5.4 AUSTRALIAN PRIVACY PRINCIPLES DIOCESAN POLICY AND PROCEDURES

1. The Policy

The Diocese of Newcastle ("**Diocese**") acknowledges and respects the privacy of all individuals and is committed to complying with the *Privacy Act 1988*, and the *Privacy (Enhancing Privacy Protection) Act 2012* together with the *Australian Privacy Principles* ("**APPs**") which sets out a number of principles concerning the strict protection of all personal information held by all entities, agencies, organisations and individuals throughout Australia. The Diocese, in adopting this Policy, acknowledges the respect and value of all people and the trust in which the individual provides such personal information to it.

All personal information held by the Diocese, Parishes and Chaplaincies that is within the meaning of "personal information" under the Privacy Act, will be treated in accordance with the APPs .

To the extent that the Diocese holds health information it is also committed to complying with the NSW Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002* in addition to the APPs.

2. Purpose of the Policy – To protect the privacy of all personal data held by the Diocese, parishes and chaplaincies.

3. Definitions within this Policy conform with those in the Privacy Act 1988

"Personal information" - means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

"Sensitive information" – includes information **or opinion** about such things as an individual's **racial or ethnic origin, political opinions**, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, **criminal record** or health information.

"Employee Record" – means a record of personal information relating to the employment of an employee, including health, engagement and resignation, training, conditions of employment, performance, salary or wages, membership of trade unions, sick and other leave, etc.

"***Health Information***" - generally speaking, is a special subset of personal information about an individual's health or a disability, including information about an individual's wishes regarding the provision of health services, genetic or biometric information, wishes regarding

organ donation or any personal information collected in the course of providing a health service.

4. Scope – This policy applies to the Diocese, all agencies of the Diocese, Parishes and Chaplaincies within the Diocese who do not have their own Privacy Policy. Unless the context clearly requires otherwise, a reference to the 'Diocese' in this policy includes an agency, Parish or Chaplaincy of the Diocese covered by this policy. The Diocese may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the Diocese's operations and practices and to make sure it remains appropriate to the changing church environment.

5. Australian Privacy Principles

The APPs replace the previous National Privacy Principles and Information Privacy Principles, and apply to most organisations (except small businesses) and government agencies both in Australia and on Norfolk Island. The full text of the APPs can be found at Appendix A. In summary the APPs set out the minimum requirements for dealing with Personal Information. Broadly speaking, they cover:

- Consideration of Personal Information Privacy – the open and transparent management of personal information
- Collection of Personal Information
- Dealing with Personal Information – its use or disclosure
- Use in direct marketing
- Sharing of information with overseas entities
- Use or disclosure of government-related identification codes
- Integrity and trust about personal information
- Access to, and correction of personal information
- Making a complaint about use of private information

Exception in relation to employee records: Under the Privacy Act and NSW *Health Records and Information Privacy Act 2002*, the APPs and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the Diocese's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the Diocese and employee.

6. Collection of Personal Information

The Diocese must not collect personal information unless it is reasonably necessary for one or more of their activities and functions.

6.1 The Types of Personal Information Collected

Personal information held by the Diocese is collected for the administrative, pastoral and missonal purposes of church ministries and may include (but is not limited to) personal information, including sensitve information, such as:

- the name and date of birth
- current and previous address
- telephone, fax and mobile phone numbers
- email addresses
- spouse's name
- date of baptism, confirmation, ordination or consecration
- incident/emergency information
- employment information including qualifications
- WH&S information
- police and working with children checks
- state of health of an individual

This personal information may be collected about a number of persons who come into contact with the Diocese, including but not limited to:

- clerics licensed by the Bishop,
- laity licensed to minister in a parish or ministry region,
- laity appointed or elected to Diocesan boards and committees,
- laity elected to positions of authority in parishes or ministry regions,
- laity involved with CEY Ministries and
- job applicants, staff members, volunteers and contractors.

6.2 Sensitive Information

The Diocese may from time to time collect sensitive information including information which is collected concerning working with children, police checks, and any information relating to misconduct is extremely sensitive.

In the case of sensitive information, the Diocese, which is a non-profit organisation under the APPs, will only collect sensitive information:

- that is reasonably necessary for one or more of its functions and the individual to whom the information relates consents to the collection; OR
- the information relates to the activities of the Anglican Church of Australia in the Diocese of Newcastle and relates solely to Church members or people who have regular contact with the Diocese in connection with its activities; OR
- a permitted general situation exists in relation to the collection of that information such as

- the Diocese has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Diocesan functions or activities has been, is being or may be engaged in; and the Diocese reasonably believes that the collection, use or disclosure is necessary in order for the Diocese to take appropriate action in relation to the matter;
- The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process;
- it is unreasonable or impracticable to obtain an individual's consent to the collection, use or disclosure; and the Diocese reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

The Diocese, will always collect the information directly from the individual to whom the information relates unless it is unreasonable or impracticable to do so.

The provision of personal information by a person to the Diocese is voluntary. However, in some cases, if the person concerned chooses not to provide personal information it may limit their involvement with the Diocese – for instance, the Diocese may not be able to provide that person with necessary documents for ministry or be able to contact them when necessary. An individual is able to opt out of receiving non essential communications from the Diocesan Office at any time. To change their Communications Indicator, they should contact Parish Services.

6.3 How Personal Information is collected

The Diocese collects personal information in a number of ways, for example:

- directly on forms requested by the Diocesan Office, such as the Parish Annual Returns
- directly on forms which the person/s will be asked to complete,
- over the telephone directly with the person,
- upon advice from you but passed on via third parties such as the Parish Incumbent or a Parish Council Secretary,
- from publicly available sources of information (White Pages)
- verbally from the individual in formal interveiws in the context of pastoral care;
- images and recordings of individuals at church activities and events.

The Diocese may also generate personal information from other data which they hold – such as the compilation of rolls, i.e. for Diocesan Synod, for NSTM.

The Diocese will take such steps as are reasonable in the circumstances to notify an individual when it is collecting their personal information and about their rights in respect of that personal information. Collection notices meeting the requirements of the APPs will be used as far as reasonably practicable.

7. The use of Personal Information

As mentioned above, the Diocese will only collect personal information if it is reasonably necessary for one or more of its activities and functions. The Diocese will only use such personal information for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which an individual has have consented. Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless an individual agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

The primary purposes for which the Diocese collects and uses personal information include:

- contacting the person by mail, telephone, email, as and when necessary;
- emergency contact numbers;
- drawing up licences (lay and ordained);
- processing and retention of safe ministry and compliance records;
- drawing up Orders, Collations and other official Diocesan documents;
- marking anniversaries;
- for inclusion in the Diocesan Yearbook, the Australian Anglican Directory, the Diocesan Handbook,and other publications such as the Synod Business Paper, on its website, in the Diocesan Encounter;
- incident reports and making insurance claims;
- maintaining Work Health Safety records;
- in the Bishop's Ad Clerum;
- Working with Children Check forms;
- contract management;
- archival records management in accordance with Section 7 of the Diocesan Handbook;
- to keep parishioners informed about matters related to the Diocese, Parish or Chaplaincy through correspondence, newsletters and magazines;
- to satisfy the Diocese's legal obligations and allow it to discharge its duty of care;
- obtaining personal information about volunteers who assist the Diocese or Parish in its functions or conduct or associated activities, to enable the Disocese, Parish or Chaplaincy to work together;
- use in publications, including newsletter and on Diocese website.

The secondary purposes include:

- keeping archival records of parish members via its electronic data management system.

In addition to the above, the Parishes also collect personal information for the following primary purposes;

- inclusion or amendment of details in the Parish Electoral Roll,
- requests for public prayer,
- Parish Registers, i.e. Marriage, Funeral, Baptism, Confirmation
- Delegation Registers, i.e. Marriage of Divorced persons, Marriage outside a Church, Chalice Assistants,

- Cemeteries, Memorial Gardens and Columbarium Registers
- Parish Facilities Hire
- Use in church rosters
- Involvemnt in and provision of Parish community programs

Public Prayers - Information included in public prayers is personal and consideration for the rights of the individual involved must be respected. As far as reasonably practicable the consent of the person to be prayed for must be sought before making it public. If the Parish is unable to obtain the individual's consent, it will only make the prayer request public if it is able to do so in a manner that protects the identity of the person. The Diocese recommends that only the first name of the person for whom the prayer is to be offered should be used.

Sharing information between the Diocese, its agencies, Parishes and Chaplaincies
Ordinarily there will be a flow of information between the Diocese, its agencies, Parishes or Chaplaincies. In the course of being used for the purposes for which it is collected, personal information collected by one of these entities may be shared with another of these entities. This will ordinarily only occur to the extent necessary for the personal information to be used for the above purposes – and will be subject to any specific direction otherwise from the individual to whom the personal information relates. By providing your personal information to the Diocese, agency, a Parish or Chaplaincy, an individual is giving consent to it being shared in this manner.

8. Disclosure of Personal Information to third parties

The Diocese does not reveal personal information to other organisations other than

- through the Diocesan Year Book which sets out:
  - contact details of clergy, their dates of ordination and when they entered the Diocese,
  - the name of those lay and ordained persons appointed or elected to Diocesan committees and boards,
  - the name and contact details of people in positions of responsibility within Diocesan groups, parishes and associations.
- through the Australian Anglican Directory;
- through distribution within the Diocese of updated contact details of clergy linked to parishes and others licensed by the Bishop.
- to other people within the Diocesan structures who may need to make contact.
- anyone an individual authorizes the Diocese to disclose information to;
- anyone to whom the Diocese are required or authorised to disclose the information by law;
- law enforcement agencies such as the police; and
- other businesses or service providers engaged to provide services to the Diocese, agency, Parish or chaplaincy in connection with the church functions and activities.

The Diocese will only disclose personal information, including sensitive information, in the Diocesean Year Book and Australian Anglican Directory to the extent that it is reasonably necessary to do so or the person affected has specifically consented to that disclosure.

The information contained in the Diocesan Year Book and the Australian Anglican Directory are updated annually, with details of clergy and laity no longer holding a position on a Diocesan committee/board or within a Parish are removed.

The Diocese does not expect to be sharing information with overseas recipients except in limited circumstances or where one of the above publications are shared with overseas partners.

In the limited circumstances that the Diocese may need to dislcose personal information overseas, it will not do so without either:

- taking reasonable steps, in the circumstances, to ensure that the overseas recipient does not breach the APPs;
- reasonably believing that the overseas recipient is subject to a law or binding scheme which provides substantially similar protection for personal information as the APPs;
- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the APPs or other applicable privacy legislation.

However, by consenting to an individual's personal information being published in the above mentioned publications, they also consent to that information potentially being disclosed to our overseas partners without the Diocese taking reasonable steps to ensure the receipient complies with the APPs.

9. Storage of Personal Information

Personal information collected by the Diocese will be held in either the Bishop's Registry (Diocesan Office) or at the Diocesan Archival site at the Newcastle University.
In some cases original documents which contain sensitive information (as defined by the Privacy Act) will be destroyed confidentially and only personal information will be stored electronically. **[See Section 7 of Diocesan Handbook for Diocesan Archival Procedures and the process to access records in Archive at the University of Newcastle.]**

The Diocesan Office maintains personal information in a secure manner via:

- an electronically secured network
- system security with access log-ons password protected at several levels;
- building access security, with 24 hour "back to base" monitoring;
- staff reminders and training in the need to maintain confidentiality, and are required to enter into a confidentiality agreement with the Diocese;
- paper records are maintained in secured areas;

- records destruction occurs via secured destruction methods.

Each Parish has in place steps to protect the personal information the Parish holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. Generally access is restricted to the extent necessary to complete a legitimate function.

Ideally a Parish should ensure that the personal information is maintained on

- an electronically secured network with access log-on password protected (if the Parish has the required facilities)
- paper records are filed in a lockable safe, filing cabinet, or other container;
- those with access are reminded of the need for confidentiality and care of the information
- records no longer required are destroyed securely, or
- relocated to the Diocesan Archival site in accordance with section 7.2 of the Diocesan Handbook.

Personal information may also be held by relevant clergy and laity to the extent necessary for them to properly fulfil their ministerial roles. The Diocese provides training and support to its ministerial personnel to ensure they maintain the security of personal information whilst in their possession.

Document retention policy

In accordance with APP 11.2, the Diocese will take such steps as are reasonable in the circumstances to destroy or de-identify any personal information it holds that is no longer needed for any purpose for which the information may be used or disclosed – unless the personal information is:

a) in a document that is otherwise covered by the Records Management Section 7 of the Diocesan Handbook; or
b) is subject to the limited exceptions from destruction or de-identification in APP 11.2.

10. Accuracy of Personal Information

The Diocese takes all reasonable steps to ensure that the personal information collected, used or disclosed, is accurate, complete and up-to-date. However, the accuracy of that information depends to a large extent on the information provided to the Diocese by those whose information it holds and uses.

For that reason the Diocese requests that it is

- kept informed of changes in personal contact details such as address, telephone numbers, emails,
- kept informed of errors in the information it has on file

- provided with contact information when elected or appointed to an office, board or committee

11. Access by individuals to their own personal information

Under the *Privacy Act* 2012 and *Health Records and Information Privacy Act 2002,* an individual has the right to obtain access to any personal information which the Diocese holds about them and to advise the Diocese of any perceived inaccuracy. There are some exceptions to these rights set out in the applicable legislation, including where:

- access to the personal information (if it is not health information) would pose a serious and imminent threat to the life or health of an individual;
- access would unreasonably impact on another individual's privacy, the request is frivolous or vexatious, or the information relates to current or intended legal proceedings;
- access to the information will adversely prejudice negotiations between the Parish and the individual;
- access to the information would be **unlawful**; or
- access would be likely to prejudice the investigation of possible unlawful activities.

In addition to providing access to the information, the Diocese is also required to take reasonable steps to correct that information if the individual shows that the information is not accurate, complete or up to date.

If a person wishes to do so they should contact the Diocesan Business Manager, in writing. The Diocese reserves the right to charge a fee for searching for and providing access to the information. Such requests will be met within 30 days of receiving the request. Failure to respond within 30 days may be construed as denial of access. APP12.7 says no fee.

If the Diocese denies an individual access to personal information or refuses to update that personal information, it must give reasons **in writing, within 30 days of receiving the request** to the individual for this. Any denial to a request by an individual for access to personal information must be consistent with this policy. Each request must therefore be assessed on its merits.

12. Privacy Checklist

The following checklist will assist in implementing this Privacy Policy within the Diocese, its agencies, parishes, and chaplaincies:

- Personal information should only be collected when it is necessary in order for the Parish to carry out its mission (e.g. Parish Electoral Roll, Baptism, Marriage and Confirmation Registers);
- Personal information collected should be accurate and current;
- Personal information collected should only be disclosed for the purpose for which it is collected, or where the individual consents if there is a different purpose of disclosure;

- Individuals should be allowed access to personal information that concerns them and the opportunity to correct information that is out of date or incorrect, except where access to the information may be withheld;
- Information should be stored safely and reasonable steps should be taken to ensure that the personal information is not the subject of misuse or unauthorised access or disclosure,
- Sensitive information should not be collected without the consent (express or implied) of the affected individual or unless an exemption applies (e.g. employee records). In this context, sensitive information includes health information about parishioners or others collected for the purpose of public prayers;
- Personal information should be securely retained with access only available to authorised persons or those having a legitimate interest;
- Certain practices may have to be reconsidered in the light of privacy laws (e.g.. the collection of sensitive or health information, using personal information for direct mailing, provision of employment references to third parties);
- If any privacy complaint arises, it should be referred immediately to the Diocesan Business Manager; and
- Employee records and stipendiary clergy records are treated differently and may contain additional information related to a person's employment or office.

13. Privacy Officer

The Diocesan Business Manager is the Diocesan Privacy Officer. If any privacy complaint or question arises, it should be referred immediately to the Diocesan Business Manager at:

The Diocesan Business Manager
Diocese of Newcastle
PO Box 817
Newcastle NSW 2300

Any queries**,** questions, or concerns regarding privacy at the parish level may first be addressed to the Parish Services and Administration Manager.

14. Complaints Management

The APPs require all entities to have a procedure for complaints to be made against an entity relating to the handling of personal information. In this regard, this policy provides for a complaint, or concern, or problem which may bencountered with either the Diocese, an agency, a Parish or a Chaplaincy to be directed to the Diocesan Business Manager who is the Diocesan Privacy Officer. The Diocesan Business Manager will investigate the matters raised and make a determination about and action which should be taken.

If dissatisfied with the outcome, or have remaining concerns, an individual may contact the

Information Commissioner via the details at http://www.oaic.gov.au/privacy/privacy-complaints.

15. Links and supporting documents

The current Privacy Policy and the Australian Privacy Principles are available on the Anglican Diocese of Newcastle Website at http://www.newcastleanglican.org.au/page16031/Policies-and-Regulations.aspx.

This Policy should be read in conjunction with the requirements of "Faithfulness in Service" available at http://www.newcastleanglican.org.au/page16031/Policies-and-Regulations.aspx .

16. Frequently asked questions:

Can I access my personal information?
Yes, Section 11 sets out the various ways to access your personal information.

Can I update or correct my personal information?
Yes, Section 11 sets out the various ways of updating / correcting your personal information.

How do I make a complaint about the actions of the Diocese, a parish, or a chaplain?
Section 14 of the Diocesan Policy (above) provides the steps to formally make a complaint.

How will the Diocese/Parish/Chaplaincies use my personal information?
The Diocesan/Parish and Chaplaincy use of personal information is set out in section 7 of this Policy. Section 9 also details the methods of protection of that information.

Will the Parish pass my information onto another organisation or person?
The Parish may share your information with the Diocese or other Parishes or Chaplaincies within the Diocese, as detailed in section 7. It may also disclose your information to persons or organisations outside the Diocese in the limited situations set out in section 8. However, ordinarily the Parish will not disclose your personal information to persons or organisations outside the Diocese. For instance, if someone requests the parish to provide your telephone number or email address, it would refuse to do so, but would perhaps ask for the enquirer's contact details to pass onto you for you to choose to make contact.

Related Diocesan Documents - Diocesan Handbook

Section 2	Clergy Conditions of Service
Section 5.2	Parish Electoral Roll
Section 5.5	Delegated Authority Register
Section 7	Official Records and Archives
Section 8	Employment of Laity and other Staff in Parishes
Section 15	Safe Ministry Policy and Faithfulness in Service

APPENDIX A

Office of the Australian Information Commission
Privacy Fact Sheet 17

AUSTRALIAN PRIVACY PRINCIPLES

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 (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988.* For the latest versions of these Acts please refer to the ComLaw website at 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 *[**"entities"** **are** agencies, organisations such as the Diocese, or small business operators*] manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles

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 privacy policy about the management of personal information by the entity. *[Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.] [Note: The Diocesan Privacy Policy is available on the website under "How can we help" and in the Diocesan Handbook Section 5.4.]*

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 [*i.e. APP complaint means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual*

because it breached an Australian Privacy Principle] 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.

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 Principal 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. Sub clause 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.

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 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 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 section16A of the Act. For *permitted health situation*, see section 16B of the Act.]

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.

Written note of use or disclosure

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. The 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 pupose; 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 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 Acton 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

["identifier of an individual" means a number, letter or symbol, or a combination of any or all of those things – see definitions in the Act.]

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 regulation; 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 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;
    (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;

(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 regards 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:

(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 the website at www.oaic.gov.au