

# Important Terms

In order to properly understand the Australian Privacy Principles (APPs) it is essential to have an understanding of key terms and concepts that have specific meaning in the privacy context.

These terms are defined below and guidance provided to assist in the understanding of the terms generally and in the Defence context. On this page, the term 'Defence' is used and includes the Department of Defence, the Australian Defence Force and Defence Cadet organisations.

## Agency

Under the [Privacy Act 1988](#), Defence is considered an agency. The term 'agency' includes:

- federal government departments (e.g. Defence, and the Department of Human Services);
- Commonwealth administrative bodies or organisations (e.g. the Australian Human Rights Commission, and Questacon: the National Science and Technology Centre);
- federal courts (e.g. Federal Court of Australia);
- federal law enforcement agencies (e.g. the Australian Federal Police); or
- federal government ministers and their staff (e.g. the Minister for Defence, and the Minister for Foreign Affairs).

**Note:** Under the Privacy Act, a government minister (and his or her staff) and the Minister's department are considered to be separate agencies, and thus separate APP entities. Accordingly, Defence and the Minister for Defence are considered to be separate agencies.

The separation of Defence and the Minister for Defence means that when any personal information is exchanged between Defence and the Minister, the exchange is considered to be a disclosure of personal information. For more information, see 'Disclosure'.

### Defence and the term 'agency'

Defence is an 'agency' under the Privacy Act. This includes the Department of Defence, the Australian Defence Force and Defence Cadet organisations and statutory office holders, whose positions have been established under a law for the purpose of Defence. However the APPs do not apply to the activities of some parts of Defence, those being: Australian Imagery and Geospatial Organisation, the Australian Intelligence Organisation and the Australian Signals Directorate.

### Statutory office holders explained

While the definition of agency also includes:

- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or
- a person holding or performing the duties of an appointment, being an appointment made by the Governor General, or by a Minister, otherwise than under a Commonwealth enactment;

Subsection 6(5)(c) of the Privacy Act provides that:

For the purposes of this Act, a person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of an office established by or under a Commonwealth enactment for the purposes of an agency;

This means that Defence statutory office holders, like the Chief of the Defence Force, the Service Chiefs, the Inspector General of the Australian Defence Force and the Registrar of Military Justice, are NOT considered to be separate agencies from Defence for privacy purposes. Consequently:

- personal information passing between these office holders and Defence would constitute a use of that information and not a disclosure; and
- there is no need for these statutory office holders to have their own APP 1 privacy policy.

### **Acts by a person employed in an agency**

An act done or practice engaged in by, or information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of the person's employment shall be treated as having been done or engaged in by, or disclosed to, the agency.

Accordingly, Defence may be responsible for the actions of a Defence member or Defence APS employee who is acting in the course of their duties if they act contrary to the APPs. This may also include contractors to Defence.


## **APP entity**

An 'APP entity' is defined as either an either an **agency** or an **organisation**. As an agency, Defence is considered an APP entity.


Sometimes, the Australian Privacy Principles refer to an 'APP entity that is an agency' and an 'APP entity that is an organisation'. Only principles that refer to an APP entity or an 'APP entity that is an agency' apply to Defence.

## **Collection**

An entity 'collects' personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

 [APP 3](#) regulates the collection of personal information generally. A collection of personal information can be either solicited or unsolicited.

A solicited collection happens when personal information is provided to Defence on request. For example, a Defence recruiting centre asking an applicant to fill out recruitment forms, or a Defence member submitting an application for an entitlement, would involve Defence collecting solicited information.

An unsolicited collection happens when personal information is passed to Defence without the information being requested. For example, a Defence APS employee lodging a Review of Actions would involve Defence receiving unsolicited information. In addition to APP 3,  [APP 4](#) imposes obligations on the collection of unsolicited personal information.

A collection of personal information may also arise out of information Defence creates. For example, if a Defence member were to have a fitness assessment, and the results of that assessment were put into a record, those results would be considered to have been collected.

Sometimes the collection of one person's personal information may include the collection of another person's personal information, too. For example, next of kin information.

If personal information is obtained in a conversation, but is not going to be put into a record, the information will not be 'collected'. But, if that personal information is recorded for official purposes, or is to be later put into a record of conversation or file note, the personal information would have been collected.

## **Consent**

Consent may either be 'express' or 'implied'. The Office of the Australian Information Commissioner states:

**Express consent** is given explicitly, either orally or in writing. This could include a handwritten signature or an oral statement to signify agreement.

**Implied consent** arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

An example of implied consent would be if a Defence member submits a redress of grievance to their commanding officer. The Defence member's consent to use personal information that is necessary to respond to the grievance would be implied.

Consent requires the following:

- a. it must be voluntary;
- b. it must be informed;
- c. it must be current and specific; and
- d. it must involve the capacity to understand what the consent is being provided for.

## Disclosure

(See **Use and disclosure**)

## Enforcement body and enforcement related activity

### Enforcement body

The definition of an 'enforcement body' includes a number of agencies, such as:

- the Australian Federal Police;
- Customs;
- the Immigration Department;
- Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory;
- a police force or service of a State or a Territory. (This is not a complete list)

An enforcement body also includes other agencies, such as Defence:

- to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
- to the extent that it is responsible for administering a law relating to the protection of the public revenue.

Defence is not an enforcement body generally, but parts of Defence may be when doing particular activities, such as:

- ADFIS;
- the Office of the Director of Military Prosecutions (ODMP).

Other parts of Defence may also be an Enforcement body, but this needs to be considered on a case by case basis.

### Enforcement related activities

'Enforcement related activities' may include 'the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations.' This may include investigations into a suspected breach of the [APS Code of Conduct](#) or a suspected breach of the [Defence Force Discipline Act 1982](#). A full list of enforcement related activities can be found in section 6 of the [Privacy Act 1988](#).

# Health information

(See **Personal information**)

## Permitted general situation


'Permitted general situations' are circumstances that provide exemptions to the general limitation on the collection, use and disclosure of personal information. To determine if they apply, you need to look at the relevant Australian Privacy Principle.

The permitted general situations are explained in more detail in the  [OAIC APP guidelines](#) (chapter C).

## Permitted health situation

A 'permitted health situation' is like a permitted general situation except that it applies only to the collection, use or disclosure of health information. Permitted health situations only apply to organisations, therefore they do not apply to Defence.

## Personal information

The  [Privacy Act 1988](#) defines 'personal information' as:

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

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

Personal information:

- includes sensitive information and health information;
- does not have to be true or confirmed. For example, an opinion about an identified person would be considered personal information;
- does not have to be written down. For example, telling a work colleague information about a person over the phone could be considered a use of personal information;
- could be a painting, photograph or voice recording of a person who is reasonably identifiable.
- does NOT include information about companies or the deceased.

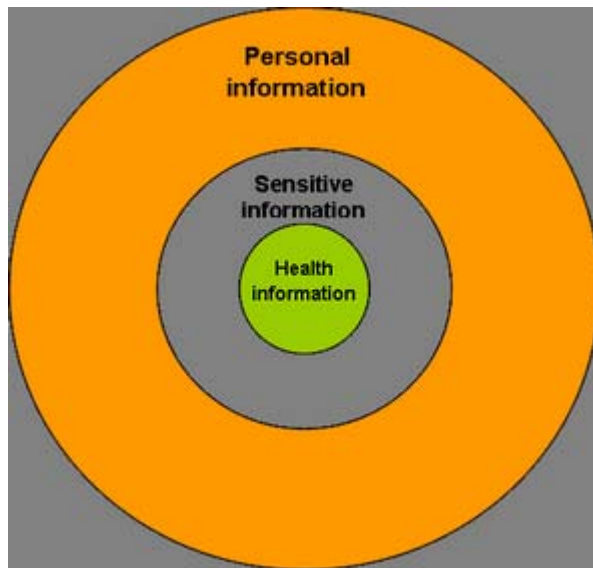
An individual does not have to be reasonably identifiable from the personal information alone, the use of other sources of information, where available may mean that sometimes information will be personal information and sometimes it won't be. A person may be reasonably identifiable by having regard to:

- the nature and extent of the information;
- the circumstances of its use and disclosure;
- context in which the information is being used or disclosed.

**Example:** Most people outside of Defence would not be able to use a PMKeyS number to identify a person because they would not have access to the Defence resources to do so. Thus, a PMKeyS number lost in a shopping mall is not personal information. However, the same number written on a white board in Russell Offices is more likely to be personal information because a person in Defence may be able to use Defence resources to identify a person from that PMKeyS number.

### Subsets of personal information

Personal information is also broken down into sensitive information and health information.



Subsets of personal information

## Sensitive information

'Sensitive information' is a subset of personal information that attracts additional conditions when collecting, using and disclosing. Sensitive information includes:

- 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 preferences or practices; or
  - ix. criminal record;
  - x. 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.

Specific rules apply to the collection of sensitive information. These rules are detailed on the [APP 3](#) page.

## Health information

'Health information' is a subset of sensitive information and includes:

- a. information or an opinion about:
  - i. the health or a disability (at any time) of an individual; or
  - ii. an individual's expressed wishes about the future provision of health services to him or her; or
  - iii. a health service provided, or to be provided, to an individual;
  - iv. that is also personal information; or
- b. other personal information collected to provide, or in providing, a health service; or
- c. other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- d. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

# Quality of personal information

APP 10 requires an APP entity to take reasonable steps to ensure that personal information collected is 'accurate', 'up-to-date', 'complete' and 'relevant'. These terms are discussed below.

## Accurate

Personal information may be inaccurate if it contains an error or is misleading. A record of a person's opinion, may be accurate if it reflects their opinion, even if it is factually inaccurate or another person disagrees with it.

## Complete

Personal information may be incomplete if it only reflects a partial or misleading picture. Whether the information is complete will depend on the purpose for which it will be used or disclosed. For example, where a person lives may be the country, the State or Territory, the suburb or a full residential address; whether this information is complete will depend on the purpose of the information. A suburb only would not be complete information for the purpose of visiting the individual.

What is 'accurate and complete' is self explanatory.

## Up-to-date

Anytime after information is collected, that information has the potential to become out-of-date. The likelihood of this occurring depends on the type of information collected and its purpose.

**For example:** A person's address will change when they move and will be out-of-date if you need to write to them. The address will remain up-to-date if it were collected for the purpose of knowing where the person lived at the time it was collected.

## Relevance

When using/disclosing personal information, it must be relevant to the matter at hand. There needs to be some relationship between the personal information to be used/disclosed and the particular purpose of the use or disclosure.

**For example:** The collection of the number, age and sex of a member's children may be relevant to determining the type of Service residence he/she may be entitled to because it is based on family make-up. However, this information would not be relevant to determining what qualifications the member has.

# Sensitive information

(See **personal information**)

# Use and disclosure

The distinction between use and disclosure needs to be understood because the two attract different obligations. While the distinction between use and disclosure is less important under the APPs (compared with the former Information Privacy Principles) it is still necessary to have an understanding of these terms as some different requirements still apply.

## Use

Generally, an APP entity 'uses' personal information when it handles and manages that information **within** the entity. A simple way to think about this is when personal information is used by, or transferred between,

individuals, work areas, groups and/or services **within** Defence, this exercise is considered a use of the personal information. As an example, sending an email that contains personal information to a Defence work colleague, or reading a work file, would be considered a use of personal information.

Remember that the APP entity is 'Defence', so when one service (eg: Navy) gives personal information to another (eg: Army), this is still a use.

Sometimes, we need a more complex understanding of use, for example when we are dealing with contractors, such as service providers. In these circumstances we need to look at whether Defence retains **effective control** of the information. This is usually done under contract. In these circumstances, there would still be a use, as Defence retains effective control over the personal information.

## Disclosure

A 'disclosure' of personal information refers to a situation in which an APP entity loses effective control of that information. This loss of control can be intentional or unintentional, and lawful or unlawful.

Generally, an APP entity discloses personal information when it gives that information to someone outside the entity. As an example, a lawful disclosure most commonly happens when Defence provides personal information to the Minister, another agency or to an individual.

In some circumstances the provision of personal information between Defence personnel can be considered a disclosure. If the person receiving the information is acting in their personal capacity, rather than in the course of duty, this would be a disclosure. For example, a disclosure would occur when a manager gives a copy of a quick assessment, in response to a complaint, to one of the people involved.

An example of an unlawful disclosure would involve a unit putting a Defence member's personal information on the Defence internet, where members of the public can then access that information, without their permission.

Use =	within Defence	Defence retains effective control of the information
Disclosure =	outside of Defence	Defence loses effective control of the information