

DEFENCE PRIVACY POLICY

Part 1 – Overview

Defence's Privacy Policy is designed to inform individuals about the way Defence collects, stores, uses and discloses personal information. This Privacy Policy also provides guidance about how you can access, or seek correction of, personal information held by Defence about you.

Who should read this Privacy Policy?

You should read this Privacy Policy if you:

- are, or are considering becoming:
 - an Australian Defence Force (ADF) member^{*}
 - an Australian Public Service (APS) employee[†] of Defence[‡]
 - a Defence civilian[§]
 - a Defence locally engaged employee
 - an outsourced service provider, contractor or consultant to Defence
 - a Cadet, Officer or Instructor of Cadets in the Australian Navy Cadets, Australian Army Cadets and the Australian Air Force Cadets
- are involved in an Australian Government security clearance process, conducted by the Australian Government Security Vetting Agency (AGSVA), for example as a clearance subject or a referee
- are seeking to export Defence strategic goods and technologies
- seek a licence, permit or approval under Defence's legislative or regulatory framework
- are an individual whose personal information has been, or will be, collected or held by Defence.

The Australian Privacy Principles (APPs) contained in Schedule 1 of the [TTUU Privacy Act 1988](#) (Privacy Act), regulate how Defence, as an APP entity, collects, holds, uses and discloses personal information.

Generally, Defence collects personal information about individuals **within** Defence, including:

- members of the ADF
- Defence APS employees
- Defence civilians
- a Cadet, Officer or Instructor of Cadets in the Australian Navy Cadets, Australian Army Cadets and the Australian Air Force Cadets
- Defence locally engaged employees,

and individuals **external** to Defence, including:

- dependants, next of kin and emergency contacts of ADF members and Defence APS employees
- contractors, consultants and outsourced service providers
- candidates seeking entry into the ADF and prospective Defence APS employees
- individuals requiring an Australian Government security clearance, or otherwise involved or associated with a clearance process, undertaken by the Australian Government Security Vetting Agency (AGSVA)
- people and agents of organisations doing business with Defence
- individuals involved in disciplinary proceedings, investigations and/or inquiries
- people seeking a licence, permit or approval under Defence's legislative or regulatory framework
- people who make contact with Defence or the Minister for Defence.

Defence collects personal information both directly from the individual concerned, and from other persons, bodies or entities, including an individual's commander, manager and supervisor, and from specialist service providers, such as medical practitioners.

The purposes for which Defence collects personal information are outlined below in [Part 4](#).

You are entitled to request access to personal information Defence holds about you or to request correction of that information. Information about how to do this is provided in [Part 7](#).

Enquires regarding the Defence Privacy Policy or Defence's privacy practices in general should be directed to the [Defence Privacy Officer](#).

Detailed information on the APPs can be found on the website of the [Office of the Australian Information Commissioner](#).

The Defence Privacy Policy is reviewed annually to ensure the information it contains is accurate, complete, relevant and up-to-date.

Part 2 – Exemptions from the Privacy Act

The following Defence Intelligence Agencies are exempt from the requirements of the Privacy Act and are not included in this privacy policy:

- Defence Intelligence Organisation
- the Australian Geospatial-Intelligence Organisation
- the Australian Signals Directorate.

Additionally, the APPs do not apply to operational information collected by Defence and personal information for special access programs under which foreign governments provide restricted access to technologies.

Part 3 – The kinds of personal information Defence collects and holds

The nature and extent of personal information Defence collects and holds will vary depending on an individual's particular relationship and interaction with Defence. The kinds of personal information collected and held by Defence are outlined in Part 1 [Annexure 1](#) of this Privacy Policy.

What is personal information?

'Personal information' is defined in subsection 6(1) of the Privacy Act as:

information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a. whether the information or opinion is true or not; and*
- b. whether the information or opinion is recorded in a material form or not.*

Personal information collected by Defence may also be sensitive information. Sensitive information has a particular meaning under the Privacy Act and includes types of personal information that are of a more sensitive nature. For example information about your health, political opinions and other listed personal circumstances. The kinds of sensitive information collected and held by Defence are outlined in Part 2 [Annexure 1](#) of this Privacy Policy.

Information about corporate entities, such as businesses, firms or trusts, or other commercially sensitive information, is not personal information and is not covered by this Privacy Policy or the APPs.

Part 4 – Purposes for which Defence collects personal information

Defence will only collect personal information that is reasonably necessary for, or directly related to, its functions or activities.

As reflected in the Commonwealth of Australia [Administrative Arrangements Order](#) (AAO), which sets out the legislative and functional responsibility of the Minister for Defence and the Department, the Minister for Defence is responsible for the defence of Australia, which includes:

- international defence relations and defence co-operation
- defence scientific research and development
- defence procurement and purchasing
- defence industry development and co-operation.

In order to satisfy these responsibilities and Defence's responsibilities under the various pieces of legislation it administers, Defence collects personal information for various purposes depending on the individual's relationship with Defence. Generally, Defence collects personal information for the following purposes:

- the recruitment, enlistment, appointment, command, administration, management and discipline of ADF members
- the recruitment, employment and management of APS employees in Defence
- the provision of health, rehabilitation and veterans' services to Defence personnel**
- the management of the welfare of Defence personnel and their dependants
- the provision of housing services to Defence members and their families
- processing, evaluating and granting security clearances for the Commonwealth
- conduct of Defence operations
- Defence community engagement, including cadet and youth programs and Defence awards, sponsorships and scholarships

- the conduct of Defence business activities with the individual
- the engagement of external service providers
- maintaining historical records
- compiling diagnostic information
- conducting approved human research
- identifying potential conflicts of interest
- performing security functions associated with information management, which includes website and email access
- legislative and regulatory purposes that require the grant of a licence, permit or approval and the consideration thereof.

Use of consultants, contractors and outsourced service providers

Defence uses consultants, contractors and outsourced service providers to undertake certain business functions. Personal information about you may be collected by or provided to a Defence consultant, contractor or outsourced service provider when necessary. In situations where personal information about you is provided to a consultant, contractor or outsourced service provider, Defence practice is to generally retain effective control of the information. This is done by specifying in the terms of the contract that Defence is to maintain effective control of any personal information disclosed to and/or used by consultants, contractors or outsourced service providers. In situations where Defence discloses personal information about you to consultants, contractors or outsourced service providers and Defence does not retain effective control of the information, the information will only be used for purposes which are reasonably necessary for, or directly related to, Defence's functions or activities.

Consultants, contractors and outsourced service providers who have access to personal information collected by Defence, or who collect personal information on behalf of Defence, may, if specified in the terms of their contract, be subject to the same information security policy, training and auditing requirements as Defence personnel and must also comply with the APPs.

Disclosure

Defence may disclose personal information about you to other APP entities, including:

- the Minister for Defence, the Assistant Minister for Defence or the Parliamentary Secretary to the Minister for Defence
- other Defence-related agencies, regulatory bodies, and organisations such as the Department of Veterans' Affairs, Defence Housing Australia and the Australian War Memorial
- other non-Defence related government departments, regulatory bodies, and organisations that have a function in relation to, or affecting the administration of, ADF members and Defence APS employees, such as the Australian Taxation Office, Comsuper, Comcare, the Child Support Agency, the Australian Institute of Health and Welfare, SmartSalary and Toll Transitions
- in the case of security clearances, the Australian Security Intelligence Organisation and the Australian Federal Police
- Department of Immigration and Border Protection
- law enforcement agencies such as the Australian Federal Police, State and Territory policing agencies
- federal, state and territory courts and tribunals
- other Australian Government departments and agencies for legislative and regulatory purposes
- overseas recipients for legislative, regulatory and reporting purposes to meet Australia's national security and international obligations.

Defence may disclose personal information about members who are attending the Australian Defence Force Academy to the University of New South Wales or to other educational institutions.

Defence may disclose personal information about you to a person who is not in Australia or an external territory (overseas recipient) where it relates to Defence activities or functions. Personal information about you may be disclosed in the country where the recipient is ordinarily located, or in a country where the recipient is or, is soon to be, undertaking work related activities. For example, where Australia is undertaking or participating in military operations or exercises, where it has a Defence establishment (such as RMAF Base Butterworth, located in Malaysia), or where Defence personnel are located overseas on posting, such as those performing a Defence Attaché role or an exchange posting, personal information may be disclosed to 'overseas recipients' in the countries where the activity is being undertaken.

Defence does not disclose personal health information to any other person, including next of kin, unless the individual about whom the information relates has given express consent, or the disclosure is required or authorised by or under Australian law, or in circumstance where it is unreasonable to obtain the individual's consent and the disclosure is necessary to lessen or prevent a serious threat to life, health or safety of an individual or to public health and safety.

If it is necessary for the acquisition or use of Defence equipment and capability, Defence may also disclose the personal information of those involved directly, or indirectly, to recipients in the countries where the recipients are located or the activities or functions are performed.

Part 5 – How Defence collects personal information about you

Defence endeavours to collect personal information about you directly from you where it is reasonably practicable to do so. Defence collects this information by the use of various forms; from information provided to commanders, managers and supervisors; and through PMKeyS (Defence's personnel and organisational data management system).

Due to the scope and nature of Defence activities it is not always possible to collect personal information from the individual concerned. Defence may collect personal information about you indirectly from a range of other sources including, but not limited to:

- publicly available sources
- your access to Defence websites, or information and communications networks and systems
- your family members
- past and present employers and character referees
- health practitioners
- other government agencies and organisations.

Defence may also generate personal information about you in the course of undertaking its functions or activities.

Part 6 – How Defence holds personal information about you

Defence stores personal information about you as hardcopy documents or as electronic data within its record management systems.

Defence protects personal information about you in accordance with the policy provided for in the Defence Security Manual in order to take reasonable steps to protect that information against loss, unauthorised access, use and disclosure, modification and misuse. Defence regularly conducts system audits to ensure that it adheres to its established protective and information security practices. Protective measures include password protections, access privileges, secure cabinets/containers and physical access restrictions. Documents containing personal information also carry the 'Sensitive: Personal' dissemination limitation marker and may also include a warning notation of 'Health Information', where appropriate.

Access to personal information about you is restricted to Defence personnel who have a need to access the information for purposes which are directly related to or reasonably necessary for their duties in support of Defence's functions or activities.

Defence personnel are also required to undertake mandatory annual protective and information security training, and personnel with access to the Defence personnel management system must demonstrate knowledge and an understanding of the APPs. In addition to the statutory and policy security measures for the protection of personal information practised by Defence, reasonable steps must be taken to ensure that the information is protected.

Defence will only destroy personal information in accordance with statutory requirements, including the [Archives Act 1983](#) and in consultation with relevant authorities authorised to destroy the information. The Defence Records Management Manual also contains policy on the retention and destruction of documents. Generally speaking, Defence records must be retained and accessible for as long as they are legally required.

Part 7 – Access to and correction of personal information

You have a right to request access to, or seek correction of, personal information held by Defence about you. Defence will attempt to provide you with access to personal information about you in the format you request. However, on occasion, this may not be possible and in some circumstances, access may only be

granted through a third party, such as a medical practitioner. Defence will consult with you in these circumstances.

You can request correction of personal information about you from the area within Defence that collected the information. If you are unsure which area of Defence collected the personal information, you can contact the [Defence Privacy Officer](#), who will coordinate your application for correction. You should be aware that Defence's ability to correct or amend personal information may be limited where the information is contained in a Commonwealth record, as defined in the [Archives Act 1983](#).

You can request access to the personal information Defence holds about you in several ways, depending on your circumstances.

Current ADF members

Current ADF members can request access to their personal information through their chain of command.

Former ADF members

Former ADF members can request access to their personal information contained in:

- Navy health records
- Navy personnel records after 1947
- Air Force health and personnel records after 1952
- Army health records after 1947
- Army personnel records after 1947.

by contacting:

Defence Archive Centre—Fort Queenscliff (DAC-FQ)
GPO Box 1932
MELBOURNE VIC 3001

Defence no longer holds Army health records prior to 1947 or Air Force health records prior to 1952. For information about how to request these records, contact the Department of Veterans' Affairs (www.dva.gov.au).

All ADF World War I and World War II records are held by the National Archives of Australia. For information about how to request these records contact the National Archives of Australia (www.naa.gov.au).

Current and former Defence APS employees

Current Defence APS employees may request personal information directly through their line manager, from the area that holds the information, or by contacting the Defence Service Centre – Cooma on 1800 333 362.

Former Defence APS employees may request personal information about them by contacting the Defence Service Centre – Cooma on 1800 333 362.

ADF recruitment applicants

ADF recruitment applicants should contact the Defence Force Recruiting Centre at which their application was initially submitted, or call 13 19 01.

Security clearances

Individuals may request personal information about them held by the Australian Government Security Vetting Agency, which was provided for a security clearance process, by contacting the Director Vetting Governance at SecurityClearances@defence.gov.au.

All other requests

If you are requesting personal information held about you and you are not, or have not been, an ADF member or Defence APS employee (for example a person doing business with Defence or a Defence contractor), you can request personal information about you by contacting the relevant area within Defence (for example, AGSVA or the Defence Export Control Office), or by contacting the [Defence Privacy Officer](#), who will assess and coordinate your access to the personal information requested. This can be done by emailing defence.privacy@defence.gov.au.

Further information on the types of records held at the Defence Archives can be obtained from the Defence Archives web site at: <http://www.defence.gov.au/Records/>.

Part 8 – Concerns about how personal information about you is handled

If you have questions about how personal information about you will be, or has been, handled by Defence, or if you believe that Defence has breached the APPs, you should contact the [Defence Privacy Officer](#). Your concerns may be forwarded to the relevant area within Defence for consideration and action, if appropriate.

Defence is committed to quick and fair resolution of privacy complaints. However, some cases may require more detailed inquiry. Defence undertakes to keep you informed of the progress of your complaint.

If you are dissatisfied with the way Defence handles your privacy-related complaint, you may contact the Office of the Australian Information Commissioner. Contact details for the Office of the Australian Information Commissioner are in [Part 9](#).

Part 9 – Contact details

Defence Privacy Officer

Email: defence.privacy@defence.gov.au
Post: BP35-01-066
PO Box 7927
Canberra BC
ACT 2610

Office of the Australian Information Commissioner

Phone: 1300 363 992
Web: <http://www.oaic.gov.au/privacy>
Email: enquiries@oaic.gov.au
Post: GPO Box 5218
Sydney NSW 2001

* An ADF member is defined in section 4 of the [Defence Act 1903](#) to include an officer, soldier, sailor, airman or airwoman.

† A Defence APS employee means a person employed in the Department of Defence under the [Public Service Act 1999](#).

‡ For the purposes of the Privacy Act, the Department of Defence includes the Australian Defence Force and the Australian Defence Force Cadet Organisations (Australian Navy Cadets, Australian Army Cadets and the Australian Air Force Cadets) and are collectively referred to as Defence.

§ Defence civilian as defined in [section 3 of the Defence Force Discipline Act 1982](#) (DFDA), is a person (other than a Defence member) who:

- a. with the authority of an authorised officer as defined in the DFDA, accompanies a part of the ADF that is outside Australia, or on operations against the enemy; and
- b. has consented, in writing, to subject themselves to ADF discipline while so accompanying that part of the ADF.

** Defence personnel includes Australian Public Service employees in the Department of Defence (Defence APS employees), Defence members, Defence locally engaged employees, Defence civilians, and foreign personnel on exchange to Defence.

Annexure 1 to the Defence Privacy Policy

Part 1 – Personal Information collected by Defence

- The kinds of **personal information** collected by Defence for purposes directly related to or reasonably necessary for its functions or activities include:

Name	Records relating to attendance and overtime
Title	Leave applications and approvals
Date of birth	Payroll and pay related information
Place of birth	
Contact details	Performance appraisals
Addresses	Trade, skill and aptitude test records
Residency details	Honours and awards
Citizenship details	Completed questionnaires and personnel survey forms
Passport information	
Gender	Information relating to removals
Marital status	Information related to travel
Equity and diversity information	Information relating to welfare
Next of kin details	Information relating to allowances
Emergency contact details	
Occupation	Information related to character checks and security clearances
Rank or classification	
Post nominals	
Professional areas of interest	Applications for compensation
Languages spoken	Information relating to rehabilitation and fitness for duty
Hobbies/interests	
Driver license details	Information relating to complaints and grievances
Education	Information relating to FOI requests
Qualifications	Information relating to workplace incidents
Certificates/awards	
Training and development	Information relating to social media accounts (e.g. Facebook, Twitter)
Family details	Information relating to the use of Defence websites, including:
Dependant details and information	- User's server address
Relationship details	- User's top level domain name (e.g. .com, .gov, .au)
Family support history	- Date and time of visit
Financial information	- Pages accessed and documents downloaded
PMKeys/Service number	- Email address
AGS number	
Employment history	Voice data
General information relating to an employee's employment	Video images
Information relating to professional references	Photographic images
Personal history	
Discipline history	Information relating to court proceedings
Conduct history	
Workplace management history	Evidence provided in relation to inquiries and other investigations
Biographies	Witness statements
Application for recruitment/employment	
Written tasks undertaken during selection process	Information related to seeking legal advice
Notes taken about you during selection process	Legal advice
Personal information contained in selection process reports	Client instructions
	Court documents
Taxation information	
Superannuation information	

Part 2 – Sensitive Information collected by Defence

The kinds of **sensitive information** collected by Defence for purposes directly related to or reasonably necessary for its functions or activities include:

Racial and ethnic origin	Professional/trade association and memberships
Political opinions	
Political affiliations, associations and memberships	
Religious beliefs/affiliations	
Philosophical beliefs	

Trade union membership
Sexual preferences or practices
Health information
Genetic information
Criminal history
Criminal intelligence information