

## PRIVACY POLICY

### 1. Purpose

As an Australian government statutory authority, AFTRS must comply with the *Privacy Act 1988* (**Privacy Act**). The Privacy Act requires AFTRS to have a Privacy Policy.

This Policy provides information about AFTRS' handling of personal information, including sensitive information, according to the Privacy Act and, in particular, the Australian Privacy Principles (**APPs**).

### 2. Scope

This Policy applies to AFTRS, its potential, current and past officers, employees, contractors and volunteers (**AFTRS Personnel**), to AFTRS' students, and to members of the public (collectively **you**).

### 3. Policy Statement

AFTRS is committed to:

- protecting your privacy according to the Privacy Act; and
- ensuring that AFTRS Personnel and students understand AFTRS', and their, rights and responsibilities.

AFTRS Personnel are responsible for ensuring their own work practices comply with this Policy and any related Procedures. A breach of this Policy may constitute misconduct (and be subject to disciplinary action) or a breach of contract.

#### 3.1 Collecting personal information

AFTRS collects the personal information it needs to carry out a particular function or activity.

##### *Direct collections*

Usually, AFTRS collects this information from you when you provide it directly to AFTRS. For example, AFTRS may collect the information:

- when you apply to study at AFTRS, and when you enrol;
- when you apply for employment or are employed by AFTRS;
- when you become a member of AFTRS' library;
- when you sign up to receive AFTRS' newsletters and ask or agree to be added to AFTRS' email lists; or
- to enter into a contract with youAFTRS operates a closed circuit television system for security and safety purposes, and your image may be captured if you are filmed by this system while on AFTRS' premises.

AFTRS may collect sensitive information, for example, to deal with your workers' compensation claim, to properly meet its obligation to make reasonable adjustments

where you are a student and you have a disability, or to provide student welfare support, or criminal history for enrolment and WHS obligations

#### *Indirect collections*

Sometimes, AFTRS collects personal information indirectly from a third party. For example, AFTRS may obtain information from referees before offering employment or may collect information about prior learning from another tertiary institution that is relevant to academic progression at AFTRS. AFTRS may collect information that is an opinion about your creative work from third party assessors or referees.

#### *Anonymous and pseudonymous interactions*

Usually, AFTRS requires your name and other contact details to deal with you, for example, to employ you or to enrol you as a student. However, where possible, AFTRS will still interact with you if you wish to be anonymous or to use a pseudonym. If you make a general enquiry, for instance, AFTRS will not require you to provide your name, unless this is necessary to respond to the enquiry.

#### *Collecting information through AFTRS' website*

Information about AFTRS' collection of personal information through AFTRS' website is provided in AFTRS' [Website Collection Notice](#).

AFTRS uses social networking services such as *Twitter*, *Facebook* and *YouTube* to communicate about AFTRS' activities and its students' work. If you communicate with AFTRS using these services, AFTRS may collect your personal information, but will only use it to help AFTRS communicate with you and other people through these services. Social networking services, which AFTRS uses, will also handle personal information for their own purposes and have their own privacy policies.

#### *Examples of personal information held*

The kinds of personal information held include:

- in relation to students: name, postal address, email addresses, telephone numbers, date of birth, education, academic record, production credits, work experience, and health information;
- in relation to employees: name, postal address, employment history, details of qualifications, results of employment checks, medical records, tax file numbers; financial information;
- in relation to third party service providers and volunteers: names, postal addresses, email addresses, superannuation fund details, telephone numbers and employment details of key personnel; work experience;
- for mailing lists: name, postal address, telephone numbers, fax numbers, email addresses, name of organisation, history as student or employee of AFTRS;
- in relation to library members and applicants for membership: name, postal address, telephone numbers, email addresses, and business name;
- for people making complaints and enquiries: name, postal address, email addresses, and telephone numbers.

If AFTRS is not able to collect your personal information, AFTRS may not be able to provide its services or products to you or do business with you or the organisation with which you are connected.

### 3.2 Collecting Sensitive Information – Criminal History

In order for AFTRS to meet the School's WHS obligations and common law duty of care AFTRS is required to obtain as part of enrolment the disclosure of all previous criminal convictions and indictable offences.

### 3.3 Using and disclosing personal and sensitive information

AFTRS may **use** personal information (that is not sensitive information) for the purposes for which it was collected, for related purposes that you would reasonably expect, or if you agree to the use. For example:

- in relation to students: to process your application and enrolment and other administrative matters; to enable you to be placed on AFTRS' electoral rolls; to communicate with you as AFTRS' students and graduates, including to foster alumni relations; for course monitoring, evaluation and surveys; to facilitate AFTRS' internal planning; for record-keeping and archiving; for student health, welfare and support; and to meet AFTRS' internal and external reporting requirements, including to the Department of Education and Training;
- in relation to employees: to assess your suitability for employment; to ensure payment to you; to manage your employment relationship with AFTRS;
- in relation to third party service providers and volunteers: to engage and pay you or reimburse you for expenses;
- on AFTRS' mailing lists: to send information about AFTRS and its functions and activities;
- in relation to library members and applicants for membership: to identify you, process your library application and manage your library membership and borrowings;
- where AFTRS receives a complaint or enquiry: to deal with the complaint or enquiry.

AFTRS may **disclose** personal information (that is not sensitive information) for the purposes for which it was collected, for related purposes that you would reasonably expect, or if you agree to the disclosure. For example:

- in relation to students: to other educational institutions and academically related professional bodies for educational or official purposes; to another agency to assist you to receive an allowance or permission to study from the agency; to the Department of Education and Training for the purpose of reports;
- in relation to employees: to financial institutions; to superannuation funds; to the Australian Taxation Office;
- in relation to third party service providers: to financial institutions; to superannuation funds;
- where AFTRS receives a complaint: to the person or organisation who is the subject of, or who is involved in the handling of the complaint.

Where AFTRS seeks your agreement to a use or disclosure of your personal information, AFTRS will consider you are capable of agreeing if you are 15 years or older, unless AFTRS is aware of circumstances that suggest the contrary. If you are under 15, AFTRS will ask your parent or guardian to agree on your behalf.

AFTRS discloses your sensitive information for the purposes, for which it is given, or for *directly* related purposes, you would reasonably expect, or for purposes, you agree to.

AFTRS will only use the sensitive information of student criminal history disclosed for the purposes of enrolment and the assessment of the School's WHS obligations and common law duty of care.

Sometimes, AFTRS is also required or authorised by law, including by the Privacy Act, to use or disclose personal information, for example, where a warrant or order issued by a court requires AFTRS to provide information or documents.

Under no circumstances will AFTRS sell or receive payment for licensing or disclosing personal information.

### **3.4 Disclosing information overseas**

There may be circumstances where AFTRS discloses personal information to an overseas recipient, including where AFTRS needs to provide a lecturer who is overseas with the contact details of students with whom they will be working or provides an overseas recipient with information relating to a student's or graduate's overseas placement.

AFTRS will not send information about you outside Australia without complying with the requirements of the Privacy Act.

### **3.5 Information quality**

To ensure that the personal information AFTRS collects is accurate, up-to-date and complete, AFTRS:

- where necessary, confirms the accuracy of information AFTRS collects from a third party or a public source;
- adds updated or new personal information to existing records as set out in the section of this Policy dealing with corrections of personal information; and
- audits AFTRS' contact lists to check their accuracy from time to time.

AFTRS also reviews the quality of personal information before AFTRS uses or discloses it.

### **3.6 Storage and Security**

AFTRS takes steps to protect records of personal information and sensitive information – criminal history disclosure, whether paper or electronic, from misuse, interference and loss, and unauthorised access, modification or disclosure.

Personal information automatically collected through our website is stored mainly in internally managed ICT systems or in external systems managed by third parties providing ICT storage facilities for AFTRS. These third parties are subject to the terms of a service agreement.

AFTRS employs firewalls for the protection of its ICT network. Passwords and graded access rights as well as auditing logs are used to regulate access to personal information. Employees are only given a level of access appropriate to their duties.

Other steps AFTRS takes to protect records of personal information include the following:

- storing all paper records in locked cabinets, commonly fire resistant;
  - restricting access to paper records to relevant staff; and
- 3.7** requiring certain employees to successfully undergo a National Police check conducted by the Australian Federal Police      Accessing and correcting personal information

You may request access to, or the correction of, your personal information and sensitive information in writing or verbally. AFTRS may correct incorrect personal information on its own initiative.

AFTRS will either give access to, or correct, the personal information requested, or inform you why access or correction is refused, within 30 calendar days after the day the request is made, unless this is impractical. AFTRS' staff may be present while you access your personal information.

You and AFTRS may agree to an intermediary having access to your personal information, for example a qualified health service provider.

In giving access, AFTRS will impose as few restrictions as possible and will not impose any charges. AFTRS will give access in the manner requested by you if reasonable and practical.

AFTRS may refuse access, or refuse to correct information, if it is required or authorised to do so by the *Freedom of Information Act 1982 (FOI Act)*, or another Commonwealth Act. In this respect, AFTRS is subject to the *Archives Act 1983 (Archives Act)*, and is not permitted to alter Commonwealth records except as permitted by the Archives Act.

If AFTRS decides to refuse access, or to refuse access in the manner requested, AFTRS will inform you in writing, giving its reasons (unless this is unreasonable) and inform you of available complaint mechanisms.

If AFTRS refuses a request for a correction, AFTRS will, at your request, take reasonable steps to attach a statement with the personal information that you believe to be inaccurate, out-of-date, incomplete, irrelevant or misleading. AFTRS will respond to a request to attach a statement within 30 calendar days after AFTRS receives the request.

Requests for access or correction must be referred to the Head of Student Services (for students), the Head of Human Resources (for employees), Payroll Manager (for employees) or to the Head of Business Affairs as the Privacy Officer (and FOI Officer).

You also have the right under the FOI Act to request access to documents that AFTRS holds and ask for information that AFTRS holds about you to be changed or annotated if it is incomplete, incorrect, out-of-date or misleading.

If there is any uncertainty as to whether a request for access fits, within this Policy the matter must be referred to the Privacy Officer or the FOI Officer before any information is given.

### 3.8 Disposing of personal information records

As AFTRS' records of personal information and sensitive information are likely to be 'Commonwealth records' for the purposes of the Archives Act, AFTRS will retain and destroy these records only according to that Act and any AFTRS' Disposal Authority issued under that Act.

Complaints about interferences with your privacy may be sent in writing to AFTRS for internal review by contacting AFTRS' Privacy Officer at [privacyofficer@aftrs.edu.au](mailto:privacyofficer@aftrs.edu.au). Please allow AFTRS a reasonable time (usually 30 days) to respond.

If you believe there has been an interference with your privacy, you may make a complaint in writing to the Information Commissioner. The Information Commissioner may investigate, determine and make declarations in a matter, but will commonly not investigate a complaint if you have not first raised it with AFTRS.

There is provision in the Privacy Act for the enforcement of the Information Commissioner's determinations, including by the Federal Court of Australia or the Federal Circuit Court.

## 4. Definitions

**personal information** means 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.

**sensitive information** means

- a. information or an opinion about an individual's:
  - i. racial or ethnic origin; or
  - ii. political opinions; or
  - iii. membership of a political association; or
  - iv. religious beliefs or affiliations; or
  - v. philosophical beliefs; or
  - vi. membership of a professional or trade association; or
  - vii. membership of a trade union; or
  - viii. sexual orientation or practices; or
  - ix. criminal record;

that is also personal information; or

- b. health information about an individual; or
- c. genetic information about an individual that is not otherwise health information; or
- d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- e. biometric templates.

## 5. Authorisation and distribution

|                                   |                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Authorisation Date</b>         | CEO<br>24 November 2017                                                                                                      |
| <b>Responsible Officer</b>        | Head of Corporate Strategy and Governance                                                                                    |
| <b>Date</b>                       | N/A                                                                                                                          |
| <b>Contact Officer</b>            | Policy and Governance Officer                                                                                                |
| <b>Effective Date</b>             | 24 November 2017                                                                                                             |
| <b>Distribution</b>               | Intranet and AFTRS website                                                                                                   |
| <b>Review Date</b>                | 4 August 2019<br>Three years from effective date; earlier or later dependent on external factors such as legislative reform. |
| <b>Current version Supersedes</b> | v2.0<br>Privacy Policy v1.2 August 2016                                                                                      |
| <b>Associated Documents</b>       | <i>Privacy Act 1988</i><br><i>(AFTRS)Website Collection Notice</i>                                                           |