PRIVACY POLICY

Caringa Enterprises Limited (CEL) has adopted a Layered format for our Privacy Policy

This page contains the CEL Privacy Policy Statement and directs interested parties to further information

Page 2 of this layered format contains The CEL Condensed Privacy Policy which summarises the key points

Pages 3 to 11 contain the CEL Complete Privacy Policy addressing each of the Australian Privacy Principles

Pages 12 to 24 contain the text of the 13 Australian Privacy Principles from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* which amends the *Privacy Act 1988*.

Privacy Policy Statement

Caringa Enterprises Ltd collects, protects and manages your personal information to provide its products and services according to the Privacy Act and the Australian Privacy Principles.

Our Complete Privacy Policy is available online at www.caringa.com.au , by email from privacy@caringa.com.au or by writing to The Privacy Officer, Caringa Enterprises Ltd, PO Box 299 Grafton NSW.

CONDENSED CEL PRIVACY POLICY

Scope

The CEL Privacy Policy applies to the collection, use and management of personal information collected and held by all divisions of Caringa Enterprises Ltd. CEL has adopted a layered policy format, which comprises a Privacy Policy Statement, a Condensed Policy, and our Complete Privacy Policy.

This condensed policy summarises the key points of the CEL Complete Privacy Policy.

You can access the full version below, online at www.caringa.com.au or request a free copy of the policy in a different format by email to privacy@caringa.com.au or by writing to the Privacy Officer, Caringa Enterprises Ltd, PO Box 299 Grafton NSW 2460. We will take all reasonable steps to provide it in the requested format.

Collecting your personal information

CEL only collects personal information for the purposes of carrying out its organisational activities - providing services and supports to people with disability, sales of goods to the public and commercial activities. CEL usually gets information directly from people, or their authorised representative. CEL sometimes gets information from third parties, but only if the individual has given consent to the collection. We may receive information from an individual through their online access.

Using and disclosing your personal information

CEL will only use the personal information it collects for the purposes for which CEL collected it. CEL does not disclose information to government or anyone else without the consent of the individual unless we are - required to do so under law, preventing a threat to someone's life or health, or for the enforcement of the law. We will not send your personal information overseas, sell it to anyone or use it for direct marketing.

Security of your personal information

CEL takes care of your personal information, and protects it against loss, disclosure, alteration or misuse. When we no longer need your personal information, we will delete or destroy it in a way to protect your security.

Accessing and correcting your personal information, and making contact with us

An individual can access the personal information which CEL holds about them, can ask CEL to correct their information if it is not accurate, and can raise a complaint if unhappy about the way CEL manages personal information .

Contact should be in writing –

- by email to privacy@caringa.com.au or
- by mail to the Privacy Officer, Caringa Enterprises Ltd, PO Box 299, Grafton NSW 2460.

We will take all reasonable steps to remedy any issues resulting from our failure to comply with our privacy obligations.

THE CEL COMPLETE PRIVACY POLICY

Caringa Enterprises Ltd (CEL) respects the privacy of all the people we have dealings with – our clients, program participants, employees, supported employees, members, volunteers, customers, donors, contractors and business partners, and web and social media users and visitors. CEL is committed to safeguarding the personal information that is collected, stored and administered.

This Complete Privacy Policy has been developed by CEL in accordance with the obligations conferred under the Privacy Act 1988, and to reflect the additional requirements in place under the 13 Australian Privacy Principles (APPs).

Additional detail, exclusions and exemptions may be located in the Privacy Fact Sheet 17 published by the Office of the Australian Information Commissioner, which is attached to this policy.

This policy is available on request in a variety of formats and print sizes. Contact

The Privacy Officer, Caringa Enterprises Ltd, PO Box 299 Grafton NSW 2460, email your request to privacy@caringa.com.au or visit our website at caringa.com.au

Open and Transparent management of Personal Information (APP1)

A Policy Purpose

The purpose of this policy is to

- Clearly communicate how CEL collects, uses, discloses and stores personal information
- Explain how individuals may access and correct personal information we hold about them
- Enhance the transparency of CEL operations
- Provide individuals with a more clear and complete understanding of the personal information that CEL holds, and the way that we manage that information

B Policy Scope

The scope of this policy

- This policy applies to the collection, use and management of information related to all **'CEL people'** – our members, employees, supported employees, volunteers, clients, program participants, customers, donors, business partners and online users.
- As CEL is a private sector employer entity, the Privacy Act 1988 and this policy do not apply to acts or practices which directly relate to the employee records of CEL.

C CEL Privacy Policy

Definitions of terms

- **CEL people** are collectively all of the people we have dealings with - our members, delegates, employees, clients, program participants, customers, donors, business partners, volunteers and our web and social media users.
- **CEL Services** refers to the full range of services that CEL and its divisions provide in supporting people with a disability, and in its commercial and other dealings with the wider community. These services include, but are not limited to Residential Support services, Day Program services, and commercial manufacturing and service activities through our Australian Disability Enterprises. During the provision of our services we engage employees, volunteers and business partners, and we receive support, funding and donations from the community, agencies, governments, groups and corporations.
- **Donors** is a term used in this policy to refer to an individual or business who provides an occasional or one off contribution to CEL, whether financial or in kind.
- **Clients, program participants and supported employees** refers to individuals living with disability who receive support from CEL on a one off, short, or long term basis.
- **Customers** are those who purchase goods or services from CEL or its divisions.
- **Business Partners** refers to a business or entity that provides support to CEL through the provision of funds, services or time. This term includes our suppliers.
- **Authorised person/s** is used to refer to anyone holding a CEL position which requires them to have access to personal or sensitive information. This will include financial and payroll functions, and people with Human Resource related duties.
- **Personal Information** is defined by the Privacy Act 1988 as being information or an opinion about an identified individual, or one who is reasonably identifiable, whether true or not, and whether recorded in a material form or not. The type of Personal Information held about **CEL people** will vary according to the nature of our dealings and any external obligations imposed upon us.
- **Sensitive Information** is a subset of Personal Information generally afforded a higher level of privacy protection. It is defined by the Privacy Act 1988 as being

information or opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record or health information about an individual; that is also Personal Information.

- **Online and social media users** refers to anyone who accesses the www.caringa.com.au or related websites and social media sites

D Our obligations under the Privacy Act

This policy sets out how we comply with our obligations under the Privacy Act 1988**.** CEL are bound by the provisions of the Australian Privacy Principles (or APPs) in the Privacy Act which regulate how organisations may collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.

E Anonymity and Pseudonymity (APP2)

If you would like to access any CEL services on an anonymous basis or by using a pseudonym, please tell us. If this lawful and possible, we will accommodate your request as much as possible; however we may not be able to provide specific programs or services if you do not provide information requested and required.

F Collection of solicited personal information (APP3)

CEL only collects personal information necessary for the purposes of undertaking its activities, and maintaining records required under relevant legislation.

CEL will only collect sensitive information in cases where we have obtained the consent of the individual or their carer/advocate/parent if applicable, except in cases where we are required to collect the information by law.

CEL will only collect information by lawful and fair means. We only collect information directly from the person involved unless it is unreasonable or impracticable to do so.

The types of personal information collected may include –

- contact details,
- personal details,
- date of birth,
- bank details,
- Centrelink Customer Reference Number (CRN),
- Tax File Numbers,
- purchase history,
- ABN details,

- payment details including credit card number and expiry date,
- health and behavioural details,
- email and server details,
- and any other details considered reasonable for us to conduct CEL activities with you.

For employees, applicants for employment and for volunteers we may also collect

- details of emergency contacts,
- place of birth and residency,
- indigenous status,
- visa details,
- employment history and qualifications,
- language/s spoken,
- driver licence details,
- information and opinions from referees and past employers,
- police check
- working with children check clearance status and verification.
- CEL may collect health information about an individual. CEL will explain why the information is collected, and will explain whether if and to whom it will be released.

G How we collect your information

Where possible, we collect your personal and sensitive information directly from you. We collect information through a variety of means – forms, face to face and phone interviews, emails and online submissions. If you feel that the information which we are requesting, either on forms or in discussion, is not information which you wish to provide, please raise this with us.

There may be circumstances where we will collect information about you from a third party source, for instance a doctor or health care professional. If this happens, we will take reasonable steps to contact you and to explain the purpose for gathering the information, and any organisations to which we will disclose the information subject to any exemptions under the Act.

H Health Information

Generally, as part of providing services to clients, participants and supported employees we will collect health information. In such cases we will obtain your consent, or ask you directly for the information, and we will explain how the information will be used or disclosed. We will not use your health information beyond the consent provided by you unless - we obtain further consent from you, in accordance with exemptions under the Act, or in compliance with another law.

I Dealing with unsolicited personal information (APP4)

CEL may from time to time receive unsolicited personal information. Where this occurs we review the information to determine whether we could have collected the information for the purpose of our core activities. Where this is so, we may hold and use the information in accordance with this policy and its practices. Where we could not have lawfully collected this information we will destroy or de-identify the information (unless it would be unlawful to do so).

J Notification of the collection of personal information (APP5)

Whenever CEL collects personal information about an individual we take reasonable steps to notify the individual before, at the time, or as soon after as practicable, of the collection, or otherwise ensure that the individual is aware of the collection. We will explain

- How when and where we collect the information, and whether there was a third party involved
- If the collection is required or authorised by law, and the name of the law or other legal agreement requiring the collection
- The primary and any secondary purpose for the collection
- Any consequences for the individual if all or some of the information is not collected
- That we do not disclose personal information to any overseas entities
- How to access this Privacy Policy in a variety of ways
- That this Privacy Policy contains information as to how to the individual may access and seek correction of any personal information held by CEL; and also how to complain about any breach of the APPs by CEL, and how CEL will deal with that complaint

K Use or Disclosure of Personal Information (APP6)

CEL only uses personal information for the primary use it was obtained, or for secondary purposes where

- The individual has consented to the secondary disclosure,
- An individual would reasonably expect the secondary use or disclosure and there is a direct relationship to the primary purpose for collection,
- The use or disclosure of the information is required by law.

Where the secondary disclosure was made in an 'enforcement related activity' CEL will make written record of the use or disclosure including the following details

- Date of use or disclosure
- Details of the information used or disclosed
- The enforcement body conducting the enforcement related activity , and

- If the body used the information – any advice we have received as to how it was used, and the basis for our reasonable belief that we were required to disclose the information.

L Direct Marketing (APP7)

CEL does not disclose or use the personal information that it holds about an individual for direct marketing purposes.

M Cross-Border disclosure of personal information (APP8)

CEL is a NSW based organisation providing services to clients, participants and supported employees within a radius of approximately 200km.

Our customers are principally within Australia, how ever our **online users** may be from any location in the world.

Some personal information controlled by Caringa is held in cloud-based formats and stored in data centres in various locations. All Caringa server data is transferred and held in encrypted formats. Due to the protection strategy of global transfer of encrypted back up data, some data may be stored outside of Australia at some times.

We do not disclose any personal information overseas, nor do we solicit any personal information from overseas. **Unsolicited personal information** collected from overseas individuals will be treated in accordance with our stated policy.

N Adoption, use or disclosure of government related identifiers (APP9)

CEL does not adopt, use or disclose a government related identifier related to an individual except

- In situations required by Australian law or other legal requirements
- Where it is reasonably necessary to do so to verify the identity of the individual
- Where it is reasonably necessary to fulfil obligations to an agency or State or Territory authority
- Or as prescribed by the Australian Privacy Principle 9 or regulations.

O Quality of personal information (APP10)

CEL takes reasonable steps to ensure that the personal information it collects is factually correct, accurate, up to date and sufficient for stated requirements.

Similarly, we take reasonable steps to ensure that the information which we use or disclose is accurate, relevant, up to date and sufficient for the purpose.

Some personal information we hold about some **CEL people** is based on opinions. CEL ensures that this information, as far as is possible, is the result of an informed and unbiased assessment based on all available valid and current evidence, and is expressed in an objective way.

CEL has quality measures in place to ensure that these standards are maintained which include

- Systems which ensure documentation and reporting is consistent and from the primary source wherever possible
- Internal practices to monitor, audit, review and correct personal information
- Regular review and updating of relevant personal information at regular or critical service points (ISP and IEP) when we engage with **CEL people.**
- CEL will take reasonable steps where appropriate to contact individuals to verify the accuracy of information held before use or disclosure, particularly if there has been a lengthy time period since collection.

P Security of personal information (APP11)

CEL views the security of all personal and sensitive information as of the highest importance. We protect personal information against loss, misuse, interference, modification, unauthorised access and disclosure through a number of means including

- Password protected access to our IT systems at all points
- Restricting access to your personal information to relevant **Authorised Persons**
- Ensuring that personal information held in hard copy format is kept in secure, lockable storage
- Secure archive storage for personal information which is kept for legal or statutory purposes
- Internal archives and other records disposed of in accordance with archiving requirements through internal confidential document destruction processes

Q Access to personal information (APP12)

If an individual requests access to the personal information we hold about them we will allow access within reasonable timeframes unless we consider there is sound reason under the Australian Privacy Principles, the Privacy Act, Freedom of Information Act, or other relevant law for us to withhold the information. It will take longer to provide Personal Information which is aged or archived, or in a format differing to that in which we hold it.

Upon receiving a request to access Personal Information we:

- Ensure through confirmation of identity that the request is made by the individual concerned, or by a person who is authorised to make a request on their behalf
- Act promptly, usually within 10 working days, to inform the individual in writing when notifying our intent to withhold access, including the reasons for refusal in writing, and the complaint mechanisms available to the individual; or
- Provide access to the information requested, in the format it is requested if possible, within 10 working days of the request being received; or in situations where the request is complicated or involves large volumes of material we will take all reasonable steps to provide access to the information requested in the format it was requested (if possible) within 20 working days of the request being received.
- We do not charge an individual for access to the Personal Information we hold about them, however we may charge for large volumes of photocopying, conversion to a different format, for printing, or for delivery or retrieval of the information if stored off site.

R Correction of Personal Information (APP13)

CEL acknowledges the requirement that the Personal Information we hold be accurate, current, and relevant. CEL has measures in place to review the relevant Personal Information which we hold, and offer regular opportunity for our clients, participants and employees through our planning and review models. All **CEL people** are able to provide us with information, and request that we update or correct the information which we hold about them.

CEL may determine that the Personal Information held for a particular purpose is no longer accurate or up to date, in which case we will make all reasonable efforts to correct that situation.

If CEL receive a request from an individual to correct Personal Information and we are satisfied that the request is in accordance with this APP, we will take reasonable steps to correct the information we hold. If CEL have provided the inaccurate information to a third party, and if requested to do so by the individual, we will take reasonable steps to notify the third party of the correction unless this would be impracticable or unlawful.

If CEL refuses to correct the Personal Information as requested by the individual, we will take reasonable steps to provide in writing

- the reasons for our decision;
- advice to the individual of any complaint mechanisms available to them; and
- any other relevant matter prescribed in the regulations

If CEL refuses to correct the Personal Information as requested by the individual, and the individual requests that we associate with the information a statement that the information is out of date, inaccurate, incomplete, irrelevant or misleading we will take reasonable steps to associate the statement in a way that will make it apparent to users of the information.

If CEL corrects your Personal Information in response to a request, or associates a statement as described, we will not charge the individual for this.

Requests for access or correction should be mailed to The Privacy Officer, Caringa Enterprises Ltd, PO Box 299 Grafton NSW 2460 or email to privacy@caringa.com.au

S Contacting us to make a complaint about privacy matters

If an individual has provided CEL with Personal or Sensitive Information, the person has a right to make a complaint about the use, storage or protection of their information, and to have the complaint investigated and dealt with in a fair way.

Any privacy complaint should be in writing and include the date, time and circumstances if the matter that the complaint is about, how you believe that your privacy has been interfered with, and how you would like the matter resolved.

Privacy complaints directed to the Privacy Officer will be initially investigated in consultation with the Manager of the relevant CEL division, and escalated to the CEO or Vice President of the Board of CEL if required. CEL will respond to the complaint after initial investigations in writing and will

- outline whether in the view of CEL there has been a breach of this Policy, or any applicable legislation
- detail any action, if any, CEL will take to rectify the situation
- provide contact details for the Office of the Australian Information Commissioner, who may investigate the actions of CEL in this matter.

Complaints can be mailed to

The Privacy Officer, Caringa Enterprises Ltd, PO Box 299 Grafton NSW 2460
or emailed to privacy@caringa.com.au

Privacy fact sheet 17
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;

(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.

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.

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; 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.

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

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):

(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.

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:

(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

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.

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**