Chapter 7. Privacy, Communication and Information Management

7.1 Introduction
ATDP functions necessitate:

• the creation, collection, management and in some circumstances, the disclosure of Personal Information about staff, volunteers, service providers and those who engage services facilitated by ATDP; and
• the communication and management of non-personal information.

7.2 Scope
This chapter outlines the policy and procedures for handling personal and other information.

The policy applies to all Members of the CFMG and RMG, Trainers and Assessors, Mentors acting on behalf of the ATDP, and any other third party that collects or manages personal information on behalf of ATDP.

The SGB Chair has advised that these policy and procedures are also to be observed by volunteer members of the Strategic Governance Board.

7.3 ATDP Privacy Policy
The following Commonwealth legislation mandates the actions ATDP must take to protect the privacy of Personal Information:

• Privacy Act 1988 (Cth):
• Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth):
• Australian Privacy Principles:

7.3.1 Commitments
ATDP recognises that all users of services ATDP provides or facilitates have a reasonable expectation that their Personal Information will be protected and managed appropriately.

ATDP is therefore committed to managing all Personal Information in accordance with the Information Privacy Principles (IPPs).

As a commitment to good privacy practice, ATDP has elected to ‘opt-in’ to the provisions of the Privacy Act 1988 (Cth). ATDP commits to compliance with:

• the provisions of the Privacy Act; and
• the additional requirements of State and Territory privacy legislation in which the person subject to that legislation lives.

ATDP’s objective is to assure client confidence and affirm client trust.
7.3.2 Application
This policy applies to the collection, use, storage, transfer, handling, right of access, and amendment of personal information within ATDP.

7.3.3 Purpose
The purpose of this policy is to:

- provide for the fair collection, management and handling of Personal Information; and
- specify the rights of access to, and amendment of, Personal Information collected by ATDP.

7.3.4 ATDP-specific Privacy Documentation
ATDP-specific considerations and procedures for disclosure of Personal Information that must be followed are detailed in the following Annexes:

- Annex A. Privacy-relevant Definitions
- Annex B. Information Privacy Statement and Collection Notice.
- Annex C. Requests for Access to Personal Information Procedure.
- Annex D. Information Communication Technology Acceptable Use Policy.
- Annex F. Records Management Policy (To be issued).

7.3.5 Prohibition on Disclosure\(^1\) of Personal Information
In law, no person with access to ATDP Personal Information is permitted to disclose Personal Information to any individual or organisation outside ATDP without the prior written consent of the person to which the Personal Information relates.

7.3.6 Information Transfer
ATDP may transfer Personal Information interstate or overseas for storage by contracted IT service providers.

Where ATDP transfers Personal information interstate or overseas it will:

1. comply with the provisions of the Privacy Act that relate to transborder data flows; and
2. take all reasonable steps to ensure that third party service providers do not use or disclose transferred Personal Information for a purpose other than that for which it was collected by ATDP.

7.3.7 Information Privacy Statement
ATDP collects Personal Information in accordance with ATDP’s Information Privacy Statement and Collection Notice (Annex B). The Notice:

---

\(^1\) Disclosure refers to release of Personal Information to another entity (e.g. a body, agency or person separate to ATDP) where ATDP will cease to have effective control of the information once it is released.
OPERATIONAL POLICY AND PROCEDURES LIBRARY

- stipulates the reasons for which ATDP collects and holds Personal Information about Candidates and Advocates, and
- nominates the situations in which ATDP may release Personal Information about Candidates and Advocates.

Before participating in ATDP activities, all Candidates and Advocates are required to:
- provide during enrolment the Personal Information identified in the Notice:
  - permit in writing disclosure of their Personal Information **ONLY** to the service providers identified in the Notice; and
  - sign and date a copy of the Notice and lodge it with their Region’s Program Support Officer (PSO).

7.3.8 Authorised Access to Personal Information
Privacy legislation permits access by ATDP staff, volunteers and service providers to Personal Information **ONLY** where this is necessary for work purposes.

Unless Clients’ files are redacted, Candidates, Mentors, Trainers and Assessors will need to access Clients’ personal information during training and assessment. Candidates are to ensure that their Clients’ Authorisation to Represent includes permission to disclose personal information for training and assessment purposes.

Day-to-day access to Personal Information is restricted to those ATDP staff, volunteers and service providers that require access to undertake the role and duties identified in their approved Job Statement.

In **NO** other circumstances, is Personal Information to be accessed without the written authorisation of the ADTP Privacy Officer (CFMG Chair). Such authorisation will be made **ONLY** on the grounds that disclosure is both necessary and acceptable in law.

7.3.9 Owner’s Access to their Personal Information
The Privacy Act provides:
- individuals with a legally enforceable right of access to, and amendment of their own personal information held by ATDP;
- unless this would, on balance, be contrary to the public interest.

Any person wishing to obtain access to, or to amend their Personal Information is to be:
- provided a copy of the Requests for Access to Personal Information Procedure (Annex C); and
- requested to complete a Request for Access to Personal Information (Appendix 1 to Annex C).

The applicant is to lodge the Request with their Region’s PSO.

The PSO is to confirm and record the validity of the Request and, pursuant to the law, facilitate access and/or amendment.
7.3.10 Restrictions on Release of Personal Information
The Privacy Act provides that access to certain documents, or to certain information contained in documents, may be refused to protect public interest or the private or business affairs of others.

The ATDP Privacy Officer (CFMG Chair) will usually refuse a request for access to documents that contain the Personal Information about the private affairs of others.

7.3.11 Refusal on Administrative Grounds
ATDP may refuse access to documents should identification, location and collation, or the volume of documents requested, incur a substantial and unreasonable workload.

If a request for access or amendment is refused, ATDP will provide written reasons for the decision and advise the applicant of their rights to appeal against the decision.

7.3.12 Protection of Personal Information
All persons with access to ATDP Personal Information must protect it against loss, unauthorised access or modification, disclosure or misuse.

7.3.13 Exclusions from this Policy
This policy does NOT apply to:

1. Routine Information;
2. Personal Information that is maintained and accessible in the public domain;
3. Information recorded in a de-identified way that cannot be linked (or re-linked) to a known individual;
4. Personal Information that is already available in a publication or other publicly available document; or
5. Information that is generally available.

7.3.14 Notifiable Breaches
Where collected or held by ATDP, the following Personal Information is subject to the Notifiable Data Breaches Scheme (NDB):²

1. Tax File Number of any person;
2. Agreements with the Commonwealth Government that require ATDP to be bound by the Privacy Act (e.g. research agreements, funding agreements);
3. Data subject to the Telecommunications (Interception and Access) Act 1979 (Cth);³ and
4. Personal Information collected or held under arrangements that would trigger a provision of the Privacy Act.

³ These data are Personal Information for the purposes of the Privacy Act.
7.3.15 Mandatory Reporting

If an ‘Eligible Data Breach’ occurs in any of the provisions at 7.3.14, notification of the Commonwealth Privacy Commissioner and the affected individual is mandatory.

7.3.16 Roles and Responsibilities

The following ATDP officers are responsible implementation of the provisions of the Privacy Act.

7.3.16.1 Chair of SGB

The Chair of SGB is the ‘Principal Officer’ under the Privacy Act and has overall responsibility for ATDP’s obligations under the Act.

7.3.16.2 General Counsel

In response to an applicant’s request, the DVA General Counsel as the Internal Review Officer under the Privacy Act is responsible for the internal review of the decision made by the Privacy Officer (refer to Annex C).

7.3.16.3 Privacy Officer

The Chair of CFMG is the ‘Privacy Officer’ under the Privacy Act and is responsible for the following:

1. Overseeing and implementing privacy management within ATDP.
2. Reviewing and approving privacy protocols.
3. Conducting privacy training.
4. Making initial decisions on access applications pursuant to the Privacy Act.
5. Coordinating ATDP’s investigation and response to any privacy complaints.

7.3.16.4 Regional Managers and Project Officers

Regional Managers and persons appointed to conduct ATDP projects are ‘Heads of Organisational Units’ under the Privacy Act. They are responsible for:

- managing privacy risk in the organisational unit and implementing business processes consistent with ATDP Privacy Policy; and
- ensuring compliance with information requests by locating information held in their areas.

If information cannot be located, a written explanation of what action was taken to locate the information is to be provided to the Privacy Officer (CFMG Chair).

7.3.16.5 Personal Information Custodians

The persons managing the ATDP Online Management System are ‘Personal Information Custodians’ under the Privacy Act. They are responsible for:

1. Complying with security measures to protect privacy of Personal Information located in ATDP information systems;
2. Determining appropriate user access levels which must be consistent with privacy requirements; and
3. Implementing appropriate mechanisms to revoke access to systems containing Personal Information, when access is no longer appropriate (eg. on change in position or formal responsibilities, or on termination of service provision).

7.3.16.6 Staff, Volunteers, Service Providers and Clients

Staff, volunteers and service providers:

- are to undertake privacy training;
- are to comply with:
  - the provisions of the Privacy Act,
  - this policy, and
  - all procedures and privacy instruments issued under the policy;
- may only access Personal Information when it is necessary to facilitate ATDP services;
- have an obligation to protect Personal Information against inappropriate use, unauthorised access, or modification, disclosure and/or mismanagement of Personal Information collected or held by ATDP; and
- must report all suspected data breaches to the Privacy Officer (CFMG Chair) in writing as soon as practicable.

7.3.17 Privacy Complaints

If an individual believes that ATDP has not handled their Personal Information in accordance with the Privacy Act, other relevant legislation, or this policy, they may make a complaint.

ATDP’s primary objective in responding to any privacy complaint is to conciliate an outcome that:

- is acceptable to the complainant; and
- addresses any broader or systemic privacy issues that may have arisen.

The following policy applies:

- A complaint must be made in writing or by email to:
  - the Privacy Officer (CFMG Chair), or
  - referred to the Privacy Officer if received by another officer of ATDP.
- The Privacy Officer is responsible for investigating and responding to the complaint.
- If a complainant does not agree with the Privacy Officer’s response, the complaint is to be referred to the General Counsel for internal review.
- If, on completion of the internal review process, the complaint is not satisfied with the handling or outcome of their complaint, the complainant may refer the matter for independent mediation through the Office of the Information Commissioner; see:
OPERATIONAL POLICY AND PROCEDURES LIBRARY

First, the wizard at:

Then, if progression by AOIC is appropriate:

7.3.18 Management of a Privacy Breach
The person responsible and actions to manage a breach of privacy follow.

7.3.18.1 Reporting of Privacy Breach
The Head of the relevant Organisational Unit must report any privacy breach to the Privacy Officer as soon as practicable after the breach has been identified.

7.3.18.2 Immediate Actions
Management of a privacy breach will include steps to:

1. contain the breach;
2. evaluate the associated risks;
3. consider notifying the affected individuals; and
4. prevent of any further privacy breach.

7.3.18.3 Serious Breaches of Privacy
The General Counsel is responsible for advising the Chair of SGB and the Delegate of the Secretary of all serious breaches of this policy and any actions arising out of any investigations of alleged breaches.

7.3.18.4 Notifiable Breach
If a Notifiable Breach (refer para 7.3.4) occurs, ATDP is obligated to inform the Australian Information Commissioner and the relevant individual(s).

Notifiable data breaches are to be managed in accordance with Personal Information – Data Breach Procedure (Annex E).

7.3.19 Policy Breach
The actions to be taken in the event of a breach of Privacy Policy follow.

7.3.19.1 Reporting
The Privacy Officer (CFMG Chair) is to report in writing to the General Counsel as soon as practicable all breaches of Privacy policy.

7.3.19.2 Inappropriate or Unauthorised Access
Inappropriate or unauthorised access by a staff member, volunteer, service provider or client of ATDP may be deemed misconduct and may result in:

- disciplinary action in accordance with Library 3, Chapter 10; and/or
- referral of the complaint to an external agency for further investigation.
7.3.19.3 **Authorised Exception**
Providing the activity has been authorised by the CFMG Chair, unauthorised or inappropriate access to Personal Information obtained during testing of system security controls (eg. penetration testing) does not constitute a Policy Breach.

7.4 **Communication and Information Management**
ATDP’s policies relating to communications and management of the broader suite of ATDP information follow.

Where any doubt exists about the nature of information, the privacy policy outlined at para 7.3 is to be applied.

7.4.1 **Australian Privacy Principles**
Australian Privacy Principles\(^4\) stipulate all Australian citizens Privacy rights and responsibilities.

The Principles apply to:
- all persons engaged in all ATDP activities, and
- all aspects of communication and information management by ATDP.

7.4.2 **Rationale**
Management and administration by the CFMG, RMG and CoP rely heavily on effective communication across the ATDP-CoP-VSC-ESO ICT network.

To militate against misunderstanding, and to ensure that communication threads are preserved, wherever possible:
- formal communications should be by email and, preferably, saved as a pdf and filed;
- notes should be taken of formal telephone and tele/video-conference calls; and
- social media posts of a formal nature should be copied and pasted into a pdf document and retained on file.

7.4.2 **Approved Information**
ATDP cannot control how information is used once it has been shared. Therefore, all members are responsible for ensuring that only approved formal information is released.

The formal information that members are free to disseminate will have been approved by the SGB and advised to members by the Secretariat.

While what formal information is to be released is centralised, how it is disseminated is the personal responsibility of each member. This frees each member to decide the language and medium best suited to the recipients. It also places the burden on each member to ensure that the facts are communicated unambiguously.

7.4.3 Ethos of Professionalism
Ensuring that approved information is disseminated widely, correctly and accurately is consistent with the characteristics of professionalism (Chapter 2.6.4). Amongst other things, the ethos of professionalism focuses members on:

- striving for the best possible outcomes, and
- accepting personal responsibility for their actions.

7.4.4 Considerations
These policies and procedures apply to the formal communication and management of information. The media that members may use to share formal ATDP information include:

- telephone and tele/video-conference calls;
- emails and social media;
- Newsletters;
- Updates; and
- face-to-face meetings and information sessions

Typical communication modalities that are covered by these policies and procedures include:

- use of established mailing lists to broadcast information widely
- general responses to operational queries that may have a wide or narrow range of recipients depending on the query
- communications for an internal audience and not for general release
- targeted communications covering recipient-specific issues/information

Each modality requires a different level of consideration and care in its drafting, communicating, responding and subsequent storage. Irrespective of the modality, the completeness and accuracy of the information communicated is critical.

7.4.5 Participants’ Responsibilities
As a general rule, formal communications should be commensurate with the level of responsibility of the sender. Specific guidance to participants’ responsibilities follows.

7.4.5.1 Policy and Procedures
Communication of policy will come from the:

- SGB Chair: strategic governance, direction and policy.
- CFMG Chair/Deputy Chair: operational policy and procedures.
- NTM: learning and development policy and procedures.

7.4.5.2 Meetings, Minutes and Internal Correspondence
Each Tier will:

- convene meetings formally through an agenda
- record actions supported by relevant detail in minutes
OPERATIONAL POLICY AND PROCEDURES LIBRARY

- use emails for all internal correspondence

7.4.5.3 Implementation
Communication of implementation instructions and information will come from the:
- CFMG Chair/Deputy Chair: training and development support activities.
- NTM: training and development activities.
- Regional Managers: implementation of national policy and procedures.
- Regional Mentors: implementation of national training and development policy and procedures

7.4.5.4 Referral
Other members would not generate communications on policy, procedures or implementation. Should the need arise they would refer any requests to their respective Chair/Regional Manager.

7.4.5.5 Requests and Complaints
Requests for information and complaints should be handled in accordance with the management procedures at Library 4, Chapter 21.

7.4.5.6 Information Copying
Members generating responses to matters that have been referred, should ensure that the referring member receives information copies of responses.

7.4.5.7 Doubt
If there is any doubt about how a proposed response should be progressed it should be discussed with the appropriate Chair before any action is taken.

7.4.6 Guidelines
Members will:
- ensure that confidential information is not sent by email or posted on social media;
- not share internal ATDP communications with any external parties without the permission of the originator;
- not copy any communication, including attachments without the permission of the originator;
- not attribute personal views or comments made in communications or forums to ATDP or as representing the views or position of the ATDP;
- only use the reply to all function if it is necessary for all recipients to see the response;
- not leave out the message thread as it provides important context and history;
- refrain from any comments about the content of emails other than providing factual information; and
- contain critical comment about ATDP decisions, policy and practices within ATDP.
7.4.7 Response to Infractions
Infractions of this policy are to be managed in accordance with the procedures at Library 3, Chapter 10.

Annexes
A. Definitions
B. Information Privacy Statement and Collection Notice.
C. Requests for Access to Personal Information Procedure.
D. Information Communication Technology Acceptable Use Policy.
E. Personal Information – Data Breach Procedure.
F. Records Management Policy (To be issued).
Definitions

The terms and policy stipulated in the relevant legislation are.

Administrative Release
Administrative Release refers to a discretionary process that allows access to information, in full or in part, in certain types of administrative or operational records. Such records are generally released as a matter of course, in response to a request, without the need for a formal application under legislation.

Clients
Clients are the ESO and VSC personnel who engage the services and Service Providers coordinated by ATDP.

Deliberate Misuse
Deliberate Misuse means the wrong or improper use of Personal Information, done consciously and intentionally (on purpose). This includes un-authorised modification of Personal Information.

Document
A Document, other than a document to which privacy legislation does not apply, is:

- a document in the possession of, or
- under the control of ATDP,
- whether brought into existence or received by ATDP, and
- includes:
  - a document that ATDP is entitled to access, and
  - in the possession, or
  - under the control of an officer of ATDP in the officer’s official capacity.

A Document may be in hard copy or electronic format and include files, reports, emails, correspondence, computer printouts, maps, plans, photographs, and audio and video recordings.

Inappropriate Use
Inappropriate Use means access to and use of personal information which is not appropriate to the individual’s role or function at the time: for example, viewing the health records of an individual out of personal interest.

Notifiable Breach
The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), also referred to as the Notifiable Data Breaches (NDB) Scheme amends the Privacy Act; see:

An eligible data breach occurs if:

1. there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity;
2. the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates; and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

**Personal Information**

Personal Information is defined by the IP Act as:

- information or an opinion,
- including information or an opinion forming part of a database,
- whether true or not, and
- whether recorded in a material form or not,
- about an individual whose:
  - identity is apparent, or
  - can reasonably be ascertained from the information or opinion.

Personal information includes usernames, passwords and Unique Identifiers such as staff and student numbers.

It can be recorded in any format including hard copy documents, electronic documents, databases, administrative systems, photographs and other images, and identity cards.

**Personal Information Custodian**

A Personal Information Custodian is an appointed member who has responsibilities for the collection and management of Personal Information within ATDP. This may include records managers, support and client services assistants, service coordinators and system administrators.

**Privacy Breach**

A Privacy Breach occurs when there is a failure to comply with the information privacy policy or the IP Act’s 11 information privacy principles (IPPs). Usually this will be the result of Inappropriate Access or Unauthorised Access, and may result in unauthorised disclosure of Personal Information.

**Privacy Complaint**

A Privacy Complaint is a complaint about an act or practice of ATDP in relation to an individual’s Personal Information that is a breach of the applicable legislation or this policy.

**Routine Information**

Routine Information is information that is solely and wholly related to the routine work duties and responsibilities of members of ATDP.
This includes information such as position title, email address, public phone numbers, opinions given in a professional capacity, authorship of documents, incidental appearances of names and attributable details in official documents, information about qualifications held, or any information which is publicly available.

**Service Providers**
A Service Provider is an external provider of services formally engaged by ATDP as part of its operations.

**Staff**
Staff includes employees (including independent contractors) engaged by ATDP under an employment instrument.

**Unauthorised Access**
Unauthorised Access means obtaining and exercising access to personal Information, for which they are not authorised (by role or function) to access.

**Unique Identifiers**
Unique Identifiers may include official staff, volunteer or client numbers which may be used as the basis for recording a large amount of personal information. Other unique identifiers include payroll numbers, tax file numbers, credit card numbers and bank account details.

**Volunteers**
Volunteers are personnel who give their time without compensation to assist with the facilitation of ATDP’ operations.