Adopted: 1 June 2015
Distributed: 1 June 2015
Review by: 1 June 2017

CATHOLIC DIOCESE OF TOWNSVILLE

PRIVACY POLICY

1.0 INTRODUCTION

The Roman Catholic Trust Corporation (RCTC) as trustee for the Diocese of Townsville (the Diocese or Diocesan entities) as part of the Catholic Church conducts a range of activities in order to fulfil the mission and ministry associated with proclaiming the good news of Jesus Christ. In conducting those activities, the Diocese, including its parishes, schools and various agencies, may, from time to time, collect personal information. The information is collected to enable these entities to minister to the faithful, provide needed services and to fulfil its canonical and civil law obligations under the Code of Canon Law and under the Civil Law (both Commonwealth and State).

This policy describes ways in which personal information is managed including how it is gathered, stored and/or disseminated.

2.0 AUSTRALIAN PRIVACY PRINCIPLES

The Diocese is bound by the 2012 amendments to the Privacy Act 1988 (Cth), which include the Australian Privacy Principles (APPs). It respects the rights of individuals to keep their personal information private and to ensure that it is accurate.

These principles underpin the Diocesan Privacy Policy. They can be found at: Attachment “A”.

3.0 APPLICATION

This policy applies to parishes, diocesan offices and agencies. Some larger agencies (e.g.Catholic Education, Centacare) will have their own privacy policy that meets their particular requirements and is in accord with the terms and intent of this policy.

This policy applies to all diocesan entities which include the ministry and financial operations conducted from the Office of the Bishop, and any operations or processes conducted by a parish within the diocese.

This policy and the provisions of the Act do not apply to records or information held or collected on behalf of or relating to existing or former employees of the Diocese, Priests or Religious. This policy does not apply to personal information collected prior to 21 December 2001.

This policy applies where personal information is to be collected and/or used by the Catholic Diocese of Townsville.

'Personal information' means information or an opinion, whether true or not, and whether or not recorded in material form, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

In addition to personal information, the Act also regulates the collection of sensitive information, including personal information about racial or ethnic origin, religion, criminal record, sexuality and union activities. Sensitive information is also health information about an individual.

3.1 PURPOSE ASSOCIATED WITH THE COLLECTION OF PERSONAL INFORMATION

The Diocese, parishes and agencies, may from time to time, collect personal information for many purposes, including:

- to minister to the faithful and to provide pastoral care
- to provide administrative support to other RCTC or Catholic Diocese of Townsville agencies
- to enable education, welfare or government funded community services to be provided to an individual, family or community
- for fundraising activities
- to assess the employment applications of prospective employees
- for other purposes that may arise from time to time.

You will be informed of the reason that your personal information is being collected at the time of collection.

3.2 COLLECTION OF PERSONAL INFORMATION

From time to time, personal information may be collected in various ways, including:

- forms filled out and/or documentation presented to a Catholic parish, school, welfare or other agency, either by the individual or their guardian/responsible person
- face-to-face meetings
- interviews
- telephone conversations
- other methods that may arise from time to time.

The Diocese, parishes and agencies will endeavour to collect your personal information directly from you. Where this is not possible, your consent will be sought prior to collecting your personal information from a third party. If your consent cannot be obtained, due regard will be given to the requirements and exemptions of the Act before making such a collection. If your personal information is collected from a third party without your consent then the Diocese will notify you of such collection and the circumstances of such collection.

In the case of children, personal information will ordinarily be collected from their parents or guardians, unless specific and/or unusual circumstances require that the collection be made directly from the relevant child.

For prospective employees, personal information may be collected by speaking with referees. This may include applicants' previous employers who have not been nominated as referees. Should this be the case, applicants will be advised prior to such contact being made.

3.3 INFORMATION HELD

Personal or sensitive information held about you may include the following:

- personal contact details
- Sacramental records
- information relating to your application for employment
- any health information required by law
- information relevant to the provision of a particular counselling or other community service
- any personal information about you that will enable the diocese, parishes or agencies to satisfy their duty of care to other individuals with whom you may come into contact in the course of your involvement with them
- information relating to pastoral care needs
- information relating to a child's enrolment at a Catholic school, Mary MacKillop child care centres or outside school care centres or kindergartens
- any other information about you that may be relevant to the contact that you have with the diocese, a parish or one of its agencies.

3.4 HOW YOUR PERSONAL INFORMATION IS USED AND DISCLOSED

Your personal information will be used for the purpose for which it was collected or for a related secondary purpose. If the personal information is also sensitive information then it will be used for the purpose for which it was collected or a directly related secondary purpose. Your personal information also may be used for another purpose where:

- your consent has been given
- it would reasonably be expected to occur
- there is a legal requirement to do so.

Your personal information will generally be used to attend to any pastoral care, ministry, educational or welfare needs that you may have.

If you are a prospective employee, your personal information will be used to assess your suitability for the position for which you have applied. Your personal information also may be used to assess your suitability for a position for which you have not applied, but to which you may be suited. Should this be the case, your consent will be sought before considering you for such a position. Other related secondary purposes are:

- to minister to the faithful and to provide pastoral care
- to fulfil educational needs and expectations in Catholic schools, Mary MacKillop child care centres or outside of school care or kindergartens
- to provide community or welfare services and/or support
- for fundraising activities
- to assess the employment applications of prospective employees
- for other purposes that may arise from time to time.

The Diocese may distribute aggregated statistical information to Government authorities, the Vatican and other Catholic Church agencies for reporting purposes. In most cases, this information will not contain any features that will identify individuals.

The Diocese of Townsville was established in 1930. It covers an area of 434,400 square kilometres, extending from Townsville on the Coast, to the Whitsunday and Burdekin regions in the South and

North to Ingham and Halifax, south-west to Winton, and west to the border with the Northern Territory, encompassing Mount Isa and all western towns and communities in between and east to Palm Island. In addressing the needs of these various communities, personal information, from time to time, may need to be shared amongst the diocese's parishes, schools and various agencies.

In some limited circumstances, external contractors and/or consultants may have access to your personal information. In most cases, confidentiality agreements are in place with these contractors or consultants so that personal information which they may come into contact with in the course of their work is protected.

A government related identifier of an individual will not be used by the Diocese or its schools, parishes or agencies as its own identifier nor will the Diocese or its schools, parishes or agencies use or disclose a government related identifier of an individual.

Your personal information will not be used for direct marketing purposes by an external entity without your prior consent.

Your personal information will not be disclosed to overseas recipients without your prior consent. Before disclosing your personal information to an overseas recipient, all reasonable steps will be taken to ensure that the recipient will not breach the Australian Privacy Principles (APPs).

3.5 STORAGE OF INFORMATION

Reasonable steps will be taken to protect and secure personal information from unauthorised access, loss, misuse, disclosure or alteration. These steps include restricted access to offices and other areas where personal information is stored, and in computer files that can be accessed only by authorised individuals using login names and secret passwords. All schools and agencies of the diocese are required to do the same.

Personal information will be stored as long as it is deemed necessary.

Any unsolicited personal information that is received from you will be assessed to determine whether it is necessary to retain any of this information to provide you with any services that you have requested.

If your unsolicited personal information is not necessary, then it will be destroyed or de-identified according to accepted practices.

3.6 ACCESSING YOUR INFORMATION

You may request access to personal information that is held about you. Access to your personal information must be provided to you, except in specific circumstances as identified by the Act and the Privacy Principles. The diocese and its parishes, schools and various agencies are entitled to impose a reasonable charge on you for providing you with the personal information, particularly where photocopying is necessary.

To access your personal information, you must make a written request to the relevant persons or position holder in charge of a diocesan parish, school or agency.

3.7 ACCURACY OF INFORMATION

The diocese will take all reasonable steps to ensure the accuracy of your personal

information. This being the case, you are required to assist the diocese in any request it makes of you to ensure that your personal information is kept up to date. In addition, if there has been a change or modification in your personal information we require that you make a written request to the Parish Priest or the School Principal or Senior Officer of the relevant agency to update your personal information. This written request should set out the changes that you wish to be made. You may at the same time request that the amended information be forwarded to other related organisations which you specify in your request.

3.8 CONSEQUENCES OF NOT PROVIDING PERSONAL INFORMATION

Subject to certain exceptions, your personal or sensitive information cannot be collected without your consent. If you withhold your consent, please note that you may limit our ability to:

- attend to your welfare needs
- attend to your child's educational needs
- attend to any pastoral care or other ministry needs that you may have
- offer you employment
- address any inquiries, difficulties or concerns that you may have.

4.0 QUESTIONS AND COMPLAINTS

If you have any queries about this policy or wish to make a complaint about the manner in which your personal information has been handled, please contact:

Executive Officer Professional Standards
Catholic Diocese of Townsville
PO Box 6139
TOWNSVILLE QLD 4810

Email: diocese@tsv.catholic.org.au

If the complaint is not resolved to your satisfaction, you may then wish to make a complaint to the Office of the Australian Information Commissioner (OAIC), who is responsible for the enforcement of the Act. Information of how to make a complaint is available on line from the OAIC at www.oaic.gov.au

The Office of the Australian Information Commissioner's contact details are:

Office of the Australian Information Commissioner (OAIC)

GPO Box 5218
SYDNEY NSW 2001
Telephone: 1300 363 992
Facsimile: (02) 9284 9666
Email: enquiries@oaic.gov.au

5.0 AUTHORITY

These guidelines are authorised by the Bishop, for and on behalf of the Roman Catholic Trust Corporation of the Diocese of Townsville. This authority remains consistent with the relevant currency of the document.

Attachment A

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 sub clause 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**