Uniting Church. **Uniting People.**

Privacy Manual

Uniting Church
Synod of South Australia

Reissued April 2014

To be read in conjunction with the relevant Privacy Policy

For further information please contact the Synod Privacy Officer at GPO Box 2145 Adelaide SA 5001.

Phone number: (08) 8236 4206. Fax number: (08) 8236 4201. Email: privacy@sa.uca.org.au

This page is intentionally blank.

Introduction

Purpose of manual

This manual is provided to assist those responsible for any Church situations, where personal information is required to be held, to respond appropriately to managing this information in their care. The manual should only be used once the reader has familiarised themselves with the relevant Church's Privacy Policy. A copy of the Church's policy is available upon request. The policy also contains within its own Appendix, a list of the key definitions and terms that are considered important when seeking to understand the implications of the legislation.

The Church's approach to Privacy

Importantly for the members of Church, the current privacy legislation is to be seen as:

- a shared responsibility between the providers and holders of personal information
- a trustee obligation for the person responsible for holding the information (termed "custodians" in this manual to emphasise the position of trust that they hold)
- an opportunity for the Church to express our pastoral sensitivity to those for whom disclosure of personal information makes them vulnerable to external events and circumstances.

The Church will take all reasonable steps to respect the privacy of personal information and to make all providers of personal information to the Church aware of the Church's policy and practice in relation to personal information management.

Explaining the Church's Privacy Policy Scope

The Church Privacy Policy has a paragraph entitled "Policy Scope". This makes clear that all of the activities and functions of Uniting Church entities will need to comply with the relevant Privacy Policy. This includes:

- all Presbytery and Synod Ministry Centres,
- all activities responsible to an Executive Officer of one of these Ministry Centres,
- any committee or board that come directly under the Property Trust umbrella,
- Mission Networks
- Joint Nominating Committees established by the Pastoral Relations Committee
- Parish Missions, and
- Faith Communities.
- Congregations

Some entities have their own autonomy provided within the UCA regulations such as Congregations or separately incorporated bodies. Notwithstanding the inter-conciliar structure of the Uniting Church, the Presbytery and Synod and individual Congregations are separately defined as an "APP entity" under the amended Act and will need to ensure they are proactive in ensuring that they continually comply with the requirements of the amended legislation. These entities are obliged to define their own policy and are encouraged to use the Uniting Church SA Congregation privacy policy template as a guide. http://sa.uca.org.au/documents/called-to-care/Privacy/Congregation-Privacy-Policy-template-2014.pdf The Synod will provide as much practical assistance as possible to achieve this goal.

Reasons for 2014 revision of the manual

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) came into effect on 12th March 2014. It includes significant changes to the Privacy Act first introduced in 1988. Many readers of this manual will have already had experience in implementing the significant changes to the Privacy Act introduced in late 2001. However care should be taken not to assume the previous conditions still apply. In particular, the number and type of exceptions has changed since the previous version of the Act.

Key aspects of the amended legislation are:

- There is now one set of Privacy Principles to govern both the public and private sectors. What were previously called the 10 National Privacy Principles that applied to the Church are now defined in 13 Australian Privacy Principles or APPs
- The increased importance of having a privacy policy in place that not only defines policy but also contains audit and review mechanisms to ensure ongoing compliance with the APPs and the Church's approved policy.
- The definition of "personal information", a key foundation to the legislation, has been widened
- Although not relevant to Church activities, there are now far more comprehensive credit reporting provisions for credit reporting bodies
- The granting of enhanced powers to the Federal Privacy Commissioner including the power to:
    - conduct investigations and performance assessments of any organisation's personal information handling procedures
    - impose significant financial penalties in the event of non-compliance
- The introduction of provisions which impose obligations on an APP entity where they receive unsolicited personal information
- New and more detailed notification requirements when collecting personal information from individuals
- More stringent cross border disclosure requirements

Accessibility to the Church's privacy policy

Members of Uniting Church governing councils (as defined by the UCA Regulations) and all custodians of personal information within these governing councils are to take all reasonable steps to ensure that:

- Providers of personal information have electronic or hard copy access to the Church's policy on the privacy of personal information and are clear about the concept of consent, primary purpose and opt in-out choices
- A copy of the Church's privacy policy is prominently displayed at any Uniting Church site
- Personal information data collection forms reference the Church's privacy policy.

The Australian Privacy Principles

Introduction

The Australian Privacy Principles are defined in their entirety in Appendix 2 of this manual. If you are a custodian of general information, you are strongly recommended to read the full text of each of the APP's.

Privacy Principles Comparative chart

A chart setting out the names of the newly introduced Australian Privacy Principles and comparing these titles with those of the National Privacy principles that they have replaced is set out below

National Privacy Principles (old - 2001)	**Australian Privacy Principles (new)**
1 – Collection	1 – Open and Transparent Management of Personal Information
2 – Use and Disclosure	2 – Anonymity and Pseudonymity
3 – Data Quality	3 – Collection of Solicited Personal Information
4 – Data Security	4 – Dealing with Unsolicited Personal Information
5 - Openness	5 – Notification of the Collection of Personal Information
6 – Access and Correction	6 – Use or Disclosure of Personal Information
7 – Identifiers	7 – Direct Marketing
8 – Anonymity	8 – Cross-Border Disclosure of Personal Information
9 – Transborder Data Flows	9 – Adoption, Use or Disclosure of Government Related Identifiers
10 – Sensitive Information	10 – Quality of Personal Information
	11 – Security of Personal Information
	12 – Access to Personal Information
	13 – Correction of Personal Information

You will note from this chart that some APPs are similar top previous NPPs but in a different order. Other APPs are subsets of previous NPPs but have been given greater emphasis in the amended legislation by having their own APP status e.g. access to and correction of personal information

In addition:

- there have been changes to the definitions of sensitive and personal information in Section 6 of the Act.
- Section 16 of the Act introduces the concept of a “permitted general situation” and a “permitted health situation” each of which can provide a reason for an exception to the application of the NPP’s. There are 7 general and 5 health situations where the APP’s do not need to be applied.

Abbreviated description of new APP contents

As noted in the next paragraph, translating APPs 2, 4, 7, 8, and 9 and any of the exceptions contained in the APPs into your local context should only be undertaken after receiving specialist advice from the Synod Privacy Officer. However, with this qualification, the table below sets out a summary of the significant differences in content and purpose of each of the APP’s. This table is provided for general information purposes only.

APP No	APP Summary Description
1	APP1 requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. It introduces more prescriptive requirements for organisations’ privacy policies. It also introduces a positive obligation on organisations to ensure that they continually comply with all APPs and any registered APP codes.
2	APP2 sets out a new requirement that an organisation must provide individuals with the option of dealing with it using a pseudonym, in addition to the previous provisions, allowing for anonymity. However, organisations are also given the ability not to comply with this principle in situations where implementing the spirit of APP2 is impracticable for them.
3	APP3 outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or other entity. In particular APP3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual’s consent and only if it’s absolutely necessary for the organisation to retain this information.
4	APP4 is a new principle which applies to the receipt of personal information that is not solicited. This principle requires that the same privacy protection applies to unsolicited personal information as it does to solicited personal information. The main sense of this APP is that an organisation should determine whether it could have collected the information under APP3 and if so it must destroy information collected in this way as soon as possible, if it is lawful and practical to do so.
5	APP5 retains all the notification requirements that were incorporated in the previous NPP1 but, in addition, requires the organisation to either notify an individual or else make sure an individual is aware that its privacy policy contains information about how to access and correct personal information, information about its privacy complaints processes and whether it is likely that someone’s personal information will be sent overseas.
6	APP6 ensures that if an organisation collects personal information for a particular purpose (known as the primary purpose) it must not use or disclose this information for a secondary purpose unless the individual has consented to this secondary use or an exception listed under APP6 applies.
7	APP7 addresses direct marketing as a discrete issue rather than, as previously, an example of a secondary purpose. Basically, this APP requires that organisations can only use or disclose personal information for direct marketing purposes if there is an exception listed as part of APP7.
8	APP8 introduces a new level of accountability on organisations prior to disclosure of personal information in cross-border situations. Prior to information being sent to an overseas recipient, an organisation is now required to ensure that they have assured themselves that

	the overseas recipient will not breach the APPs once they receive the personal information. Once again there are a number of exceptions to this principle.
9	APP9 requires that an organisation must not adopt, use or disclose a government related identifier for an individual in their own systems unless a specific exception applies. Government related identifiers are defined in Section 6 of the Act.
10	APP10 specifically requires an organisation to take reasonable steps to ensure the personal information is accurate, up-to-date and complete in relation to the purpose for which the information is being kept.
11	APP11 requires an organisation to protect personal information that it is holding including from outside interference. It also requires an organisation to destroy or de-identify personal information no longer required. Once again this principle sends a pro-activity message referred to in 1 above.
12	APP12 requires an organisation to provide access to an individual's personal information if they receive a request. There are a number of exceptions to this principle and this list of exceptions has been expanded on the previous NPP6 particularly in relation to 'serious threat' and unlawful activities.
13	APP13 expands on the correction principles contained in the previous NPPs. Previously an individual needed to establish that their personal information was either inaccurate or incomplete. However now an organisation must take reasonable steps to correct personal information to ensure it is accurate, up-to-date, complete and relevant and not misleading in regard to the purpose for which it is held - once again the emphasis being on organisations being proactive with personal information collection, storage, accessibility, accuracy and relevance.

Situations where advice to be sought on applying APPs

Any personal information issues related to the following listing should be referred in the first instance to the Synod Privacy Officer for advice. This requirement is due to the complexity and/or uniqueness and/or infrequency of having to comply with these privacy provisions within the Church context. It also removes the onus of custodians of personal information having to be fully informed about all the provisions of the Act at any time:

APP 2 – Anonymity and Pseudonymity

APP 4 – Dealing with Unsolicited Personal Information

APP 7 – Direct Marketing

APP 8 – Cross-Border Disclosure of Personal Information

APP 9 – Adoption, Use or Disclosure of Government Related Identifiers

Exceptions listed in any APP

Permitted general situations

Permitted health situations

The Church's Privacy Network

Introduction

Page 1 of this manual has already described the crucial role of custodians of personal information on behalf of the Church. Because of the breadth and complexity of the Church's operations in South Australia it is necessary to formally recognise this custodial role in:

- Assisting the Synod Privacy Officer in performing his/her legislative role on behalf of the Church
- Ensuring the application of the APPs and other aspects of the privacy legislation are appropriate for the local context within which they are called on to hold personal information.

These custodians across the Church are called “Privacy Contact Persons” or PCPs. They need to be formally recognised in this role by the most relevant governing council. As well as performing a role locally in relation to privacy issues on behalf of their governing council, they become part of a network with fellow PCP’s and the Synod Privacy Officer who together commit to applying the spirit as well as the substance of the privacy legislation within the Church.

All governing councils/committees/boards should have a nominated PCP.

Role statements

Synod Privacy Officer

This role will be to:

- oversight the application of the Act and the APPs in all church activities within the scope of this policy, including ensuring that the information being collected is appropriate, safely stored, accurate and up-to-date
- keep abreast of changes with the privacy legislation and its Codes of Practice
- liaise when necessary with the Office of Australian Information Commissioner
- provide guidance to congregations and faith communities through provision of:
    - written/telephone advice and support
    - resources and manuals
    - training
    - information about any Privacy Codes of Practice
- act as a first point of contact where a privacy query cannot be answered satisfactorily by a PCP
- receive and deal with complaints about the application or lack of application of the provisions of the Act in any part of the Church
- maintain a network of PCP’s
- oversight the annual audit of privacy processes to be conducted between 1st January and 31st March each year
- coordinate the collection of annual audit certificates from congregations and faith communities.

Governing Councils, Committees or Boards collecting personal information for their primary purpose

- ensure the development of its own governing council privacy policy statement (preferably using the Uniting Church SA Congregation privacy policy template) . http://sa.uca.org.au/documents/called-to-care/Privacy/Congregation-Privacy-Policy-template-2014.pdf
- Appoint a trusted person to the PCP role and the Church Privacy Network
- Promote compliance with privacy legislation as a pastoral as well as a legal responsibility and a critical component of its Called to Care policy and practice
- Encourage a public profile to be given to privacy matters in its context and make privacy resources e.g. pamphlets readily available
- Remain sensitive to the workload of the PCP and takes corrective action where necessary
- Receive reports from the PCP time to time on collection, security, use, access, correction, notification and disclosure processes being used
- Ensure that a regular audit of compliance with the privacy legislation is undertaken and the results of the audit are forwarded to the Synod Privacy Officer

Privacy Contact Persons (PCP)

The PCP's role will be to:

- Accept a custodial role in relation to personal information that needs to be collected for the activity or function for which their governing council has responsibility
- Familiarise themselves with the provisions of the Act and specifically the APP requirements relating to management, collection, use, correction, security, disclosure, correction and notification
- be the focus of any privacy queries or complaints from any person associated with the activities for which the governing council etc are responsible.
- distribute privacy information to individuals as appropriate
- seek to report regularly to your governing council/committee/board
- be a member of the Uniting Church SA's PCP Network
- conduct an annual audit of the appropriateness of personal information being collected, its accuracy, security, disclosure, use and relevance and:
    - complete an annual audit certificate to be sent to the Synod Privacy Officer . http://sa.uca.org.au/documents/called-to-care/Annual-Compliance-certificate.pdf
    - Make suggestions to your governing council about how privacy management could be improved in your area of responsibility
    - Maintain a Privacy Register
- Refer any privacy related questions requiring clarification to the Synod Privacy Officer and in particular queries relating to:
    - APP 2 – Anonymity and Pseudonymity
    - APP 4 – Dealing with Unsolicited Personal Information
    - APP 7 – Direct Marketing
    - APP 8 – Cross-Border Disclosure of Personal Information
    - APP 9 – Adoption, Use or Disclosure of Government Related Identifiers
    - Exceptions listed in any APP
    - Sensitive information
    - Permitted general situations
    - Permitted health situations

It is important to note that the PCP does not need to personally view any or all personal information, simply to oversee the process.

Complaints Processes

An individual involved with the life of the Church can register a complaint about an alleged breach of the APPs. The Church's preferred process is to attempt to resolve these issues internally by having the complaint mediated by the Privacy Contact Person or if necessary, the Synod Privacy Officer. However individuals can, at any time, access the provisions of the Act in relation to complaint resolution processes and address their complaint to the Office of the Australian Information Commissioner, GPO Box 5218, Sydney NSW 2001 or email enquiries@oaic.gov.au

Practical application of APP's – case studies

As highlighted earlier in the manual, there are a group of APP's that will form the main area of focus for any PCP once the respective privacy policy of a governing council/committee or board is approved.

These are:

APP1 – open and transparent management of personal information

APP3 - Collection of Solicited Personal Information

APP5 - Notification of the Collection of Personal Information

APP6 - Use or Disclosure of Personal Information

APP10 - Quality of Personal Information

APP11 - Security of Personal Information

APP12 - Access to Personal Information

APP13 - Correction of Personal Information

Some more detailed information and practical examples are included for each of these APPs in the following pages.

Australian Privacy Principle 1: Open and Transparent management of personal information

Summary: The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

To fully comply with this principle you should refer to a copy of the Australian Privacy Principles, however, in summary you should note or action the following:

- Review current practices, procedures and systems to ensure compliance with APPs
- Review all information held to determine which parts are personal and/or sensitive information
- Review current policy and if necessary amend (if not using the standard Uniting Church SA policy
- Make policy readily available and free
- Review practices, procedures and systems for handling privacy inquiries and complaints

Australian Privacy Principle 3: Collection of solicited personal information

Summary: The object of this principle is to ensure that an organisation must not collect:

- personal information (other than sensitive information) unless the information is reasonably necessary for one of more of the organisations functions or activities
- sensitive information about an individual unless the individual consents and the information is reasonably necessary for one of more of the organisations functions or activities

To fully comply with this principle, you should refer to the enclosed copy of the Australian Privacy Principles, however, in summary you should note, consider or action the following:

- When collecting information a person must be told the activity or organisational name for which the information is collected and this activity or name should be as specific as practical
- When collecting sensitive information, ensure that the higher protections built into APP 3.3 are observed
- What notification processes are in place to let individuals know the Church holds their personal information?

Practical example

The Dove Uniting Church asks visitors to complete a Welcome Card and put it in the offering plate. To comply with the Privacy Act, this card should now include a statement like the following:

"The Dove Uniting Church is a caring Christian Community. The information gathered on this form will be given to a member of the Pastoral Care Team who may make contact with you. This is done in order to allow the Church to pastorally care for you. You are free not to complete any part of this form, however, by doing so you may limit our ability to make further contact with you.

If you wish to access any personal information held about you or want to find out more about the Church's privacy policy, please contact the Church's Privacy Contact Person: Mr I B A Pigeon

Information that can be collected

Information includes data collected on forms and informal notes

- Be careful of unsolicited information that is received by accident or has not been asked for directly.– refer to APP 4
- You should only collect information that is relevant to the purpose for which it is being collected e.g. baptism, marriage, funeral, church camp, craft group, kids' club, community course.

- When personal information is obtained from a "third party", you must seek permission from the individual concerned before using it.
- Individuals must be given the option of choosing not to have their personal information used by the Church. This is called an "opt out" clause.

Typical information given to individual at the time of the collection process

In most cases the Privacy Information Brochure http://sa.uca.org.au/documents/called-to-care/Privacy/Congregation-Privacy-Information-Brochure-fillable.pdf will cover events and activities run by the church. However if you need to create your own document, the following must be included:

- the area's/activity contact details;
    - the name,
    - street and postal addresses,
    - the main telephone and fax numbers and
    - appropriate e-mail addresses;
- the kinds of personal information the Church holds;
- the main purposes for which the Church holds the information;
- how the information is collected;
- how the Church stores or secures information (but it is not required to give specific details of security measures that would jeopardise the security of the personal information it holds.)
- how the information will be used;
- who the information will be disclosed to;
- how to contact the Privacy Contact Person;
- how the Church handles requests for access to personal information

How information is collected

- Written consent is the best consent.
- An alternative is to use the standard Privacy Information Brochure that is referred to in the Resources paragraph of this manual and distribute it whenever you collect information.

  http://sa.uca.org.au/documents/called-to-care/Privacy/Congregation-Personal-Information-Form.pdf

Understanding sensitive information requirements

- "Sensitive information" is information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information.
- The Church will only collect and use sensitive information where the individual has consented.
- Further consent will be obtained if sensitive information is to be used for another use other than the purpose stated at the time of collection.
- If a person cannot give consent due to some incapacity, consent can be obtained from the individual's guardian.
- If an individual does not give consent, the individual must be made aware of the consequences.
- Sensitive information should not be collected on the off chance that it will be helpful to have it some time in the future.

Sensitive information should be destroyed when no longer required.

Practical examples

> Michael is going into hospital to have an operation on his prostate. To prayerfully support people who are part of the Church's faith community who are either unwell or going into hospital, his Church has established a prayer chain. The Church also prays for these people in the intercessory prayer during worship services.

Michael's consent must be obtained before his operation is mentioned either on the prayer chain or during intercessory prayer. If Michael does give his consent, he must also indicate what level of information he wishes the faith community to know.

Betty Jones has confided in her minister that she has cancer during a counselling session.

The church is planning a healing service. It is inappropriate for the Minister to ask the office administrator to send Betty an invitation to attend the service because, under the Privacy Act, medical information is classified as sensitive information.

However, it would be okay for the Minister to personally and discreetly invite Betty or to extend a general invitation from the pulpit.

The parents of a child planning to attend church family camp are asked to complete a medical form.

This information is gathered as part of creating and ensuring a safe environment, and to help in the case of an emergency. If you think this information is helpful to have another purpose (Eg for the weekly Kids Club) you should specify this on the consent form and give an option to "opt out".

Collecting information verbally

- In many cases a Church will legitimately collect information about a person or persons other than through the use of a printed form.
- Wherever possible you should still seek consent to collect and retain the information.

Church offices/reception areas

- Church offices and reception areas can sometimes be staffed by a team of volunteers. It is important that they are familiar with the principles of the Privacy Act.
- Three simple things that you can do are:
    - **Phone messages** – The person taking the message should only record essential information. They should not ask questions that may encourage the caller to disclose personal or sensitive information.
    - **Phone pads** – Message pads should not be left in a public place where others can view personal or sensitive information. Care should also be taken with message pads with carbon copies.
    - **Standard message sheet** – It may be helpful to have a standard sheet for collecting information to encourage a standard process. This sheet could include the statement "Do you consent to this personal information being recorded and given to other appropriate persons in the church?"

Collecting information via a website/on-line data base system

- If collected on-line, the website or on-line system must include a clearly identified privacy statement as a "primary purpose" protection. This must be a part of the login process before personal information prior to the personal information being able to be viewed. The privacy statement should be agreed to as a part of every log in process. For example the "All Contacts" data base used by Presbytery and Synod staff has the following privacy statement which a far broader consent statement than many data bases holding personal information will need to be:

  "Information collected and recorded in the Synod Database needs to be managed in accordance with the Uniting Church SA Privacy Policy.

  This information has been collected for the primary purpose of communication and correspondence related to activities conducted by the Presbytery and Synod of SA. It may also be used in relation to any authorised activities of other Synods or the Assembly of the

Uniting Church in Australia. If you need clarification on what constitutes an authorised activity please contact the Synod Office or email privacy@sa.uca.org.au.

If you have a need to pass on any information contained in this Database to another person or group, you must ensure that you are complying with the Presbytery and Synod's Privacy Policy. This Policy is available on the Presbytery and Synod website. http://sa.uca.org.au/documents/called-to-care/Privacy-Policy-2014.pdf

If you are aware of any changes required to the Synod Database, please contact the Synod Office or email databasechanges@sa.uca.org.au Please do this as soon as possible as this is a requirement of the Access and Correction Privacy Principles. (APP's 12 and 13)

Age of Consent

- The Privacy Act does not specify an age after which individuals can make their own privacy decisions.
- The Church's standard practice of requesting parents / guardians to give consent for their child's participation in an activity still applies.
- That is, when a Church needs to collect information about an individual who is under 18, it must make every effort to ensure that the parent / guardian provides express consent to information being collected.

Contractors

- When an area/activity of the Church enters into an agreement with a contractor, and that contractor will have access to personal information, the contract should include a clause stating that the contractor will adhere to the Privacy Act. Note: contracts should be between The Uniting Church in Australia Property Trust (SA.) on behalf of "area/activity name" and the contractor, as the former is the sole legal entity for the Church.

Record Keeping

- You should keep a record of all information you collect

Australian Privacy Principle 5: Notification of the collection of personal information

Summary: At the time of collection or as soon as possible after personal information has been collected, an entity must take such steps (if any) as are reasonable to notify the individual:

- the identity of the Church area/activity
- whether it collects information from sources other than the individual
- whether the information is being collected for reasons other than the individual's participation in the activity for which personal information is being collected.

Australian Privacy Principle 6: Use and Disclosure

Summary: If an area holds information for a particular purpose it should not use or disclose information for other than the purpose for which it was collected (primary purpose) unless the person has consented, or the secondary purpose is related to the primary purpose and an individual would reasonably expect such use or disclosure.

Practical Example:

Each member of Dove Uniting Church has their contact details published in a directory.

To free the church to use this data for broader purposes, it is recommended that at the time the information is collected, consent is also obtained to use the information for any other related church activity.

The consent form should also include an "opt out" clause so that the person can state if they only want this information to be used for the directory and no other secondary purpose.

An example of an "opt out clause" is:

☐ *Please tick this box if you wish your details to ONLY be used in our directory and not to be available for any other church related activity.*

To fully comply with this principle you should refer to the enclosed copy of the Australian Privacy Principles, however, in summary you should note the following:

- Sensitive information, such as medical information, should not be used for any other purpose than that stated at the time of collection, unless consent has been has been obtained.

Notwithstanding the main thrust of the above principle, there are a number of situations where it is appropriate to disclose information:

1. When it is required by law or by a law enforcement agency;
2. To lessen a serious threat to a person's health or safety (refer example below);
3. When it is in the same context as the indicated purpose (related use); or
4. When consent has been obtained.

Reasons 1 and 2 are explained in more detail below. If a situation arises and the Privacy Contact Person is uncertain of what can be required or authorised by law, contact should be made with the Synod's Privacy Officer and certainly before making contact with a recognised law enforcement agency.

1. "When it is required by law or by a law enforcement agency"
    - A Church area/activity can use or disclose personal information when it has reason to suspect that an unlawful activity has occurred.
    - Where possible, the Synod's Privacy Officer should be contacted prior to
    - The Church will use or disclose personal information where this is required by Commonwealth, State or Territory legislation, or by the Common Law. This is a legal obligation.
    - Where the use or disclosure of personal information is authorised by law, the Church can decide for itself whether to disclose the information or not.
2. "To lessen a serious threat to a person's health or safety"
    - Personal information may be given out where it is believed that there is a serious and imminent threat to the life or health of the person concerned or to a third party.
    - Where personal information is disclosed in these circumstances, it is very important that a record of the disclosure be kept.

Practical example:

Charlie Smith is a haemophiliac and is now HIV positive as a result of a blood transfusion. Charlie is a group leader at a Day Camp. Whilst participating in a recreational activity, Charlie slips and cuts himself quite severely. An ambulance is called. The qualified first aid volunteer has access to medical records of all delegates at the Day Camp and is aware of Charlie's medical condition.

In this instance there are two types of threats: the first to Charlie himself and the other to the ambulance personnel and hospital staff. In this instance, it would be appropriate for the first aid volunteer to inform the ambulance staff about Charlie's condition so they can

treat his cut both appropriately and safely. It is also very important that this information is given in a discrete manner.

Australian Privacy Principle 10: Quality of personal information

Summary: The Church will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete, up-to date and relevant.

Practical Example:

The church produces an annual directory. It would be reasonable to expect that all members in that directory would have the opportunity to update their details or opt out of inclusion in the directory at the time of its reprinting.

If the church was informed part way during the year that someone no-longer wished to be included in the directory, it would not be necessary to re-call all directories. However, any directories held in reserve should be updated.

To fully comply with this principle you should refer to the enclosed copy of the Australian Privacy Principles, however, in summary you should note the following:

Correcting information

- A Church area/activity must take reasonable steps to correct information about an individual where that information is not accurate, up-to-date and complete.
- If an individual and the group or entity collecting the information is unable to agree about whether personal information is accurate, up-to-date, complete and relevant, the Church must, at the request of the individual, take reasonable steps to note on the person's record their claim that the information held on them it is not accurate, complete and up-to-date.

Australian Privacy Principle11: Security of personal information

Summary: The Church will take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access modification or disclosure.

Practical Example:

It has been common practice for churches to invite people to sign a visitor's book. This has enabled the congregation to send the visitor a welcome letter. The book has also been available for anyone to access in the church foyer.

To be compliant with the Privacy Act, this method of collection is no longer suitable. Individual cards that can be handed to the door steward or into the offering bag are the best option. If, however, the visitor's book is only used for entry of names and a comment, then it is fine to continue with this practice provided that a sign clearly states public access.

Practical Example:

Church directories should not be kept in the foyer for anyone to access. All surplus directories should be held in a secure location, and made available upon request.

Practical Example:

Dove Uniting Church runs the following activities: KUCA Camp Out, Ignite (a youth group activity), Alpha, Cancer Support Group, Adult Fellowship, Marriage Preparation Courses and 4 soccer teams.

The Church Council has decided to place all personal information into an electronic database and that only the office administrator should have full access to the database. It has also decided that each activity co-ordinator should only be able to access the part of the database relevant to them.

A hardcopy of all original data will be kept in a secure location for future reference.

To fully comply with this principle you should refer to the enclosed copy of the Australian Privacy Principles, however, in summary you should note the following:

Storage and Back up

- All paper records should be kept in lockable storage in a central location. eg a filing cabinet.
- All computers should be password protected with the passwords updated on a regular basis. Where multiple users access computers it is advisable to limit access to only the files they need to use.
- When sending emails to multiple recipients, addresses should be placed in the BCC (blind copy) field.
- Back up files should also be held in a secure location.

Destroying records

- Information no longer needed should be destroyed.
- Personal information should only be destroyed by secure means. Eg shredding, incineration.
- Garbage disposal or recycling of documents should only be used for documents that do not contain personal information.

Sharing information

- If personal information is shared via phone, fax or e-mail, the Church should take every step to ensure the information is sent to the intended recipient. Such steps will include double-checking facsimile numbers and e-mail addresses before sending personal information, and confirming receipt; and checking a person's identity before giving out personal information over the telephone.

Australian Privacy Principle 12: Access to personal information

Summary: An individual has the right to request access the personal information that the Church holds about them unless prevented by the exception provisions listed in APP 12.3

Practical Example:

Jenny's parents are divorced and share joint custody of Jenny. Jenny's Day Camp registration has the contact details for both Jenny's mother and father. Jenny's father has made a request to access the personal details held about Jenny and himself.

The Church does not have to refuse access to the details as long as it is able to remove details of Jenny's mother from the document before it is released to Jenny's father or consent has been given by Jenny's mother.

Practical Example:

John Brown has concerns about the information that the stewardship recorder has in relation to his planned giving.

John contacts the Privacy Contact Person who, in turn, contacts the stewardship recorder and arranges for the information to be available for John to view.

The Privacy Contact Person does not need to personally view the information, simply to oversee the process. This ensures John's privacy is maintained.

To fully comply with this principle you should refer to the enclosed copy of the Australian Privacy Principles, however, in summary you should note the following:

Checklist for requests to view personal information

Prior to granting a person access to the information that the Church holds about them, the Privacy Contact Person should follow this basic checklist:

1. Ask for the request in writing.

- Record the request in the Privacy Register.
- Determine if an exception should be used after consultation with the Synod Privacy Officer. The exception provisions include the following possible scenarios:
- it is unlawful to provide the information;
- it poses a serious and imminent threat to the life or health of any individual;
- it has an unreasonable impact upon the privacy of other individuals; or
- the request is frivolous or vexatious.
-
- If an exception is used, the Privacy Contact Person is required to give their reasons for denying access or refusing to correct personal information. However, this is not required where such a disclosure would prejudice an investigation against fraud or other unlawful activity.
- Acknowledge the request and arrange a time to view the information.
- A request to access personal information does not need to be acted upon immediately.
- A written request for access should be acknowledged within 14 days.
- If granting access is straight forward, it is appropriate for the Church to grant access within 14 days, or if giving it is more complicated, within 30 days.
- Authenticate the identity of the person seeking access to the personal information (E.g. photo ID).
- 6. If the information needs to be corrected this should be done as soon as possible.
- 7. If the individual is not happy with the outcome despite the prior consultation with the Synod Privacy Officer, contact the Synod Privacy Officer again to inform the position of the dissatisfaction of the individual.

Australian Privacy Principle 13: - Correction of personal information

Summary Where personal information is being held, and the APP entity satisfies itself that the information is inaccurate, out of date, incomplete, irrelevant or misleading or if the individual requests a correction, the entity must take reasonable steps to correct this information on the individual.

To fully comply with this principle you should refer to the enclosed copy of the Australian Privacy Principles but it should be noted that APP13 carries specific provisions dealing with:

- The notification of correction to a third party
- The process if a correction request is refused
- The preparation of an associate statement if a refusal is given
- Deadlines for dealing with requests for correction
- Charging to undertake the correction

Consent for holding personal information

The Presbytery and Synod Privacy Policy contains two specific pieces of guidance in relation to consent.

General Consent Table

The general consent template used in the policy uses wording that implies the maximum breadth of consent to be sought by the Church. As indicated earlier in this manual the more specific the definition of the primary purpose for collection, the better. The minimum standard is as follows:

"This information has been collected for the primary purpose of communication and correspondence related to activities conducted by the Presbytery and Synod of SA. It may also be used in relation to any authorised activities of other Synods or the Assembly of the Uniting Church in Australia."

Opt in/Opt out

The Uniting Church policy position for choosing an **opt in** or **opt out** information collection process are as follows:

"Individuals giving consent to having their personal information collected, stored ands used for the primary purpose can be asked to provide one of two types of consent:

- *Opt in – this consent requires the specific authority of an individual to have their information collected.*
- *Opt out – this consent is a default position in that, unless the organisation is advised by the individual to remove personal information, the information will continue to be stored.*

The Church's policy is that for the first time entry of an individual's personal information on any data base or recording system, an "opt in" process must be used and the accompanying consent form stored securely. A continuation of the "opt in" process is strongly recommended for regular events such as annual registration processes to ensure changes of personal information since the last registration process are captured. However in situations where a periodic review of the accuracy of personal information being held on data bases and other personal information storage mechanisms and where using an "opt in" process is impractical or unreasonable, putting an an "opt out" option to individuals is acceptable."

Conducting an audit

Conducting an audit will allow you to assess what corrective action (if any) needs to be taken. An audit is a fundamental requirement of APP1 – open and transparent management of personal information. Continuous improvement is a key management process,

You will need to audit any activity that involves the collection of personal information. These may include:

- Church groups (E.g. Sunday school, kids' club, youth group, sports team, fellowship groups, home groups, prayer network)
- Outreach programs (E.g. Alpha group, craft group, playgroup)
- Pastoral care program
- Church sponsored excursions and camps
- Church publications (E.g. directories, community newsletter)
- Stewardship program
- Minister's counselling notes
- Preparation for baptism, confirmation, marriage, funerals

Audit checklist

It is recommended that you use the following checklist when undertaking an audit:

1. Make a list of the activities that your church/ area of activity runs that involve collecting information.
2. Photocopy an audit information sheet (refer resources section of the manual) for each activity.
3. In consultation with the co-ordinator/s for each activity, complete an audit information sheet. A sample of how to complete the form is enclosed
4. As you complete each audit, put together an action plan outlining the further tasks you need to take to ensure compliance. These may include:
    - destroying information that is no longer required;
    - correcting current information;
    - determining what information held is "sensitive information" and taking appropriate action;
    - making any appropriate changes to how you store information. Distribution methods may need to be revised – e.g. directories.
5. File each audit information sheet in your Privacy Register. It is important that you keep this information so that you have a record of how you conducted your audit.

Keeping a privacy register

The Church's Privacy Contact Person should keep a register.

- A "register" is a record of all matters relating to compliance with the Privacy Act in your church. It should include:
    - A record of how the Privacy Act has been implemented in your church (E.g. when and how your congregation was informed about the Act, and any action that your Church Council has taken)
    - Audit information sheets for each activity;
    - A copy of your Privacy Compliance Certificate;
    - A record of any enquiries or complaints made in relation to personal information.
    - A record of any disclosure of any personal information other than what consent has been gained for.
    - A record of all requests to "opt out."
- All records will be kept for a minimum of seven years unless directed by law or the Privacy Commissioner to do otherwise.

Other important information about church records

- It should also be noted that some church records are required to be permanently held and not destroyed e.g. Baptisms, Funerals & Memberships (Refer UCA regulations).
- The Register of Marriages should also be permanently held.
- All of these records should be kept securely in a locked filing cabinet or cupboard.
- Historic church records (e.g. membership roles, and records of baptisms and funerals) should be sent to the Synod archivist who will forward them to the Mortlock Library.

Privacy Resources and contact details

RESOURCES

Link to the Information Commissioners website www.oaic.gov.au

Congregation privacy and public prayer

Congregation privacy brochure

Congregation information and permission form

Congregation Privacy policy template

CONTACT DETAILS

Uniting Church SA Synod Privacy Officer: Mr Malcolm Wilson

GPO Box 2145 Adelaide SA 5001.

Phone number: (08) 8236 4206.
Fax number: (08) 8236 4201.
Email: privacy@sa.uca.org.au

Office of the Australian Information Commissioner (Privacy)

Enquiries Line 1300 363 992.

Email: enquiries@oaic.gov.au

Further contact details : http://www.oaic.gov.au/about-us/contact-us-page

Privacy Complaints: http://www.oaic.gov.au/privacy/privacy-complaints

Appendices

Uniting Church SA Privacy Policy and key definitions

Approved by Standing Committee April 4th 2014

Download here http://sa.uca.org.au/called-to-care/privacy-policy

Australian Privacy Principles

(for definitions of terms not included in the Uniting Church SA policy, refer to the Act)
http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act

Part 1 – Consideration of personal information privacy

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

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

Compliance with the Australian Privacy Principles etc.,

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

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

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

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

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

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

(a) free of charge; and

(b) in such form as is appropriate.

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

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

2 Australian Privacy Principle 2—anonymity and pseudonymity

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

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

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2—Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

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

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

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

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

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

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

4 Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

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

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

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

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

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

5 Australian Privacy Principle 5—notification of the collection of personal information

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

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

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

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

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

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other 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

6 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

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

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

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

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

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

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

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

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

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

7 Australian Privacy Principle 7—direct marketing

Direct marketing

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

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

Exceptions—personal information other than sensitive information

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

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

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

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

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

Exception—contracted service providers

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

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

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

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

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

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

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

Interaction with other legislation

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.

8 Australian Privacy Principle 8—cross-border disclosure of personal information

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

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

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

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

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

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

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

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

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

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

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

Use or disclosure of government related identifiers

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

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

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

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

Regulations about adoption, use or disclosure

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

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

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

Part 4—Integrity of personal information

10 Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

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

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

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

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

12 Australian Privacy Principle 12—access to personal information

Access

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

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

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

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

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

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

Access charges

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

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

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

Refusal to give access

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

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

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

13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

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

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

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

Refusal to correct information

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

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

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

Dealing with requests

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

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).