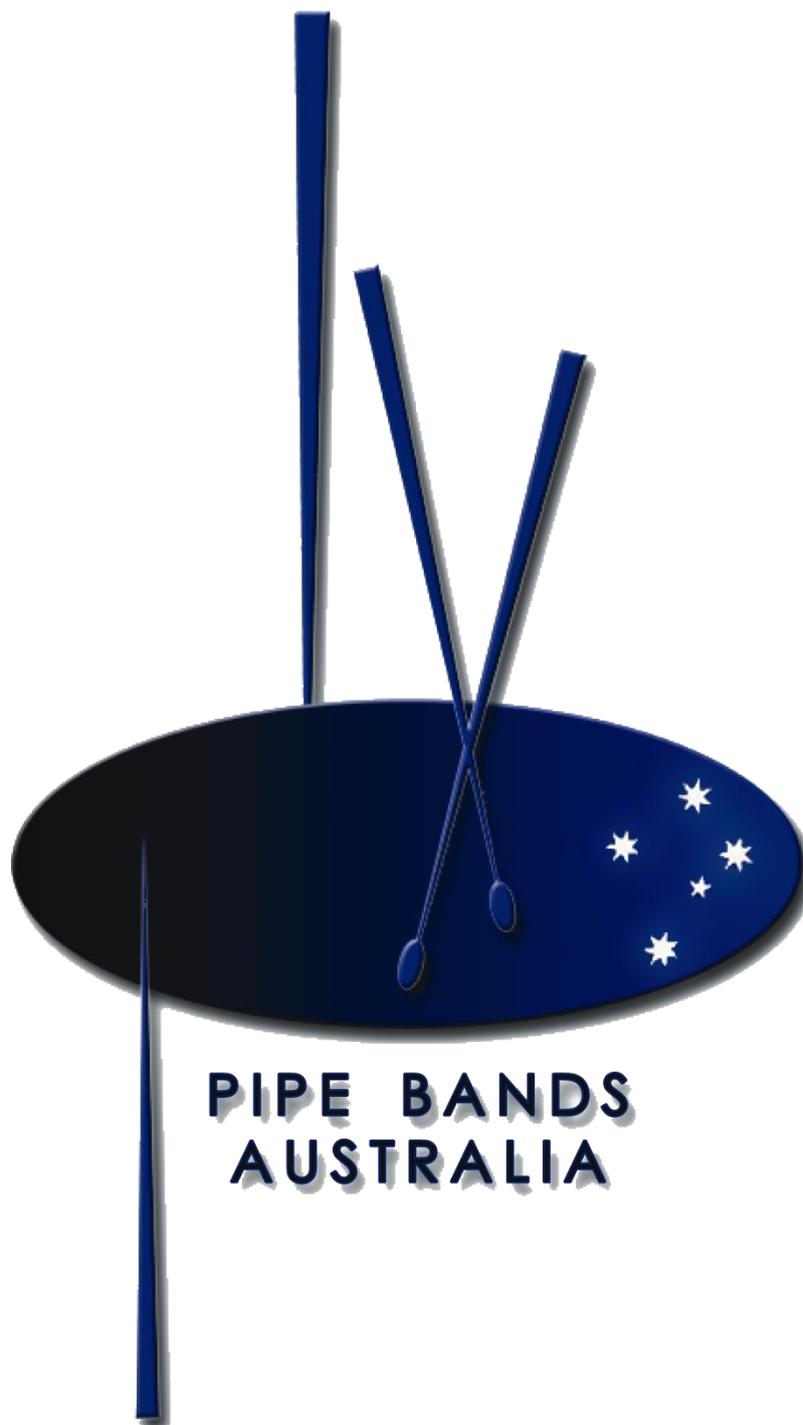


PRIVACY POLICY

of

PIPE BANDS AUSTRALIA INC
(A0035346S)



**PIPE BANDS
AUSTRALIA**

Version 1.2 - Update adopted 07 July 2014

Contents

Part A - PRIVACY POLICY	3
1. POLICY STATEMENTS	3
Part B – GUIDING STATEMENTS.....	4
2. General	4
3. Definitions	4
CHANGES TO THE PRIVACY ACT	4
4. At a glance	4
5. Background and overview	5
6. The four key changes to the pre-existing NPPs are:.....	5
7. Cross-border disclosure of personal information	5
THE AUSTRALIAN PRIVACY PRINCIPLES	7
Part 1 - Consideration of personal information privacy	7
1. Australian Privacy Principle 1 - Open and transparent management of personal information 7	
2. Australian Privacy Principle 2 - Anonymity and pseudonymity.....	7
Part 2 - Collection of personal information	8
3. Australian Privacy Principle 3 - Collection of solicited personal information	8
4. Australian Privacy Principle 4 - Dealing with unsolicited personal information	9
5. Australian Privacy Principle 5 - Notification of the collection of personal information.....	9
Part 3 - Dealing with personal information	10
6. Australian Privacy Principle 6 - Use or disclosure of personal information	10
7. Australian Privacy Principle 7 - Direct marketing	11
8. Australian Privacy Principle 8 - Cross-border disclosure of personal information.....	13
9. Australian Privacy Principle 9 - Adoption, use or disclosure of government related identifiers	13
Part 4 - Integrity of personal information.....	14
10. Australian Privacy Principle 10 - Quality of personal information	14
11. Australian Privacy Principle 11 - Security of personal information.....	14
Part 5 - Access to, and correction of, personal information.....	15
12. Australian Privacy Principle 12 - Access to personal information	15
13. Australian Privacy Principle 13 Correction of personal information.....	16

Part A - PRIVACY POLICY

1. POLICY STATEMENTS

- 1.1. Pipe Bands Australia Inc. [“the association”] affirms the Australian Privacy Principles.
- 1.2. The association’s primary purpose in collecting information is to pursue its purposes as set out in its Rules in accordance with relevant Acts of Parliament, regulations and its rules and procedures.
- 1.3. It collects personal information from members and intending members to the least extent reasonably enabling it to carry out its stated primary purpose.
- 1.4. It collects sensitive information as permitted to the least extent possible.
- 1.5. It manages personal and sensitive information held by it in accordance with Australian Privacy Principles. In particular, the Council directs all officers and members of the association that the disclosure of any such information to which an officer or member may become privy is permitted only to an officer or member of the association who has an immediate and direct need to have that information, and otherwise only with the consent of the person whose information it is or in accordance with the law.
- 1.6. Disclosure of any personal or sensitive information to a law-enforcement or other interested agency for investigation or prosecution of an illegality must be recorded in writing without delay, and a copy of that record passed to the Secretary for filing.
- 1.7. Disclosure of personal information in accordance with the primary purpose above shall be recorded in a register kept for the purpose.
- 1.8. The statutory rights of access to information and to its correctness and being up to date shall be faithfully observed by the association and its officers.
- 1.9. Personal and sensitive information shall be destroyed promptly upon it becoming out of date or of no continuing use in the operations of the association and the fulfilment of its purposes and a record shall be kept of the destruction of that information.

Part B – GUIDING STATEMENTS

2. General

- 2.1. These notes seek to indicate the nature of the restrictions affecting the association's collection and release of information, and a mention of privacy issues arising from security surveillance of association premises and property.

3. Definitions

- 3.1. "personal information" means 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. [Section 6 (1)]
- 3.2. "Sensitive information" means
 - 3.2.1. information or an opinion about an individual's
 - 3.2.1.1. racial or ethnic origin; or
 - 3.2.1.2. political opinions; or
 - 3.2.1.3. membership of a political association; or
 - 3.2.1.4. religious beliefs or affiliations; or
 - 3.2.1.5. philosophical beliefs; or
 - 3.2.1.6. membership of a professional or trade association; or
 - 3.2.1.7. membership of a trade union; or
 - 3.2.1.8. sexual preferences or practices; or
 - 3.2.1.9. criminal recordthat is also personal information; or
 - 3.2.2. health information about an individual.

CHANGES TO THE PRIVACY ACT¹

4. At a glance

- New amendments to the Privacy Act came into force on 12 March 2014.
- You will need to review and most likely update your privacy policy and your collection statement (that is, the statement you provide to individuals when you collect their personal information).
- You will also need to review and most likely update your internal practices about how you collect and manage personal information. You may also need to review how your organisation's IT systems store and manage personal information, as well as reviewing the security of those systems.
- Credit providers and credit reporting bodies will need to seek detailed advice relating to their specific business practices.
- The Australian Privacy Commissioner will have new powers to investigate and penalise non-compliance.

¹ The text derived from Privacy Compliance Package Manual by Norton Rose Fulbright, Australia is gratefully acknowledged.

5. Background and overview

The Privacy Act regulates the collection, use, storage and disclosure of personal information in Australia.

In the period before 12 March 2014, personal information is defined in the Privacy 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.”

After 12 March 2014, the definition of personal information is replaced by a similar definition:

“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.”

The phrase “reasonably identifiable” deals with the concept of data matching. Data matching occurs where data about an unidentified individual is linked or matched with other data with the effect of causing the individual to become identified. This is sometimes called re-identification. The concept of “reasonably identifiable” is important and relevant to any organisation that intends to disclose anonymised or de-identified personal information (eg. to research or analytics organisations).

The previous NPPs applied to the private sector generally (to organisations having an annual turnover greater than AU\$3 million). The amendments to the Privacy Act have introduced numerous changes to Australia’s privacy regime, including the replacement of the NPPs with a new set of APPs, which took effect on and from 12 March 2014. The APPs will apply to any organisation that must previously have had to comply with the NPPs, and such organisations are defined in the Privacy Act as **APP entities**.²

On their commencement, the APPs will apply to existing collections of personal information. They will also apply to any arrangements that are already in place concerning the use of personal information, including contractual arrangements between organisations and their service providers or any other parties to whom organisations disclose personal information. In effect, this means that the APPs will have a retrospective effect on your organisation’s existing collections and databases of personal information and to your organisation’s contractual arrangements.

6. The four key changes to the pre-existing NPPs are:

- updated requirements for privacy policies and collection statements;
- dealing with unsolicited personal information;
- direct marketing; and
- cross-border disclosure of personal information.

7. Cross-border disclosure of personal information

Another significant change to the Privacy Act comes in a tightening of the rules on cross-border data flows. APP 8, which replaces the old NPP 9, requires an organisation to ensure that, before disclosing personal information to an overseas recipient, it takes such steps as are reasonable to ensure that the recipient does not breach the APPs in relation to that information.

² Although by this definition Pipe Bands Australia is not an APP Entity, its Privacy Policy states that it affirms the Australian Privacy Principles.

The concept of “reasonable” is intended to be flexible and adjust to each organisation’s individual circumstances. The reasonable steps used by many organisations are the imposition of contractual obligations between themselves and the overseas recipient (who could be a data processor or a provider of outsourcing or cloud computing services). A question then arises: what contractual provisions are sufficient?

The Privacy Commissioner has previously indicated that a simple and general contractual clause will not be sufficient in many cases if it merely requires the overseas recipient to comply with the Privacy Act. Instead, contractual clauses should itemise key privacy requirements and be accompanied by additional provisions such as warranties, audit rights and indemnities in appropriate cases.

The new section 16C of the Privacy Act provides additional motivation for Australian organisations to protect themselves in their dealings with overseas recipients. Under section 16C, an organisation can be deemed to be liable for a breach of the APPs by an overseas recipient of personal information disclosed by the organisation.

The “reasonable steps” requirement under APP 8.1 will apply unless the organisation can take advantage of one of the exceptions in APP 8. The main exceptions are:

- the organisation reasonably believes (after making enquiries) that the overseas recipient is subject to laws that protect information in a substantially similar way to the APPs and there are ways for the individual to take steps to enforce those laws; or
- the individual consents to the cross border disclosure after being informed that their consent means that APP 8.1 will not apply. Previously, a simple consent was enough and did not require any preliminary explanation to the individual of the circumstances.

An important change in APP 8 is the change in terminology from ‘transfer’ to ‘disclosure’. This change means that organisations will need to consider whether, even if the information is stored in Australia, a disclosure has been made to an overseas entity if that entity can access the information that is being stored in Australia. Conversely, the mere archiving or storage of personal information overseas (if it cannot be accessed overseas) will probably not be a disclosure and therefore not subject to APP 8. However, disclosure has not been defined and it remains to be seen how broadly the term will be interpreted.

APP 8 will be of particular concern to organisations using technologies involving the transfer of personal information such as outsourcing, off shoring or cloud computing.

Organisations should consider their contractual arrangements with any overseas third party to whom they transfer personal information and ensure that they include detailed privacy obligations in their agreements. Despite some general guidance by the Privacy Commissioner, there is no definitive guidance about how detailed contractual provisions need to be in order to comply with APP 8.1.

When considering overseas disclosures, organisations will also need to determine where the personal information is to be stored. It may be the case that the personal information will be stored in multiple locations around the world. Further, these storage locations may change. It is important to ascertain from your IT staff or from your IT service provider:

- where will the personal information we collect be stored?
- how often will the storage location change?

THE AUSTRALIAN PRIVACY PRINCIPLES

Part 1 - Consideration of personal information privacy

1. Australian Privacy Principle 1 - Open and transparent management of personal information

1.1. The object of this principle is to ensure that organisations manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2. An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

- (a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and
- (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3. An APP entity must have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the entity.

1.4. Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

- (a) the kinds of personal information that the entity collects and holds;
- (b) how the entity collects and holds personal information;
- (c) the purposes for which the entity collects, holds, uses and discloses personal information;
- (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- (e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- (f) whether the entity is likely to disclose personal information to overseas recipients;
- (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5. An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

- (a) free of charge; and
- (b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6. If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

2. Australian Privacy Principle 2 - Anonymity and pseudonymity

2.1. Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2. Subclause 2.1 does not apply if, in relation to that matter:

- (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
- (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2 - Collection of personal information

3. Australian Privacy Principle 3 - Collection of solicited personal information

Personal information other than sensitive information

- 3.1. If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
- 3.2. If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

- 3.3. An APP entity must not collect sensitive information about an individual unless:
 - (a) the individual consents to the collection of the information and:
 - i. if the entity is an agency - the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
 - ii. if the entity is an organisation - the information is reasonably necessary for one or more of the entity's functions or activities; or
 - (b) subclause 3.4 applies in relation to the information.
- 3.4. This subclause applies in relation to sensitive information about an individual if:
 - (a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
 - (b) a permitted general situation exists in relation to the collection of the information by the APP entity; or
 - (c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or
 - (d) the APP entity is an enforcement body and the entity reasonably believes that:
 - i. if the entity is the Immigration Department – the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or
 - ii. (ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
 - (e) the APP entity is a non-profit organisation and both of the following apply:
 - i. the information relates to the activities of the organisation;
 - ii. the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

- 3.5. An APP entity must collect personal information only by lawful and fair means.
- 3.6. An APP entity must collect personal information about an individual only from the individual unless:
 - (a) if the entity is an agency:

- i. the individual consents to the collection of the information from someone other than the individual; or
 - ii. the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or
- (b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7. This principle applies to the collection of personal information that is solicited by an APP entity.

4. Australian Privacy Principle 4 - Dealing with unsolicited personal information

4.1. If:

- (a) an APP entity receives personal information; and
- (b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2. The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3. If:

- (a) the APP entity determines that the entity could not have collected the personal information; and
- (b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4. If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

5. Australian Privacy Principle 5 - Notification of the collection of personal information

5.1. At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

- (a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or
- (b) to otherwise ensure that the individual is aware of any such matters.

5.2. The matters for the purposes of subclause 5.1 are as follows:

- (a) the identity and contact details of the APP entity;
- (b) if:
 - i. the APP entity collects the personal information from someone other than the individual; or
 - ii. the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

- (c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or

- authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);
- (d) the purposes for which the APP entity collects the personal information;
 - (e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
 - (f) any other APP entity, body or person, or the types of any other organisations, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
 - (g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
 - (h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
 - (i) whether the APP entity is likely to disclose the personal information to overseas recipients;
 - (j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3 - Dealing with personal information

6. Australian Privacy Principle 6 - Use or disclosure of personal information

Use or disclosure

- 6.1. If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:
- (a) the individual has consented to the use or disclosure of the information; or
 - (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

- 6.2. This subclause applies in relation to the use or disclosure of personal information about an individual if:
- (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
 - i. if the information is sensitive information—directly related to the primary purpose; or
 - ii. if the information is not sensitive information—related to the primary purpose; or
 - (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
 - (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or
 - (d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
 - (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3. This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

- (a) the agency is not an enforcement body; and
- (b) the information is biometric information or biometric templates; and
- (c) the recipient of the information is an enforcement body; and
- (d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4. If:

- (a) the APP entity is an organisation; and
- (b) subsection 16B(2) applied in relation to the collection of the personal information by the entity; the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5. If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6. If:

- (a) an APP entity is a body corporate; and
- (b) the entity collects personal information from a related body corporate; this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7. This principle does not apply to the use or disclosure by an organisation of:

- (a) personal information for the purpose of direct marketing; or
- (b) government related identifiers.

7. Australian Privacy Principle 7 - Direct marketing

Direct marketing

7.1. If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2. Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- (a) the organisation collected the information from the individual; and
- (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
- (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- (d) the individual has not made such a request to the organisation.

7.3. Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- (a) the organisation collected the information from:

- i. the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
- ii. someone other than the individual; and
- (b) either:
 - i. the individual has consented to the use or disclosure of the information for that purpose; or
 - ii. it is impracticable to obtain that consent; and
- (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- (d) in each direct marketing communication with the individual:
 - i. the organisation includes a prominent statement that the individual may make such a request; or
 - ii. the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and
- (e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4. Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5. Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

- (a) the organisation is a contracted service provider for a Commonwealth contract; and
- (b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and
- (c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6. If an organisation (the first organisation) uses or discloses personal information about an individual:

- (a) for the purpose of direct marketing by the first organisation; or
- (b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

- (c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and
- (d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and
- (e) request the first organisation to provide its source of the information.

7.7. If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

- (a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and
- (b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

- (a) This principle does not apply to the extent that any of the following apply:
- (b) the Do Not Call Register Act 2006;

- (c) the Spam Act 2003;
- (d) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

8. Australian Privacy Principle 8 - Cross-border disclosure of personal information

8.1. Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

- (a) who is not in Australia or an external Territory; and
- (b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2. Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

- (a) the entity reasonably believes that:
 - i. the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
 - ii. there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- (b) both of the following apply:
 - i. the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;
 - ii. after being so informed, the individual consents to the disclosure; or
- (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or
- (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or
- (f) the entity is an agency and both of the following apply:
 - i. the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
 - ii. the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

9. Australian Privacy Principle 9 - Adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1. An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

- (a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or
- (b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2. An organisation must not use or disclose a government related identifier of an individual unless:

- (a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or
- (b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or
- (c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or
- (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or
- (e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- (f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3. This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

- (a) the identifier is prescribed by the regulations; and
- (b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and
- (c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

9.4. Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4 - Integrity of personal information

10. Australian Privacy Principle 10 - Quality of personal information

- 10.1. An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.
- 10.2. An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

11. Australian Privacy Principle 11 - Security of personal information

- 11.1. If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
 - (a) from misuse, interference and loss; and

- (b) from unauthorised access, modification or disclosure.
- 11.2. If:
- (a) an APP entity holds personal information about an individual; and
 - (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and
 - (c) the information is not contained in a Commonwealth record; and
 - (d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5 - Access to, and correction of, personal information

12. Australian Privacy Principle 12 - Access to personal information

Access

- 12.1. If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

- 12.2. If:
- (a) the APP entity is an agency; and
 - (b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:
 - i. the Freedom of Information Act; or
 - ii. any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

- 12.3. If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:
- (a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
 - (b) giving access would have an unreasonable impact on the privacy of other individuals; or
 - (c) the request for access is frivolous or vexatious; or
 - (d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or
 - (e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
 - (f) giving access would be unlawful; or
 - (g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or
 - (h) both of the following apply:
 - i. the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
 - ii. giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

- (i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- (j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4. The APP entity must:

- (a) respond to the request for access to the personal information:
 - i. if the entity is an agency—within 30 days after the request is made; or
 - ii. if the entity is an organisation—within a reasonable period after the request is made; and
- (b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5. If the APP entity refuses:

- (a) to give access to the personal information because of subclause 12.2 or 12.3; or
- (b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6. Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7. If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8. If:

- (a) the APP entity is an organisation; and
- (b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9. If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

- (a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- (b) the mechanisms available to complain about the refusal; and
- (c) any other matter prescribed by the regulations.

12.10. If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

13. Australian Privacy Principle 13 Correction of personal information

Correction

13.1. If:

- (a) an APP entity holds personal information about an individual; and
- (b) either:
 - i. the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

- ii. the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2. If:

- (a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and
- (b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3. If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

- (a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- (b) the mechanisms available to complain about the refusal; and
- (c) any other matter prescribed by the regulations.

Request to associate a statement

13.4. If:

- (a) the APP entity refuses to correct the personal information as requested by the individual; and
- (b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5. If a request is made under subclause 13.1 or 13.4, the APP entity:

- (a) must respond to the request:
 - i. if the entity is an agency—within 30 days after the request is made; or
 - ii. if the entity is an organisation—within a reasonable period after the request is made; and
- (b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).