conflict of interest or a lack of probity involving Commonwealth resources, including personnel, property or premises;
- d. is a suspected security incident (excluding minor security incidents), whether intentional, negligent or accidental, resulting in a failure to comply with a security

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

requirement outlined in the [Defence Security Principles Framework](#) or that may impact on a clearance holder's suitability to hold a security clearance;

- e. involves the death, serious injury (including self-harm) or disappearance of Defence personnel or the death, serious injury or disappearance of non-Defence personnel, involved in any Defence activity, or at any Defence property or premises (even where there may be no reasonable suspicion of an offence having been committed)
- or
- f. is an incident deemed by a manager or a commander to be serious, sensitive or urgent, not covered by the definitions above. That is, one that may bring Defence into disrepute; attract adverse media or parliamentary attention; or may adversely affect the efficiency of Defence, or impact on operational effectiveness or capability.

ADMINISTRATION AND GOVERNANCE
POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

Title:	AG5 – <i>Conflicts of interest and declarations of interest</i> (AG5).
Object:	AG5 prescribes and proscribes conduct relating to declaring, recording and managing conflicts of interest in Defence.
Policy owner:	First Assistant Secretary Defence Integrity
Policy contact:	Director Fraud Control
Cancellations:	NIL

AG5.1 All Defence personnel **must**:

- a. take reasonable steps to avoid any conflicts of interest (actual, potential or perceived) in connection with their official duties
- b. disclose any conflict of interest in writing as and when it is identified in the following manner:
 - i. Non Senior Executive Service personnel and non star ranked personnel **must** make this disclosure to their Branch Head or One Star through their manager
 - ii. Senior Executive Service and Star Ranked personnel with a conflict of interest **must** raise this directly with their Group Head or Service Chief
- c. act transparently when making work-related decisions, reflecting the probity and ethical standards of the Commonwealth and Defence, including Australian Public Service Values and Defence Values and Behaviours
- d. take reasonable steps to restrict the extent to which a private interest could compromise, or be seen to compromise, their impartiality when carrying out their official duties
- e. report to their manager or commander as soon as practicable, but before accepting, any offer of post separation employment that could lead to a conflict of interest.

AG5.2 Defence personnel **must not**, either by action or inaction:

- a. make improper use of their authority, status, power, position or access to information in order to solicit or obtain a benefit or advantage, or to cause a disadvantage, for themselves or any other person or group (including partners, relatives, friends, associates and any person that does or may do business with Defence)
- b. use Defence resources to gain, or seek to gain, a private benefit or advantage or to cause a disadvantage for themselves or any other person or group

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

- c. accept any benefit that might lead a reasonable person to view such acceptance as a conflict of interest
- d. behave in a manner in which their action or inaction could be construed as favouritism, bias or coercion
- or
- e. take improper advantage of their official position or privileged information gained in that position when seeking or participating in employment, business or other activities outside of Defence.

AG5.3 Defence personnel **must** consider possible strategies that may be available to resolve or appropriately manage the conflict of interest. Defence personnel **must** cooperate with their Branch Head or One Star to resolve the conflict of interest.

AG5.4 Defence personnel **must** report situations where their partners, family, friends and associates are engaged in activities or have interests that place Defence personnel in an actual, potential or perceived conflict of interest situation.

AG5.5 Defence personnel who award or manage contracts should be aware that a conflict of interest can arise at any stage of a procurement activity. Conflicts of interest identified by Defence personnel, person/s engaged under a contract, and potential suppliers at the time of tendering and during a tender evaluation process **must** be documented and appropriately managed. The delegate for a procurement activity **must** be notified immediately of any conflicts of interest that could affect the integrity of a procurement process.

AG5.6 If the conflict of interest occurs in relation to an existing contract, Defence personnel and person/s engaged under a contract **must** also report this conflict to the contract manager.

AG5.7 Branch Heads and One Stars or Group Heads and Service Chiefs **must** assess each situation reported to them and determine if a conflict of interest exists as soon as is practicable. They **must** promptly decide on an appropriate strategy to manage the situation and retain appropriate records of the facts surrounding the conflict of interest and the process adopted to manage it. Branch Heads and One Stars **must** bring any serious conflicts of interest involving Defence personnel within their chain of command or Branch to the attention of their Group Head or Service Chief.

AG5.8 If the conflict of interest is serious, continues indefinitely or is unresolved, Branch Heads and One Stars or Group Heads and Service Chiefs **must** seek advice from the First Assistant Secretary Audit and Fraud Control.

AG5.9 If a suspected conflict of interest has been reported by a third party, the Branch Head and One Star or the Group Head and Service Chief **must** after consultation with any investigative authority advise the affected individual that a

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

report has been made. The affected individual **must** have the opportunity to respond to the report.

AG5.10 If notified of a post separation employment conflict of interest, Branch Heads and One Stars **must** determine whether a letter of notification is required. Where required, Branch Heads and One Stars **must** ensure the letter of notification is submitted to the appropriate decision maker, who is at least one level above the Defence personnel submitting the notification and no lower than a One Star or SES Band 1.

AG5.11 Group Heads and Service Chiefs **must** bring any serious conflicts of interest, and any conflict of interest involving themselves, to the attention of the Secretary or Chief of the Defence Force (CDF), respectively.

AG5.12 Annual Declarations of Interest **must** be provided by:

- a. members of the Senior Leadership Group (SLG) including all Star Ranked Officers, all Star Ranked Reserve Officers who are SERCAT 3, 4 or 5, Senior Executive Service Officers, Medical Officers Class 5 and 6, and Chiefs of Divisions
- b. other positions in which the level of decision making or advice is deemed by a Group Head or Service Chief as being equivalent to that of the SLG
- c. anyone acting in one of the above positions
- and
- d. anyone below SLG level who is designated by their Group Head or Service Chief because their responsibilities require them to be particularly transparent about their financial and personal interests.

AG5.13 All newly appointed SLG members **must** submit a Declaration of Interest within one-month of taking up their appointment.

AG5.14 Group Heads and Service Chiefs **must** identify Defence personnel occupying positions (other than SLG positions) who will be required to provide Declarations of Interest.

AG5.15 SLG members and Defence personnel acting in SLG positions **must** submit their declarations to their Group Head or Service Chief. Declarations made by Group Heads, Service Chiefs **must** be submitted to the Secretary or the CDF through the Directorate of Senior Officer Management (DSOM). Declarations of Interest **must** be revised and resubmitted by personnel throughout the year where there is a change in responsibilities or personal circumstances that could impact upon their official duties.

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

AG5.16 The day-to-day management of conflicts of interest is the responsibility of all Defence personnel, managers and commanders, contract managers, procurement panels and procurement delegates.

AG5.17 [The Integrity Policy Manual](#) is an administrative policy framework document. It contains policies, procedures and outlines situations that may give rise to a conflict of interest. It also describes additional roles and responsibilities associated with managing declarations of interest. It enables Defence personnel to comply with AG5. The Integrity Policy Manual is intended to be read in conjunction with AG5.

Conflict of interest refers to any situation where there is, or may appear to be, a conflict between an individual's personal interests and their public duties and responsibilities.

ADMINISTRATION AND GOVERNANCE
POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

Title:	AG7 – <i>Legal Services in Defence</i> (AG7)
Object:	AG7 outlines the arrangements for the provision of all legal advice in Defence and when Defence personnel must engage with Defence Legal.
Policy owner:	Chief Counsel
Cancellations:	NIL

Delivery of Legal Services in Defence

AG7.1 The Chief Counsel is authorised to exercise technical control over the provision of legal advice in Defence. Legal advice includes the legal review and clearance of documents.

AG7.2 The Chief Counsel permits certain Defence personnel (for the purposes of this Instruction ‘Defence Legal Practitioners’) to provide legal advice on his/her behalf only if they hold the following essential qualifications:

- a. a practising certificate issued by an Australian State or Territory (unless the Chief Counsel provides an exemption)
- b. a written approval issued by the Chief Counsel.

AG7.3 Defence personnel **must not** provide legal advice to Defence unless permitted to do so by the Chief Counsel in accordance with AG7.2.

AG7.4 Defence personnel **must** only procure legal advice and legal services, including from external legal providers, through Defence Legal.

AG7.5 Defence personnel **must not** interfere with the ability of Defence Legal Practitioners or external legal service providers to give independent legal advice. This includes attempting to improperly influence the outcome of legal advice or acting in a way that abrogates from appropriate management of legal risk.

Mandatory engagement with Defence Legal

AG7.6 Defence personnel and, where it is a term of their contract, a person(s) engaged under a contract, **must** engage Defence Legal in relation to:

- a. any matter, decision or activity that involves:
 - i. constitutional law issues
 - ii. non-compliance with the [Legal Services Directions 2017](#)
 - iii. public international law issues

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

- iv. the drafting, negotiation, or interpretation of an international government-to-government agreement or arrangement¹
- v. the study, development, adoption or acquisition of new or materially modified weapons, means and methods of warfare
 - 1. This includes all formal decision gates for any planned study, development, adoption or acquisition
 - 2. A new or materially modified weapon, means and method of warfare **must** be legally reviewed before introduction into service²
- vi. Intellectual property policy and practice
- vii. actual or likely litigation against Defence
- viii. the occurrence of an act, omission, accident, incident or error that is likely to result in legal proceedings being brought against the Commonwealth
- ix. an order, notice or request to provide Defence documentation to, or appear before, a civilian court, tribunal or enforcement body (such as a subpoena or Notice to Produce)
- x. legal risks that are assessed as high or extreme legal risk
- b. a project or activity where:
 - i. the endorsed Defence contracting template would normally be used but is not used
 - ii. the endorsed Defence contracting template would normally be used but is modified in any material respect, including modifications to clauses that concern contractor default, indemnities, limitations of liability, warranties, financial or performance securities or guarantees, insurances or liquidated damages
 - iii. the procurement of products or services outside the ordinary services and functions of government is proposed and requires legislative authority

¹ Refer to the [Defence International Agreements and Arrangements Instruction Guide](#) for further detail.

² Refer to the [Defence Legal Review of New Weapons Guide](#) for further detail.

ADMINISTRATION AND GOVERNANCE POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

- iv. a contingent liability, financial liability or complex and potentially costly indemnity is proposed
- v. there is a proposed termination of a contract, waiver or standstill of contractual rights or exercise of other contractual remedy, either as a consequence of contractor breach or by agreement
- vi. a contractor is subject to any change of control, either as a result of a takeover or some other form of sales process
- vii. a complaint has been received under the [Government Procurement \(Judicial Review\) Act 2018](#) and it is known that the complainant has engaged a law firm to represent them
- viii. a Public Interest Certificate is proposed to be issued under the [Government Procurement \(Judicial Review\) Act 2018](#)
- c. claims for compensation arising from defective administration and requests for act of grace
- d. matters relating to new legislation or legislative amendments including:
 - i. proposals to develop or amend Defence administered legislation
 - ii. engaging the Office of Parliamentary Counsel to draft bills or legislative instruments
 - iii. Defence input to reviews or amendments of other Commonwealth legislation
- e. the legal review of a Defence Inquiry conducted under the Defence (Inquiry) Regulations 2018
- f. the exercise of a delegation to approve financial assistance to an official for legal proceedings
- g. any other matters as identified in other extant policy as requiring consultation or engagement with Defence Legal.

ADMINISTRATION AND GOVERNANCE
POLICY DOMAIN PROVISIONS

Accountable officer – Associate Secretary

AG7.7 This Instruction **must**, where relevant, be read in conjunction with the:

- a. [Defence Legal Review of New Weapons Guide](#)
- b. [Defence International Agreements and Arrangements Instruction Guide](#).

AG7.8 This Instruction is not to be interpreted as limiting any other matters that **must** be referred to, or require engagement with, Defence Legal.

AG7.9 Risk owners are to use sound judgement at all times to ensure that the Chief Counsel, as the accountable officer for legal services in Defence, is made aware of legal risks and consulted as appropriate in the management of legal risk.

STRATEGY, POLICY, AND INDUSTRY
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Strategy, Policy, and Industry

THERE ARE NO PROVISIONS BELONGING TO THIS POLICY DOMAIN
CURRENTLY IN FORCE

SUBMISSIONS MEETING PARTICULAR CRITERIA OUTLINED ON [FACT SHEET 1](#)
CAN BE SUBMITTED TO THE [ADMINISTRATIVE POLICY TEAM](#) FOR
CONSIDERATION AND POSSIBLE INCLUSION IN
THE NEXT EDITION OF THIS INSTRUCTION

[VIEW POLICIES](#) BELONGING TO THIS DOMAIN

SECURITY AND ESTATE POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Security and Estate

Title:	SE1 - <i>Defence Security Principles Framework</i> (SE1)
Object:	AG1 prescribes conduct with respect to risk controls identified in level 4c of the <u>Defence Security Principles Framework</u> . Risk controls are necessary to enable Defence to effectively manage security risk and protect its people, information and assets from threats.
Policy owner:	First Assistant Secretary Defence Security
Policy contact:	Assistant Secretary Security Policy and Services
Cancellations:	NIL

SE1.1 Defence personnel and – where it is a term of their contract – a person/s engaged under a contract, **must** comply with the *Principles and Controls* of the [Defence Security Principles Framework](#) unless a policy variation is granted by the designated officer or entity in accordance with defined risk thresholds.

SE1.2 Defence personnel and – where it is a term of their contract – a person/s engaged under a contract **must** comply with the mandatory provisions of the [Defence Security Principles Framework](#) described through the words ‘**must**’ and ‘**must not**’ unless a dispensation is granted by the relevant Control Owner.

SE1.3 Documents that are part of the [Defence Security Principles Framework](#) are administrative policy framework documents. They outline principles, expected outcomes, procedures and guidance that enable Defence to meet its security obligations under the Australian Government’s [Protective Security Policy Framework](#). Documents that are part of the [Defence Security Principles Framework](#) is to be read in conjunction with SE1 as if it is part of SE1.

SE1.4 AGSVA may collect Sensitive Information from a Referee about a Clearance Subject without obtaining the Clearance Subject’s consent provided:

- a. it is unreasonable or impracticable for AGSVA to obtain the Clearance Subject’s consent; and
- b. AGSVA is reasonably satisfied that to collect the Sensitive Information in the absence of the Clearance Subject’s consent will significantly promote AGSVA’s Core Function

SE1.5 If AGSVA collects Sensitive Information in accordance with paragraph SE1.4, AGSVA **must** make a written record of the event, which **must** include reasons for the collection without consent.

SE1.6 Paragraph SE1.4 is made for the purposes of APP3.4(a) in Schedule 1 to the *Privacy Act 1988*.

SECURITY AND ESTATE POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Security and Estate

SE1.7 Paragraph SE1.4 is subject to any limiting provision in the PSPF. In the event of an inconsistency between paragraph SE1.4 and the PSPF, the PSPF will prevail to the extent of the inconsistency.

SE1.8 AGSVA may disclose Personal Information collected from a Referee to another Referee about a Clearance Subject without obtaining the Clearance Subject's consent provided:

- a. it is unreasonable or impracticable for AGSVA to obtain the Clearance Subject's consent; and
- b. AGSVA is reasonably satisfied that to disclose the Sensitive Information in the absence of the Clearance Subject's consent will significantly promote AGSVA's Core Function

SE1.9 If AGSVA discloses Sensitive Information in accordance with paragraph SE1.8, AGSVA **must** make a written record of the event, which **must** include reasons for the disclosure without consent.

SE1.10 Paragraph SE1.8 is made for the purposes of APP6.2(b) in Schedule 1 to the *Privacy Act 1988*.

SE1.11 Paragraph SE1.8 is subject to any limiting provision in the PSPF. In the event of an inconsistency between paragraph SE1.8 and the PSPF, the PSPF will prevail to the extent of the inconsistency.

For the purpose of SE1:

AGSVA means the Australian Government Security Vetting Agency, being the branch of Defence Security Division that provides independent security clearance vetting services and advice to non-exempt government agencies, including Defence, in accordance with the PSPF.

AGSVA's Core Function means AGSVA's function of Vetting in relation to personnel who have, or who are intended to have, access to Australian Government resources (people, information and assets), in accordance with Chapter 12 – *Eligibility and suitability of personnel* of the PSPF

APP means 'Australian Privacy Principle' within the meaning of the [Privacy Act 1988](#)

Clearance Subject means an individual whose eligibility and suitability to hold a Security Clearance is being assessed.

Personal Information means "personal information" as defined in the [Privacy Act 1988](#) (which includes Sensitive Information)

SECURITY AND ESTATE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Security and Estate

PSPF means the [Protective Security Policy Framework](#)

Referee means a person who is interviewed by AGSVA in connection with Vetting, who knows the Clearance Subject and can supply AGSVA with relevant information about the Clearance Subject.

Security Clearance means a determination by AGSVA that an individual is eligible and suitable to access security classified information and assets.

Sensitive Information means “sensitive information” as defined in the [Privacy Act 1988](#)

Vetting means the process of checking and assessing a Clearance Subject’s eligibility and suitability to hold a security clearance at a specified level.

FINANCE
POLICY DOMAIN PROVISIONS

Accountable officer – Chief Finance Officer

PARAGRAPH 14 OF THIS INSTRUCTION REFERS TO ACCOUNTABLE
AUTHORITY INSTRUCTIONS (AAIs).

[VIEW AAIs AND FINANCE POLICIES](#)

INFORMATION AND COMMUNICATIONS TECHNOLOGY
POLICY DOMAIN PROVISIONS

Accountable officer – Chief Information Officer

THERE ARE NO PROVISIONS BELONGING TO THIS POLICY DOMAIN
CURRENTLY IN FORCE

SUBMISSIONS MEETING PARTICULAR CRITERIA OUTLINED ON [FACT SHEET 1](#)
CAN BE SUBMITTED TO THE [ADMINISTRATIVE POLICY TEAM](#) FOR
CONSIDERATION AND POSSIBLE INCLUSION IN
THE NEXT EDITION OF THIS INSTRUCTION

[VIEW POLICIES](#) BELONGING TO THIS DOMAIN

MILITARY COMMAND SUPPORT POLICY DOMAIN PROVISIONS

Accountable officer – Vice Chief of the Defence Force

Title:	MCS1 – <i>Defence seaworthiness management system</i> (MCS1)
Object:	The Defence seaworthiness management system is intended to regulate for, and assure achievement of, the seaworthiness outcome. The seaworthiness outcome is to maximise the likelihood of delivering the intended operational effect where risks to personnel, public and environment have been eliminated or minimised so far as is reasonably practicable. The objects of MCS1 are to appoint the Defence Seaworthiness Authority and to define the powers and functions of the Defence Seaworthiness Authority.
Policy owner:	Chief of Navy
Policy contact:	Defence Seaworthiness Regulator
Cancellations:	NIL

MCS1.1 The Secretary and the Chief of the Defence Force appoint the Chief of Navy as the Defence Seaworthiness Authority.

MCS1.2 The Defence Seaworthiness Authority **must** establish and implement the Defence seaworthiness management system.

MCS1.3 To effectively assure the delivery and management of seaworthiness by the regulated community, the Defence Seaworthiness Authority is authorised to direct all Defence personnel whose duties involve activities in support of the maritime environment.

MCS1.4 The [*Defence seaworthiness management system manual*](#) is an administrative policy framework document. It contains policies and procedures relating to associated roles and responsibilities and definitions that should be read in conjunction with MCS1.

MCS1.5 The Defence Seaworthiness Authority appoints the Head of Navy Engineering as the Defence Seaworthiness Regulator.

MCS1.6 The Defence Seaworthiness Regulator is required to act as the Regulator of the Defence seaworthiness management system.

MILITARY COMMAND SUPPORT POLICY DOMAIN PROVISIONS

Accountable officer – Vice Chief of the Defence Force

Title:	MCS2 – <i>Defence Landworthiness</i> (MCS2)
Object:	The Defence Landworthiness Authority is intended to regulate for, and assure achievement of, a defined operational state for land capability systems and force elements. In a landworthy capability, the fundamental inputs to capability are synchronised, and are likely to remain so for the review period. In this state, the Land Capability System can interface or is integrated with other Defence capabilities. Risks have been appropriately assessed and are balanced across risk domains and the risks are the lowest that they can be, so far as is reasonably practicable. The objects of MCS2 are to appoint the Defence Landworthiness Authority and to define the powers and functions of the Defence Landworthiness Authority.
Policy owner:	Chief of Army
Policy contact:	Defence Landworthiness Regulator
Cancellations:	NIL

MCS2.1 The Secretary and the Chief of the Defence Force appoint the Chief of Army as the Defence Landworthiness Authority.

MCS2.2 The Defence Landworthiness Authority **must** establish and implement the Defence Landworthiness Management System.

MCS2.3 To effectively assure the delivery and management of land capability by the regulated community, the Defence Landworthiness Authority is authorised to direct all Defence personnel whose duties involve activities in support of the Joint Land Force.

MCS2.4 The [Defence Landworthiness Policy](#) is an administrative policy framework document. It contains the principles and regulations relating to associated roles and responsibilities and definitions that should be read in conjunction with MCS2.

MILITARY JOINT ENABLING POLICY DOMAIN PROVISIONS

Accountable officer – Chief of Joint Capabilities

Title:	MJE1 – <i>Disclosure of certain personal information in relation to youth protection incidents</i> (MJE1)
Object:	As a youth-safe organisation, MJE1 is one of the elements necessary to protect the health, wellbeing, interests and safety of young people. It provides for circumstances in which it may be appropriate for Defence personnel to disclose personal information in relation to youth protection incidents.
Policy owner:	Head Joint Support Services Division
Policy contact:	Director Youth
Cancellations:	NIL

MJE1.1 Defence personnel **must** protect the health, wellbeing, interests and safety of young people.

MJE1.2 Defence personnel are authorised to disclose personal information held by Defence about a young person under the age of 16 to their parent or a Responsible Third Person, if:

- a. the young person has been involved in a Youth Protection Incident, and
- b. it is reasonably believed necessary in the circumstances for the purposes of lessening or preventing a serious threat to life, health or safety of young person.

MJE1.3 Factors that may be relevant when deciding whether to release personal information include, but are not limited to:

- a. the young person's level of competence
- b. any wishes expressed by the young person
- c. the nature of the personal information, and/or
- d. the nature of the Youth Protection Incident.

MJE1.4 Defence personnel are authorised to disclose personal information held by Defence about any young person if:

- a. there is a Commonwealth, State or Territory legislative requirement to report certain matters to a Government oversight agency or enforcement body (the reporting requirement), or
- b. the disclosure of certain information is required by a Court or tribunal order, and
- c. all of the conditions or criteria required by subparagraph (a) or (b) are satisfied.

MILITARY JOINT ENABLING POLICY DOMAIN PROVISIONS

Accountable officer – Chief of Joint Capabilities

MJE1.5 Except as required by MJE1.4, Defence personnel must **not** disclose personal information about a young person 16 years of age or older to their parent, Responsible Third Person or any other person unless:

- a. it is unreasonable or impracticable to obtain the young person's consent, and
- b. it is reasonably believed necessary for the purposes of lessening or preventing a serious threat to life, health or safety of an individual (or to public health or safety)

Definitions

- a. **Youth Protection Incident** means any incident of unacceptable behaviour/sexual misconduct, as defined in the Youth Safe Code of Conduct policy, which adversely affected or had the potential to adversely affect the health, protection or wellbeing of a youth(s).
- b. **Responsible Third Person** includes a guardian or a person in the position of a parent

MJE1.6 Defence personnel who award contracts on behalf of the Commonwealth are **not** authorised to include in the terms of a contract the requirement for a person/s engaged under a contract, to comply with MJE1.

MJE1.7 The [Youth Policy Manual](#) is a framework document. It contains policy and procedural material and definitions that should be read in conjunction with MJE1.

MJE1.8 Other related material can be accessed in [Good decision-making in Defence: A guide for decision-makers and those who brief them](#).

MJE1.9 Defence privacy policy contains relevant policy regarding issues that are not related to youth protection incidents.

MILITARY JOINT ENABLING
POLICY DOMAIN PROVISIONS

Accountable officer – Chief of Joint Capabilities

Title:	MJE2 – <i>Defence health policy</i> (MJE2)
Object:	The Secretary and the Chief of the Defence Force are committed to ensuring quality health care is provided to Defence members and Defence civilians. MJE2 is one of the tools necessary to support the health preparedness of Defence for operations and in support of operations.
Policy owner:	Surgeon General Australian Defence Force
Policy contact:	Joint Health Command
Cancellations:	NIL

MJE2.1 The Surgeon General Australian Defence Force is authorised to exercise technical authority for all health matters across the Australian Defence Force. The Surgeon General Australian Defence Force is also the authoritative source of strategic health advice across Defence.

MJE2.2 The Surgeon General Australian Defence Force is authorised to approve a Defence scope of practice for an individual Defence health practitioner or for a class of Defence health practitioners. The Defence scope of practice defines the range of services a Defence health practitioner may provide to Defence members, which may be more or less than the scope of practice available to that practitioner outside Defence. Defence health practitioners are authorised to provide health treatment to Defence members in accordance with a Defence scope of practice. Pursuant to section 49 of [Defence Regulation 2016](#) treatment of a Defence member (rendering continuous full time service) in accordance with a Defence scope of practice is not required to comply with a law of a state or territory. The Defence scope of practice approved in writing by the Surgeon General Australian Defence Force, or appointed delegate, may be varied or revoked. A Defence scope of practice may:

- a. apply indefinitely or for a fixed period of time
- b. be unconditional or subject to conditions.

MJE2.3 Defence health practitioners are authorised to supply pharmaceuticals and conduct associated activities, for the purposes of providing medical and dental treatment to Defence members in accordance with the [Defence health manual](#). Defence personnel and Defence health practitioners are authorised to collect, use and disclose health information about Defence members in accordance with MJE2 and Vol 1, Part 3, Chapter 1 of the [Defence health manual](#). Defence health practitioners **must** inform the manager or commander of a Defence member of any limitations known to the Defence health practitioner on the fitness of the Defence member to perform their duties.

MJE2.4 A Defence member who accesses a health service not provided on behalf of Defence **must** inform a Defence health practitioner.

MILITARY JOINT ENABLING
POLICY DOMAIN PROVISIONS

Accountable officer – Chief of Joint Capabilities

MJE2.5 Health information about a Defence member may be disclosed to a responsible person for the Defence member to enable appropriate care or treatment if the Defence member is incapable of giving consent.

MJE2.6 Volume 1 of the [*Defence health manual*](#) is a framework document. It contains policies, procedures and definitions that should be read in conjunction with MJE2.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL1 – <i>Authority in an integrated Defence workplace</i> (PPL1)
Object:	PPL1 prescribes conduct with respect to supervisory relationships in Defence workplaces. It is one of the tools necessary to promote productive supervisory relationships in an integrated Defence workplace.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director Military People Policy
Cancellations:	NIL

PPL1.1 In a Defence workplace, the duties of an Australian Public Service (APS) employee may place them under the supervision of a Defence member. APS employees **must** comply with all lawful and reasonable directions given by their supervisor that relate to the carrying out of functions within the responsibility of that supervisor.

PPL1.2 In a Defence workplace, Defence members whose posting or duties place them under the supervision of an APS employee **must** comply with all lawful and reasonable directions given by their supervisor that relate to the carrying out of functions within the responsibility of that supervisor.

PPL1.3 In a Defence workplace, APS employees in Defence **must** cooperate with a Defence member carrying out an inquiry under the *Defence (Inquiry) Regulations 2018* in circumstances where the inquiry officer reasonably suspects that the APS employee can make a material contribution to the inquiry as a witness.

PPL1.4 In a Defence workplace, Defence personnel **must** cooperate with a Manager, or Defence personnel acting as a Manager's agent, carrying out fact finding into a matter concerning the Manager's area of responsibility, in circumstances where the Manager or Manager's agent reasonably suspects that the Defence personnel can make a material contribution to the inquiry as a witness.

For the purpose of PPL1:

Defence workplace. Means any of the following that are owned or occupied (whether permanently or temporarily) by the Commonwealth for use by Defence:

- a. an area of land or any other place (whether or not it is enclosed or built on)
 - b. a building or other structure, in part or in whole
 - c. any platform, vehicle, air or seagoing vessel including any fixed or moveable ramp stairs or other means of access to, or exit from the platform, vehicle, vessel or aircraft
- or
- a prohibited area, within the meaning of the [*Defence \(Special Undertakings\) Act 1952*](#).

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Cooperate means to assist:

- a. the Defence member carrying out an inquiry under the *Defence (Inquiry) Regulations 2018*
or
- b. the Manager, or Defence personnel acting as a Manager's agent, carrying out fact finding,
(as the case may be), with their lawful and reasonable requests including by:
- c. attending an interview appointment at a specified place and time
- d. participating in the interview by answering relevant questions
producing a relevant document or thing at a specified place within a specified period,
or by a specified means within a specified period.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL2 - <i>Disclosure of certain personal information in relation to the Department of Veterans' Affairs and the Commonwealth Superannuation Corporation</i> (PPL2)
Object:	PPL2 is one of the tools necessary to allow Defence to work cooperatively with the Department of Veterans' Affairs and the Commonwealth Superannuation Corporation. This relationship allows care and support to be delivered to current and eligible former Defence members and their families.
Policy owner:	Head People Capability
Policy contact:	Director General Veterans' Support
Cancellations:	NIL

PPL2.1 Defence personnel are authorised to disclose personal information held by Defence about a Defence member to the Department of Veterans' Affairs and the Commonwealth Superannuation Corporation in certain circumstances.

PPL2.2 Defence personnel are **not** authorised to disclose sensitive information to the Department of Veterans' Affairs or the Commonwealth Superannuation Corporation.

PPL2.3 The [*Military personnel policy manual*](#) Part 7 Chapter 9, *Disclosure of certain personal information to the Department of Veterans' Affairs and the Commonwealth Superannuation Corporation* is an administrative policy framework document. It should be read in conjunction with PPL2. It contains:

- a. details regarding certain circumstances in which disclosures are authorised in accordance with PPL2
- b. information authorised to be disclosed and mechanisms for, and timings of, disclosures in accordance with PPL2
- and
- c. definitions that are specific to PPL2.

PPL2.4 Defence personnel who award contracts on behalf of the Commonwealth are not authorised to include in the terms of a contract the requirement to comply with PPL2.

For the purpose of PPL2 Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL3 – <i>Alcohol testing in the Australian Defence Force</i> (PPL3)
Object:	The object of PPL3 is to establish a regime for alcohol testing in the Australian Defence Force.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director Military People Policy
Cancellations:	NIL

PPL3.1 Defence members, Defence civilians and members of foreign Defence forces serving with Defence (where alcohol testing is permitted within an international agreement or arrangement) **must** maintain a zero percent blood alcohol concentration while on duty in, or visiting a safety critical area.

PPL3.2 Where it is a term of their contract - a person/s engaged under a contract, **must** maintain a blood alcohol concentration of zero percent while in a safety critical area. Where it is a term of their contract – a person/s engaged under a contract, **must** meet the requirements of PPL3.

PPL3.3 Defence members, Defence civilians and members of foreign Defence forces serving with Defence (where alcohol testing is permitted within an international agreement or arrangement) **must**, when directed to do so by an authorised person, undergo alcohol testing and provide a sufficient test sample.

PPL3.4 Refusing to undergo testing or failing to provide a sufficient test sample may be considered an offence under section 29 of the [Defence Force Discipline Act 1982](#). This may also lead to issue of a termination notice under subsection 24(1) of the [Defence Regulation 2016](#).

PPL3.5 Defence personnel who are nominated by a testing authorising officer and meet the prescribed training requirements of [Military personnel policy manual](#), Part 4, Chapter 2 are authorised to conduct alcohol testing on Defence members, Defence civilians and members of foreign Defence forces serving with Defence (where alcohol testing is permitted within an international agreement or arrangement).

PPL3.6 Defence personnel are authorised to collect, use and disclose personal information, including sensitive information, for official purposes relating to the alcohol testing program, including (but not limited to) the:

- a. administration of testing
- b. administration and management of actions to be taken following testing by the testing personnel and command
- c. management and analysis of the testing program
- d. statistical reporting of the testing program

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

- e. medical treatment or rehabilitation of a Defence member, Defence civilian or foreign Defence personnel concerned
- f. disclosure of personal and sensitive information about a member of a foreign Defence force to an overseas recipient, being their parent Defence force.

PPL3.7 The [Military personnel policy manual](#), Part 4 Chapter 2, *Alcohol testing in the Australian Defence Force* is an administrative policy framework document. It should be read in conjunction with PPL3. It details the authorisations, roles, responsibilities and requirements associated with alcohol testing in the Australian Defence Force. It also contains definitions that are specific to PPL3.

For the purpose of PPL3:

Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Zero percent blood alcohol concentration means blood alcohol concentration readings below 0.02 percent.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL4 – <i>Management of the use of prohibited substances in the Australian Defence Force</i> (PPL4)
Object:	The object of PPL4 is to establish the prohibited substance testing program in the Australian Defence Force.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director Military People Policy
Cancellations:	NIL

PPL4.1 Defence members and Defence civilians **must not** inappropriately use or involve themselves with prohibited substances. This behaviour is unacceptable and will not be tolerated by the Secretary and the Chief of the Defence Force because it reduces the capability of the Australian Defence Force.

PPL4.2 Defence members and Defence civilians **must**, in accordance with section 94 of the [Defence Act 1903](#), undergo a prohibited substance test if required to do so by an authorised person. Failing to provide a sufficient specimen or sample, or failing to undergo a screening test is an offence under section 106 of the [Defence Act 1903](#) and section 29 of the [Defence Force Discipline Act 1982](#). These offences may also lead to the issue of a termination notice under subsection 24(1) of the [Defence Regulation 2016](#).

PPL4.3 If the authorised person is satisfied that the presence of any prohibited substance revealed by testing was wholly attributable to substances administered by or taken at the direction or recommendation of:

- a. a medical practitioner registered with the [Medical Board of Australia](#)
- b. an [Australian Health Practitioner Regulation Agency](#) registered health professional who, under section 94 of the *Health Practitioners Regulation National Law Act 2009*, is registered, in a health profession for which their National Board is established, as being qualified to administer, obtain, possess, prescribe, sell, supply or use a scheduled medicine or class of scheduled medicines

or

- c. Defence endorsed person for the prescribing or dispensing of medication (i.e. Defence pharmacists, dentists, nurse practitioners, medical assistants, overseas medical practitioner etc)

the authorised person **must** disregard the positive test result.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

PPL4.4 Testing of hair, saliva or urine samples for prohibited substances **must** be undertaken by an accredited laboratory.

PPL4.5 The [Military personnel policy manual](#), Part 4 Chapter 3, *Management of the use of prohibited substances in the Australian Defence Force* is an administrative policy framework document. It should be read in conjunction with PPL4. It details the authorisations, roles, responsibilities and requirements associated with the prohibited substance testing program. It also contains definitions that are specific to PPL4.

For the purpose of PPL4:

An **accredited laboratory** is a laboratory accredited by the [National Association of Testing Authorities, Australia](#) (NATA) and identified, from time to time, on the NATA internet site through the “Find Accredited Facilities” functionality. It is an accredited laboratory for the purposes of Section 93 of part VIIIA of the [Defence Act 1903](#).

An **authorised person** is a person who have been appointed by the Chief of the Defence Force under section 93A of the [Defence Act 1903](#) as an authorised person or who under subsection 116M(1) and subsection 120A(3D) have been delegated the powers of an authorised person under the [Defence Act 1903](#), Part VIIIA, section 93A.

Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL5 – <i>Disclosure of certain personal information to foreign entities</i> (PPL5)
Object:	PPL5 authorises Defence personnel to disclose certain personal information relating to activities involving Defence members overseas to overseas entities.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director Military People Policy
Cancellations:	Nil

PPL5.1 Defence personnel are authorised to disclose personal information about Defence personnel (except those with Protected Identity Status) to an overseas recipient, if:

- a. Defence personnel are undertaking, or are scheduled to undertake:
 - i. personnel exchanges
 - ii. exercises, deployments
 - iii. third-country deployments
 - iv. placements
 - v. training
 - or
 - vi. visits with foreign forces, governments or a person/s engaged under a contract
- and
- b. the disclosure of that information is reasonably necessary to facilitate, manage or administer such activities.

PPL5.2 Defence personnel are authorised to disclose to an overseas recipient personal information about Defence personnel (except those with Protected Identity Status) involved, directly or indirectly, with the acquisition, sustainment or use of Defence equipment and capabilities if the disclosure is reasonably necessary to facilitate, manage or administer such uses or activities.

PPL5.3 Defence personnel making a disclosure to an overseas recipient **must** record and maintain details of the disclosure on unit or other official records. The record **must** include detail about the type of information disclosed. Where a disclosure

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

occurs via an automated information system, records kept by that system are considered sufficient.

PPL5.4 Defence personnel are **not** authorised to disclose the personal information of Defence personnel to an overseas recipient if the disclosure is otherwise specifically prohibited by law or contrary to another Defence Instruction or general order.

PPL5.5 Defence personnel who award contracts on behalf of the Commonwealth are **not** authorised to include in the terms of a contract the requirement to comply with PPL5.

PPL5.6 PPL5 should be read in conjunction with AG1 to ensure Defence meets its security obligations in providing personal information.

For the purpose of PPL5 Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL6 – <i>Reporting, recording and dealing with civil offences, service and civil convictions and diversionary programs</i> (PPL6).
Object:	PPL6 prescribes mandatory reporting by Defence members, and authorises Defence personnel to collect, use and disclose sensitive information, as defined in the Privacy Act 1988 , about a Defence member's civil offences, service and civil convictions and diversionary programs. The sensitive information enables Defence to determine employment suitability of Defence members and potential Defence members.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director of Military People Policy
Cancellations:	NIL

PPL6.1 A Defence member who has been arrested or charged with or convicted of a civil offence **must** notify their commander/manager within 24 hours of return to duty by completing part A of Form [PD052](#). The member is to provide details of the nature of the arrest charge or conviction, including pending court dates and any further requirements that may affect their availability for duty.

PPL6.2 Defence personnel are authorised to collect, use and disclose sensitive information about a Defence member for the purpose of reporting, recording and dealing with civil offences, service and civil convictions and diversionary programs.

PPL6.3 Other uses and disclosures of the same sensitive information, which are consistent with:

- a. the [Australian Privacy Principles](#),
- b. Defence Instruction – Administrative Policy
- or
- c. any other interim Instruction

are not excluded by the operation of PPL6.

PPL6.4 Defence personnel who award contracts on behalf of the Commonwealth are not authorised to include in the terms of a contract the requirement to comply with PPL6.

PPL6.1 The [Military personnel policy manual](#) Part 9 Chapter 7, *Reporting recording and dealing with civil offences, service and civil convictions and diversionary programs* is an administrative policy framework document. It should be read in conjunction with PPL6. It contains:

- a. details regarding certain circumstances in which disclosures are authorised

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

- b. information authorised to be disclosed and mechanisms for, and timings of, disclosures

and
- c. definitions that are specific to PPL6.

For the purpose of PPL6 Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL7 – <i>Required behaviours in Defence</i> (PPL7)
Object:	PPL7 establishes the behaviours the Secretary and the Chief of the Defence Force expect of Defence personnel. Adhering to the Defence Values and avoiding unacceptable behaviours contributes significantly to morale and promotes a cohesive, healthy, safe and effective workplace. It builds the capability of the Australian Defence Force and helps to protect and enhance the reputation of Defence.
Policy owner:	First Assistant Secretary People Services
Policy contact:	Director Complaints and Resolution
Cancellations:	NIL

PPL7.1 Defence personnel are responsible for their own behaviour. Defence personnel must give appropriate consideration to how they behave at work and in any situation that may be connected to Defence outside of official duty.

PPL7.2 Defence members **must not** engage in unacceptable behaviour.

PPL7.3 Defence personnel found to have engaged in, contributed to, ignored, assisted, or encouraged unacceptable behaviour, including misconduct of a sexual nature, may be held personally responsible.

PPL7.4 Annex 3G to Chapter 3 of the [Complaints and Alternative Resolutions Manual](#) is a framework document. It specifies the types of unacceptable behaviour as well as obligations, functions and duties with respect to managing and reporting unacceptable behaviour, including sexual misconduct. Annex 3G to Chapter 3 of the [Complaints and Alternative Resolutions Manual](#) is to be read in conjunction with PPL7 as if it is part of PPL7.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

For the purposes of PPL7:

unacceptable behaviour is unreasonable conduct at work or in any situation that may be connected to Defence that is offensive, belittling, abusive or threatening to another person, or adverse to morale, discipline or workplace cohesion. This includes unlawful discrimination and harassment.

conduct means actions or omissions

NOTE: Refer [Annex 3G, Chapter 3](#) of the [Complaints and Alternative Resolutions Manual](#) for detailed descriptions of all types of unacceptable behaviour.

Refer to [Annex 3A to Chapter 3](#) of the [Complaints and Alternative Resolutions Manual](#) for the Defence Values.

Refer [Chapter 9](#) of the [Complaints and Alternative Resolutions Manual](#) for definitions and complaint management guidance relating to all types of sexual misconduct.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL8 – <i>Engaging in political activities</i> (PPL8)
Object:	PPL8 prescribes and proscribes particular conduct by Defence members and Defence civilians with respect to engaging in political activities, to ensure that the ADF is, and is perceived to be, an apolitical organisation.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director of Military People Policy
Cancellations:	NIL

PPL8.1 Unless permitted by the Chief of the Defence Force or a person authorised by the Chief of the Defence Force, Defence members **must not**:

- a. take a leading or publicly prominent position or part in the affairs of a political organisation or party where that role would identify any part of Defence
 - i. with a political activity
 - and/or
 - ii. impair their ability to adequately fulfil their obligations to Defence
- b. take part in activities of a political nature on Defence premises unless all of the following applies:
 - i. the Department of Prime Minister and Cabinet has issued relevant Caretaker Conventions
 - ii. Defence has issued specific guidance
 - and
 - iii. the area has been set aside as a polling place on polling days in accordance with section 80 of the [Commonwealth Electoral Act 1918](#)
- c. when taking part in activities of a political nature, use any information gained by, or conveyed to them through their connection with Defence
- d. allow activities of a political nature to interfere with the functioning of Defence in the performance of its roles, or prejudice performance of their duties as Defence members
- e. engage in conduct in such a manner as to identify Defence with a political activity, position or perspective

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

- f. when taking part in activities of a political nature, use their rank when identifying, describing, or referring to themselves
- g. wear their uniform while taking part in activities of a political nature
- h. publish pictures of themselves or other Defence members in uniform in the context of political activity
- i. wear party ribbons or emblems or other political badges while on duty or in uniform.

PPL8.2 The [Military personnel policy manual](#) is an administrative policy framework document. Part 7 Chapter 5 of the [Military personnel policy manual](#) contains further requirements with respect to engaging in political activities. It should be read in conjunction with PPL8.

For the purpose of PPL8:

Defence member means a member of the Permanent Navy, the Regular Army, the Permanent Air Force, or the Reserves.

Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL9 – <i>Religious and spiritual services to the Australian Defence Force</i> (PPL9)
Object:	PPL9 prescribes and proscribes particular conduct by Defence members and establishes authorities relating to the provision of religious and spiritual services in the Australian Defence Force.
Policy owner:	Head People Capability
Policy contact:	Chair of the Australian Defence Force Chaplains' Committee
Cancellations:	NIL

PPL9.1 Unless operational imperatives preclude, commanders must take all reasonable and practical steps to provide Defence members and Defence civilians with their families, the opportunity to adhere to their religious, philosophical or spiritual practices and requirements.

PPL9.2 Australian Defence Force (ADF) chaplains and Navy Maritime Spiritual Wellbeing Officers (MSWO) must provide religious and/or spiritual services to the full spectrum of Defence peacetime and operational environments in accordance with PPL9 and the ADF Chaplaincy Policy (CHAPPOL). CHAPPOL is an administrative policy framework document and should be read in conjunction with PPL9. It describes principles, roles and responsibilities associated with the provision of chaplaincy services to the ADF.

PPL9.3 The Chief of the Defence Force or approved delegate, may advance an ADF chaplain or MSWO by appointing them to a higher honorary rank commensurate to the member's experience and competence. An ADF Chaplain or MSWO granted an honorary rank is taken to also hold one of the divisions or classes detailed at Part 4 of the [Defence Determination 2016/19, Conditions of Service](#).

PPL9.4 ADF Chaplains and MSWO do not have, and must not exercise, military executive authority and must not be appointed to any position that would require them to exercise such authority.

PPL9.5 Notwithstanding PPL 9.4, ADF Chaplains and MSWO must exercise and comply with normal administrative and technical authority consistent with an officer of the ADF and commensurate with their role and honorary rank.

PPL9.6 The Navy, Army and Air Force Directors General Chaplaincy exercise technical control for all religious, spiritual and pastoral policy matters on behalf of their respective Service Chief.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

For the purpose of PPL9:

An **ADF Chaplain** is a commissioned officer who is honorarily appointed to a rank specified in Schedule 1 of the [Defence Act 1903](#) and who is a religious leader appointed to provide religious, spiritual and pastoral care to members of the ADF.

A **religious leader** means a person who is endorsed by a particular faith group, where that faith group is recognised by the Chief of the Defence Force.

A **MSWO** is a commissioned officer appointed to chaplaincy positions within Navy to provide spiritual services. All provisions of PPL9 apply to MSWO, with the exception of the provision of religious ministry and support.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL10 – <i>Notification of Protection Order or Weapons Prohibition Order</i> (PPL10)
Object:	PPL10 prescribes conduct of Defence members with respect to Protection Orders and Weapons Prohibition Orders.
Policy owner:	First Assistant Secretary People Policy and Culture
Policy contact:	Director Military People Policy
Cancellations:	Nil

PPL10.1 A Defence member serving in SERCAT 6 or 7 who is a respondent to a Protection Order (PO) or a Weapons Prohibition Order (WPO) **must** notify their commander in writing no later than 24 hours after becoming aware they are respondent to the Order, or of any changes to an existing Order. A member in SERCAT 2-5 **must** notify their commander on commencement of the first period of duty, or no later than 14 days (whichever is earlier) after becoming aware they are respondent to the PO or WPO, or of any changes to an existing Order.

PPL10.2 Upon initial notification by a Defence member who is a respondent to a PO or WPO, the commander **must** immediately prevent the member from accessing weapons, ammunition, body armour and explosives stored in Australian Defence Force armouries, magazines, and other designated storage facilities.

PPL10.3 The [Military personnel policy manual](#) Part 9 Chapter 4, *Protection Orders and Weapons Prohibition Orders* is an administrative policy framework document. It is to be read in conjunction with PPL10. It details the roles, responsibilities and requirements associated with these POs and WPOs in Defence. It also contains definitions that are specific to PPL10.

For the purpose of PPL10 Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

PEOPLE
POLICY DOMAIN PROVISIONS

Accountable officer – Deputy Secretary Defence People

Title:	PPL11 – Defence Transition System (PPL11)
Object:	The object of PPL11 is to establish Head People Capability as the Technical Authority for the Defence Transition System.
Policy owner:	Head People Capability
Policy contact:	Director General Joint Transition Agency
Cancellations:	NIL

PPL11..1 The Secretary and the Chief of the Defence Force appoint Head People Capability as the Technical Authority for Defence Transition (the Transition Technical Authority).

PPL11..2 The Transition Technical Authority is responsible for integrating, synchronising and assuring the Defence Transition System's governance, management, planning and delivery is fit for purpose.

PPL11..3 The [Military Personnel Policy Manual \(MILPERSMAN\)](#), Part 10 Chapter 6 – *Defence Transition System* is an administrative policy framework document. It should be read in conjunction with PPL11.

For the purpose of PPL11:

Manager means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

INTELLIGENCE
POLICY DOMAIN PROVISIONS

Accountable officer – Chief of Defence Intelligence

THERE ARE NO PROVISIONS BELONGING TO THIS POLICY DOMAIN
CURRENTLY IN FORCE

SUBMISSIONS MEETING PARTICULAR CRITERIA OUTLINED ON [FACT SHEET 1](#)
CAN BE SUBMITTED TO THE [ADMINISTRATIVE POLICY TEAM](#) FOR
CONSIDERATION AND POSSIBLE INCLUSION IN
THE NEXT EDITION OF THIS INSTRUCTION

[VIEW POLICIES](#) BELONGING TO THIS DOMAIN

INNOVATION, SCIENCE AND TECHNOLOGY
POLICY DOMAIN PROVISIONS

Accountable officer – Chief Defence Scientist

THERE ARE NO PROVISIONS BELONGING TO THIS POLICY DOMAIN
CURRENTLY IN FORCE

SUBMISSIONS MEETING PARTICULAR CRITERIA OUTLINED ON [FACT SHEET 1](#)
CAN BE SUBMITTED TO THE [ADMINISTRATIVE POLICY TEAM](#) FOR
CONSIDERATION AND POSSIBLE INCLUSION IN
THE NEXT EDITION OF THIS INSTRUCTION

[VIEW POLICIES](#) BELONGING TO THIS DOMAIN

ADMINISTRATIVE POLICY DOMAIN STRUCTURE

ACQUISITION & SUSTAINMENT DOMAIN Accountable officer Deputy Secretary Capability, Acquisition & Sustainment - Project management - Engineering - Procurement management - Contract management - integrated product support	INFORMATION & COMMUNICATIONS TECHNOLOGY DOMAIN Accountable officer Chief Information Officer - Information & communications technology (ICT) - Technical authority (single information environment), including ICT Cyber Security
ADMINISTRATION & GOVERNANCE DOMAIN Accountable officer Associate Secretary - Communications - Service delivery - Data - Legal - Audit & fraud & integrity - Information management - Risk - Governance	MILITARY COMMAND SUPPORT DOMAIN Accountable officer Vice Chief of the Defence Force - One Defence Capability System - ADF reputation management - Military justice - Joint force authority - Military strategic commitments and plans - Capability generation - Mobilisation - Testing and evaluation
STRATEGY, POLICY & INDUSTRY DOMAIN Accountable officer Deputy Secretary Strategy, Policy, and Industry - Strategic policy development - Industry policy development - International policy development - Contestability	MILITARY JOINT ENABLING DOMAIN Accountable officer Chief of Joint Capabilities - Joint education & training - Defence education & training - Joint logistics - Joint military policing & investigations - Youth & reserves - Military technical authorities (joint health) - Military technical authorities (cyber)
SECURITY & ESTATE DOMAIN Accountable officer Deputy Secretary Security & Estate - Infrastructure, facilities, estate & environment - Base services - Security	PEOPLE DOMAIN Accountable officer Deputy Secretary People - Personnel - Work, health & safety - Diversity & inclusion - Corporate training - APS Learning & development - Transition technical authority - People research (low ethics clearance)
FINANCE DOMAIN Accountable officer Chief Finance Officer - Budget & financial reporting - Financial control & assurance - Financial services - Financial & costing	INTELLIGENCE DOMAIN Accountable officer Chief of Defence Intelligence - Intelligence capability development - Geospatial intelligence development - Development of strategic intelligence assessments - Intelligence policy development
INNOVATION, SCIENCE & TECHNOLOGY Accountable officer Chief Defence Scientist - Capability innovation system - Science & technology portfolio - Research & development	