COMPANY POLICY

PRIVACY & CONFIDENTIALITY

Pelin Bright, CEO
pelin@macquariecentres.com.au
This policy outlines and provides information on MCOE’s commitment to privacy and confidentiality within the Practice and thus, MCOE recognises that it has an obligation to protect the privacy of the information it collects, receives, processes and retains for its patients, staff and suppliers.

MCOE shall adhere to the requirements of legislative bodies and guidelines, including any/all amendments to the Privacy Act 1988 and the Australian Privacy Principles included in the Privacy Act (Attachment-4). MCOE recognises the importance of maintaining employee, patient and client confidentiality and is committed to protecting the privacy of all persons interacting with the Practice.

MCOE shall comply with the 13 Australian Privacy Principles (APP) in its dealings with personal information relevant to all activities conducted by the Practice. The following schedule sets out an overview of the five parts of the APP:

1. **Consideration of Personal Information Privacy**
   - AAP 1 - Open and transparent management of personal information.
   - AAP 2 - Anonymity and pseudonymity.

2. **Collection of Personal Information**
   - AAP 3 - Collection of solicited personal information.
   - AAP 4 - Dealing with unsolicited personal information.
   - AAP 5 - Notification of the collection of personal information.

3. **Dealing with Personal Information**
   - AAP 6 - Use or disclosure of personal information.
   - AAP 7 - Direct marketing.
   - AAP 8 - Cross-border disclosure of personal information.
   - AAP 9 - Adoption, use or disclosure of government related identifiers.

4. **Integrity of Personal Information**
   - AAP 10 - Quality of personal information.
   - AAP 11 - Security of personal information.
5. **Access to, and Correction of, Personal Information**

- AAP 12 - Access to personal information.
- AAP 13 - Correction of personal information.

In addition to the legislative requirements of the Privacy Act, human resources management shall keep confidential information and personal information in locked in cabinets and all documents on computers shall include a password or passcode.

**Requirements**

All staff (including volunteers) that enters into employment or voluntary engagement with MCOE (long or short term) must sign and comply with the organisation's Confidentiality Agreements (Attachment-1-2-3).

All staff and volunteers who enter into employment or voluntary engagement with MCOE must read the organisation's Code of Conduct Policy and make sure that it is adhered to at all times.

Any information that an employee or a volunteer learns about MCOE, its staff members, patients and its clients as a result of working for/with the Practice, and which is not otherwise publicly available, constitutes confidential information.

Employees or volunteers may not disclose confidential information to anyone who is not employed by MCOE who do not need to know such information to assist in rendering services.

The disclosure, distribution, electronic transmission or copying of MCOE confidential information/records and forms is strictly prohibited. Any employee, patient or volunteer who discloses confidential information will be subject to disciplinary action, even if he or she does not actually benefit from the disclosure of such information.

Discussions involving sensitive information should always be held in confidential settings to safeguard the confidentiality of the information. Conversations regarding confidential information generally should not be conducted on cellular phones, or in elevators, rest-rooms, restaurants, or other places where conversations might be overheard.

MCOE shall take steps as are reasonable in the circumstances to implement practices and procedures, relating to MCOE's functions and activities that:

- Will ensure that the Practice complies with the APP
- Will enable the Practice to deal with inquiries or complaints from individuals about the organisation's compliance with the APP.
1. Consideration of Personal Information Privacy

Management of Personal Information

- MCOE will collect and hold personal information with regards to the:
  - Company (such as; Company and Not-for-Profit Organisation registration, charity, taxation and superannuation and banking details)
  - Personal information which is completed by the employee, volunteer, patient, client, and/or the client’s authorised representative. Any required information unavailable at the time of completing the form may be collected via an alternative written medium submitted by the individual.

- Personal information is mainly held in a computer database, which is accessible by applying a password granted to only authorised individuals. Personal information is also held in a locked steel filing cabinet, and the keys opening that cabinet are held by the Practice Manager, the CEO or Manager(s) who are all authorised to access those files.

- MCOE will collect, hold, use, and disclose the kind of personal information required for the purpose of enabling the Practice to carry out its stated mission and to conduct interactions with or on behalf of its employees, volunteers, patients and clients effectively and efficiently in accordance with written statements/forms signed by individual employees, volunteers, patients or clients.

- An individual may access their own personal information and may seek the correction of such information by contacting the Practice Manager and/or the CEO requesting access to the personal information held about that individual, and by providing corrected information in writing whenever this is appropriate.

- An individual may not obtain or copy any documentation from their files without the permission of the Practice Manager and/or the CEO.

- An individual may complain about a breach of the APP verbally or in writing to the Practice Manager and/or CEO. If the Practice Manager or Supervisor is unable to resolve the complaint, it will be referred to the Chief Executive Officer (CEO). If the CEO is unable to resolve the complaint, it will be referred to the Director.

- MCOE will not disclose personal information to overseas or interstate recipients.

- The Practice’s Confidentiality and Privacy Policy is available free of charge to all individuals who may currently be, or who may consider entering into interactions with the Practice and thus become, affected by the organisation’s compliance with the APP. Details of the Practice’s open and transparent management of personal information are also made available on Company's website(s).

- If a person or body requests a copy of MCOE’s policy on management of personal information, MCOE will take such steps as are reasonable and practicable in the circumstances to give the person(s) or body a copy in that requested form.
Anonymity and Pseudonymity

- Individuals will have the option of not identifying themselves, or of using a pseudonym, when dealing with the Practice in relation to a particular matter, unless:
  a) The Practice is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves in relation to that matter; or
  b) It is impracticable for the Practice to deal with individuals who have not identified themselves or who have used a pseudonym in relation to that matter.

2. Collection of Personal Information

- MCOE will only collect solicited personal information which is necessary for, or related to, one or more of the organisation’s functions or activities.
- If any personal information collected is of a sensitive nature, the individual has consented to the collection of the information; and/or the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or a permitted general situation applies to the collection of the information by MCOE or the information relates solely to individuals who have regular contact with MCOE in connection with the organisation’s activities.
- If the Practice receives unsolicited personal information about an individual and determines that the Practice could not have collected the personal information under Australian Privacy Principle 3 and that the information is not contained in a Commonwealth record, MCOE will destroy the information, provided it is lawful and reasonable to do so.
- If MCOE receives unsolicited personal information about an individual which the organisation could have collected under Australian Privacy Principle 3, the Practice will:
  a) Take such steps as are reasonable in the circumstances to ensure that the individual is aware of the fact that the organisation has collected the information and the circumstances of that collection;
  b) Notify the individual of all matters relevant to the purpose for which the Practice collects the personal information received.

3. Dealing with Personal Information

Use and/or Disclosure

- MCOE does not use or disclose personal information held about an individual for any purpose other than the primary purpose for which the information was collected, unless:
  a) The individual has consented to the use or disclosure of the personal information for a secondary purpose; or
  b) The individual would reasonably expect the Practice to use or disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose. In the case of sensitive information, the secondary purpose would be directly related to the primary purpose; or
c) The use of disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
d) One or more of the below relevant permitted general situations exist:
   - Lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety
   - Taking appropriate action in relation to suspected unlawful activity or serious misconduct
   - Locating a person reported as missing
   - Asserting a legal or equitable claim
   - Conducting an alternative dispute resolution process
   - The existence of any of those 5 (five) situations would cause the use or disclosure of the information
e) MCOE 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. The Practice will make a written note of the use or disclosure under such circumstance(s).

**Direct Marketing**

- MCOE may use or disclose personal information (other than sensitive information) held about an individual for the purpose of direct marketing, if:
  a) The Practice collected the information from the individual; and
  b) The individual would reasonably expect the Practice to use or disclose the information for that purpose; and
  c) The Practice 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 Practice.
- MCOE may use or disclose personal information (other than sensitive information) held about an individual for the purpose of direct marketing, if:
  a) The Practice collected the information from the individual, who may not reasonably expect the Practice to use or disclose the information for that purpose, or from someone other than the individual; and
  b) The individual has consented to the use or disclosure of the information for that purpose, or it is impracticable to obtain that consent; and
  c) The Practice 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, the Practice 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 Practice.
- MCOE will not use or disclose sensitive information about an individual for the purpose of facilitating direct marketing by other organisations.
Cross-border Disclosure of Personal Information
MCOE does not disclose personal information about an individual to an overseas recipient; nor does it disclose personal information about an individual to an Australian interstate recipient.

Adoption, Use or Disclosure of Government Related Identifiers

- MCOE does not adopt a government related identifier of an individual as its own identifier of the individual.
- MCOE will 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 fulfil its obligations to a government agency like Centrelink; or
  b) The use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or
  c) The Practice 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.

4. Integrity of Personal Information

- MCOE will take any reasonable steps to ensure that the personal information collected by the organisation is accurate, up-to-date and complete, and that the information being used or disclosed by the Practice is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.
- The Practice will take any reasonable steps to ensure that the personal information held is:
  a) Protected from misuse, interference and loss; and
  b) Protected from unauthorised access, modification or disclosure.
- The Practice will take any reasonable steps to destroy the personal information held or to ensure that the information is de-identified, if:
  a) MCOE no longer needs the information for any purpose for which the information may be used or disclosed by the Practice under this policy; and
  b) The Practice is not required by or under an Australian law, or a court/tribunal order, to retain the information.

5. Access to, and Correction of, Personal Information

Access to Personal Information

- MCOE will, on request by the individual, give the individual access to their personal information, unless:
  a) The Practice 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 deemed to be frivolous or vexatious; or
d) The information relates to existing or anticipated legal proceedings between the Practice 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) MCOE has reason to suspect that unlawful activity, or a serious breach of the spirit or the stated requirements of the Practice’s Code of Conduct has been, is being or may be engaged in; and 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 Practice in connection with a commercially sensitive decision-making process.

- The Practice will respond to the request for access to the individual’s personal information within a reasonable time after the request is made and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so. The Practice will take any steps as are reasonable in the circumstances to give access in a way that meets the needs of the organisation and the individual.

**Correction of Personal Information**

- If MCOE holds personal information about an individual and 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 the individual requests the Practice to correct the information, the organisation will take any steps that are reasonable in the circumstances to update and correct the information.

- If the Practice corrects personal information about an individual that the organisation previously disclosed to another APP entity, and the individual requests the Practice to notify the other APP entity of the correction, the Practice will take such steps as are reasonable in the circumstances to give that notification, unless it is impracticable or unlawful to do so.

- If the Practice refuses to correct the personal information as requested by the individual, the Practice will give the individual a written notice that sets out:
  a) The reason(s) 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.
Relevant Legislation/Guidelines
Privacy Act 1988 (ComLaw), as amended, which includes the Australian Privacy Principles
- Privacy Regulation 2013 (ComLaw)
- NSW Privacy and Personal Information Protection Act 1998

Authorisation
Pelin Bright, CEO
Macquarie Centres of Excellence
Australian Privacy Principles

January 2014

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

This privacy fact sheet provides the text of the 13 APPs from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988. For the latest versions of these Acts visit the Comlaw website: www.comlaw.gov.au.

Part 1—Consideration of personal information privacy

Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities 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.

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

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) 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; and
      (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:
   (e) 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.

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:
   (c) 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 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 APP entities, 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

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;

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
(c) 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(c),
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.

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—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.

Exception—sensitive 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:

(e) 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

7.8 This principle does not apply to the extent that any of the following apply:

(a) the Do Not Call Register Act 2006;
(b) the Spam Act 2003;
(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

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):

(e) 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 16A, 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:

(e) 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;

(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;

(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.
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.

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

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.

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:
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

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
(iii) 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.

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).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information

   telephone: 1300 363 992
   email: enquiries@oaic.gov.au
   write: GPO Box 5218, Sydney NSW 2001
   GPO Box 2999, Canberra ACT 2601
   or visit our website at www.oaic.gov.au