A PRACTICAL EXPLANATION

OF THE

PRIVACY AMENDMENT ACT 2000

PRIVACY POLICY OF
THE BAPTIST UNION OF VICTORIA

The Privacy Amendment (Private Sector) Act 2000

Baptist Churches in Victoria and the Baptist Union of Victoria all collect personal information from people for a number of reasons.

In society today most people consider the privacy of each individual important.

There is an element of trust involved in giving personal details to an organisation. This document is designed to assist churches to honor that trust as well as to ensure that, where possible, Baptist churches and organisations comply with the Privacy legislation applicable to the Private Sector.

The Privacy Amendment Act (Private Sector) Act 2000 was passed in the Federal Parliament in December 2000. The legislation amended the Privacy Act 1988 that had covered public sector agencies.

The new legislation applies to most private sector organisations. It is the recommendation of the Baptist Union of Victoria that the Baptist Churches in Victoria opt to comply with the requirements of the Privacy Act. This is in order to demonstrate our wish to honor the trust placed in our churches by those who give personal information.

The legislation contains ten National Privacy Principles (NPP's). They cover the areas of:

- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive information.

For more information on these principles, see the legislation, contact the Privacy Commissioner's Office or go to www.privacy.gov.au .

Privacy Policy of The Baptist Union of Victoria

The Baptist Union of Victoria has made a commitment to adhere to the Privacy Act (2000) and to the National Privacy Principles (NPP's) that are contained in the Act. The ten NPP's contained in the Act cover the areas of:

- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive information.

The range of activities in which our Victorian Baptist Churches are involved means that there are a large number of uses that we have for personal information within the church.

Information that is collected includes names, addresses, email addresses, telephone and facsimile numbers, medical details, family information (including spouses, children, guardians and parents' details) credit card numbers and account numbers and any notes that may be taken for counseling purposes.

Churches only collect personal information that is necessary for their activities and in particular only collect sensitive information where it is consented to by the individual or their parent or guardian. Sensitive information is only shared where the churches have a belief that its use or disclosure is necessary to prevent threats to health, life or safety to any individual.

Personal information is not shared without the consent of the individual and it is not distributed to any organisation that is not associated with a Baptist Church.

At the Baptist Union Office, all personal information is stored in secure cupboards, and where possible in secured offices and premises. Any personal information that is in an electronic form is stored in secured facilities. The Baptist Union of Victoria recommends that churches follow this model.

All papers containing personal data is disposed of either by secure paper destruction, shredding or incineration. Disks and other electronic storage devices containing personal data are destroyed when no longer in use.

Individuals may access data that is held by The Baptist Union of Victoria or a church on themselves, by notifying the BUV or the church concerned in writing of their request. The request will be acknowledged by the BUV or the church within 14 days and will arrange a time for the viewing of the data. Information that is out of date or is inaccurate will be updated on written request, or the applicant will be notified of the reason the information will not be updated.

The Baptist Union of Victoria or a Victorian Baptist Church may send out information including newsletters including information from organisations associated with The Baptist Union of Victoria. If an individual in receipt of this information no longer wishes to receive it they should notify The Baptist Union of Victoria or the church concerned in writing of their wish not to receive any further information. Any correspondence of this nature should be addressed to the Privacy Officer.

National Privacy Principles

The Privacy Amendment Act sets out how we should collect, use, keep, secure and disclose personal information. It also gives to individuals the right to know what information an organisation holds about him or her and the right to correct it if it is wrong. The Act has ten National Privacy Principles (NPP's) that cover the following areas:

NPP	Topic	Overview
NPP 1	Collection	Collection of personal information must be fair, lawful and not intrusive. A person must be told the church's name, the purpose of collection, and how to get access to their personal information, and what happens if the person chooses not to give the information.
NPP 2	Use and disclosure	The church should only use or disclose information for the purpose it was collected (primary purpose) unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure.
NPP 3	Data Quality	The church will take reasonable steps to ensure the personal information it collects is accurate and up-to-date.
NPP 4	Data Security	The church will take reasonable steps to protect the personal information it holds against misuse, loss and unauthorised access, modification or disclosure.
NPP 5	Openness	The church will have a document outlining its information handling practices and make this available to anyone who asks for it.
NPP 6	Access and correction	An individual has the right to access the personal information that the church holds about them (although there are some exceptions).
NPP 7	Identifiers	The church must not adopt, use or disclose an identifier that has been assigned by a Commonwealth government agency (ie Tax File number, Medicare number)
NPP 8	Anonymity	Organisations must give people the option to interact anonymously whenever it is practical and lawful to do so.
NPP 9	Transborder data flows	The church can only transfer personal information to a recipient in a foreign country in circumstances where the information can have the appropriate protection.
NPP 10	Sensitive Information	An organisation must not collect sensitive information unless the individual has consented, it is required to do so by law or the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

Practical applications of the National Privacy Principles

National Privacy Principle 1: Collection

Overview

Collection of personal information must be fair, lawful and not intrusive. A person must be told the church's name, the purpose of collection, and how to get access to their personal information, and what happens if the person chooses not to give the information.

What information can we collect?

Information includes data collected on forms and informal notes taken by a Minister or church member.

It also includes information that has been come across by accident or has not been sought directly.

You should only collect information that is relevant to the purpose for which it is being collected, e.g. church camp, craft group, community centre, and baptism.

When information is obtained from a third party you must seek permission from the person concerned before using it.

Individuals must be given the option of choosing not to have their personal information used by the church.

Collecting information on paper

Written consent is the best consent

When information is collected, the following information should be included on the form:

- The identity of the Church and how it can be contacted
- That the person can access their information
- Why the information is being collected
- To whom the information will be disclosed and any law that requires the information to be collected
- The consequences (if any) for the individual if the information isn't provided.

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

A team of volunteers often staffs Church offices. It important that they, as well as paid office staff, are familiar with the principles of the Privacy Act.

Some simple suggestions for the church office are:

- Phone Messages – the person taking the message should only record essential information.

- Phone Pads – message pads should not be left in a public place where others can view personal or sensitive information.
- Standard message sheet – it could 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

If information is collected on-line, the website must have a clearly identified privacy statement. It should be prominent; users should not have to move through several pages to get to it.

Age of Consent

The Privacy Act does not specify an age after which people can make their own privacy decisions.

The standard practice used by the Church or requesting parents or guardians to give consent for their child’s participation in an activity still applies.

Contractors

When a church enters into an agreement with a contactor, and that contractor will have access to personal information, the contract should include a clause stating that the contractor will adhere to the requirements of the Privacy Act.

National Privacy Principle 2: Use and Disclosure

Overview

The church should only use or disclose information for the purpose it was collected (primary purpose) unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure.

The most obvious example of this is in the Church Directory. In most churches the contact details of members are contained in a church directory. So that the church is free to use this data for broader purposes, it is recommended that at the time the information be collected consent be obtained to use the information for other church related activities.

The consent form should include an 'opt out' clause so that the person can have their information in the church directory (primary purpose) but can determine that they do not want their details used for any secondary purposes. The 'opt out' clause could read; please tick this box if you wish your details to ONLY be used in our directory and not be available for other church related activity. There are a number of situations where it is appropriate to disclose information:

- Where it is required by law or a law enforcement agency
- To lessen a serious threat to a person's health or safety
- When it is in the same context as the indicated purpose (related use)
- When consent has been obtained.

Sensitive Information

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 obtained. (Refer also to NPP 10, Sensitive Information.

Serious threats to life, health or safety

Personal information can be given out where it is believed 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 important that a record of the disclosure is kept.

Direct Mailing

There may be occasions where the church will use personal information for direct mailing purposes. Only non-sensitive information can be kept for direct marketing. Recipients should be given an opportunity to 'opt out'. Information collected by the Church CANNOT be passed onto any other organisation so that the latter can use the information to direct market unless consent has been given.

Unlawful Activity

A Church can use or disclose personal information when it has reason to suspect that an unlawful activity has occurred. Where possible, the Baptist Union of Victoria Director of Admin Services should be contacted prior to making contact with a recognized law enforcement agency.

Required or Authorised by Law

A 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. When the use or disclosure of personal information is authorised by law, the Church can decide for itself whether to disclose the information or not. If a situation arises and the Church Leadership is uncertain of what can be required or authorized by law, contact should be made with the BUV's Director of Admin Services.

National Privacy Principle 3: Data Quality

Overview

The church will take reasonable steps to ensure the personal information it collects is accurate and up-to-date.

A Church 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 a Church are unable to agree about whether personal; information is accurate, up-to-date and complete, 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 is not accurate, complete and up-to-date.

As an example, most churches produce an annual church directory. It would be reasonable to anticipate 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 partway through the year that someone no longer wished to be included in the directory it would not be necessary to re-call all the directories. However, any directories that were held in reserve should be updated.

National Privacy Principle 4: Data Security

Overview

The church will take reasonable steps to protect the personal information it holds against misuse, loss and unauthorised access, modification or disclosure.

Storage and backup

- All paper records should be kept in lockable storage in a central location, e.g. a filing cabinet.
- All computers should be password protected with the passwords updated on a regular basis. When multiple users access computers it is advisable to limit access to only the files they need to use.
- When sending emails to multiple users, addresses should be placed in the BCC (blind carbon copy) field.
- Backup 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; i.e. shredding.
- 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 by phone facsimile or email, the church should take steps to ensure the information is sent to the intended recipient. Such steps will include double-checking facsimile numbers and email addresses before sending personal information, and confirming receipt, and checking a person's identity before giving our personal information over the telephone.

National Privacy Principle 5: Openness

Overview

The church will have a document outlining its information handling practices and make this available to anyone who asks for it.

In creating your own document, which is recommended, to cover activities and events run by the church you will need to include the following information:

The church's contact details:

The name

Street and postal addresses

Main telephone and facsimile numbers

Appropriate email addresses

The kinds of personal information the church holds

The main purposes for which the church holds the information

How the information is collected

To whom the information will be disclosed

How to contact the Privacy Contact Person

How the church handles requests for access to personal information.

National Privacy Principle 6: Access and Correction

Overview

An individual has the right to access the personal information that the church holds about them (although there are some exceptions).

Prior to granting a person access to the information the Church holds about them, as a minimum, the following basic checklist should be followed:

- Ask for the request in writing
- Record the request in your Privacy Register
- Determine if an exception is applicable (exceptions are);
- 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
- The request is frivolous or vexatious.

If an exception is used, the Church 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, we recommend, should be acknowledged within 14 days
If granting access is straight forward, the church should do so within 14 days or if giving access is more complex, then within 30 days.

Authenticate the identity of the person seeking access to the personal information

If the information needs to be corrected this should be done as soon as possible

National Privacy Principle 7: Identifiers

Overview

The church must not adopt, use or disclose an identifier that has been assigned by a Commonwealth government agency (i.e. Tax File number, Medicare number)

The Church may allocate its own identification numbers or codes to identify members of the church it so wishes.

The Church cannot adopt a Tax File or Medicare number as that identification number.

National Privacy Principle 8: Anonymity

Overview

Organisations must give people the option to interact anonymously whenever it is practical and lawful to do so.

Unless a church has a good practical reason which they have described at the time of the collection of the information e.g. ‘we want to send you information about our church’, or legal reasons to require identification, people must be given the opportunity to remain anonymous.

National Privacy Principle 9: Transborder Data Flows

Overview

The church can only transfer personal information to a recipient in a foreign country in circumstances where the information can have the appropriate protection

Before a Church sends information internationally it must obtain the individual’s consent in writing and the individual’s directions for secure transfer of the information.

National Privacy Principle 10: Sensitive Information

Overview

An organisation must not collect sensitive information unless the individual has consented, it is required to do so by law or the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

Sensitive information is information about an individual’s racial or ethnic origin, political opinions, memberships or affiliations, 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.

A 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 the individual cannot give consent due to some incapacity, consent can be obtained from the individual’s guardian.

If the individual does not give consent, the individual must be made aware of the consequences (if any).

Sensitive information should not be collected on the ‘off chance’ that it would be helpful to have it some time in the future.

Sensitive information should be destroyed when it is no longer required.

An individual's consent MUST be obtained before any medical condition or operation is mentioned either in a prayer chain or in a worship service. If consent is given, it must also indicate what level of information the individual wishes the faith community to know.

If information regarding a medical condition is obtained in a counseling session, it is NOT APPROPRIATE for that information to be passed to a third party even if that was simply to invite the individual to a healing service.

Conducting a Privacy Audit

Conducting a privacy audit will help you to determine if there is any action that needs to be taken at your church.

You need to include in the audit any organization within your church that collects personal information. These groups may include;

- Church groups; (Sunday school, kids club, youth group, sporting teams, fellowship and home groups, prayer network)
- Outreach programs (Alpha, craft group, playgroup)
- Pastoral Care Program
- Church sponsored excursions and camps
- Church publications (newsletters, directories)
- Stewardship or giving program
- Pastor's counseling notes
- Preparation for Baptism, confirmation, marriage funerals.

Audit Checklist

Make a list of the activities in your church that collect information.

Photocopy an audit information sheet for each activity

In consultation with the co-ordinator of the activity complete the audit sheet.

As each audit is completed, put together an action plan outlining the issues to be addressed to ensure compliance for each particular group. This could include:

- Destroying information no longer required
- Correcting current information
- Determining what information is 'sensitive information' and taking appropriate action
- Making appropriate changes to how you store information.

File each completed audit in your Privacy register. You should keep this information to indicate how you went about conducting the audit.

Audit Information Sheet

NOTE: There are no "right: answers. This form is designed to help you think through the issues and required actions.

Name of Activity: _____

Questions & Example	**Answer**	**Further Action Required**
What type of information is collected? (eg Contract details, family information, date of birth, medical details)		
Does this information include "sensitive information?" (eg medical records, counselling notes)		
Has consent been given to hold the information stated in the above answers?		
Purpose of collection? (eg to ensure safety, pastoral care)		
Is it relevant? Do we need to collect it? (eg Yes)		Note: If you answered "No" you must delete this information.
Is the information we have correct? (eg Don't know)		Note: If you answered "No" you must destroy or update your information.
How often is the information updated? (eg annually)		
Who is it collected from? (eg the individual or a third party?)		Note: If you answered "Third Party" consent should be sought from the individual.

Questions & Example	Answer	Further Action Required
How is it collected? (eg verbally or by form?)		
Is the person who collects the information aware of the Privacy Act and its implications? (eg elder, minister, fellowship leader)		Note: If you answered "No" – do you need to offer training?
Is the information being used for the purpose it was originally collected for? (eg No. Alpha Newsletter is sent to people who registered for our craft group)		
Where is the information stored? Is it secure? (eg church office, foyer, individual's home?)		Note: If you answered "No" – you will need to make it secure.
Is access to the information limited to only those people who need it? (eg anyone with a key to the storage cupboard can get it)		Note: If you answered "No" – you may need to limit access.
Is the distribution method of collected information appropriate? (eg pigeon holes and foyer table are open to anyone to access)		Note: If you answered "No" – you may need to rethink your distribution method.
What needs to be done next time we update this information? (eg Add appropriate wording to registration forms)		

All sections of this form have been completed and steps are in place to undertake any actions required.

_____ _____ _____

Privacy Contact Person 's Signature Activity Co-ordinator's Signature Date

Keeping a Privacy Register

The Church's Privacy Contact Person (usually the Secretary, Administrator or Pastor) should keep a Privacy Register

A register is a record of all the 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
- Audit information for each activity
- 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 should be kept for a minimum of seven years unless otherwise directed by law or the Privacy Commissioner.

Other important information about church records

Some church records contain information that is required to be kept permanently and never destroyed such as Baptisms, Weddings, Funerals and Membership.

The register of Marriages should also be permanently kept. All of these records should be kept in a locked filing cabinet or cupboard.

Historic church records that are no longer used such as full membership roles and records of funerals and baptisms should be forwarded to the Baptist Union of Victoria Archives where they will be catalogued and stored.

Disclosure and collection statements

Suggested wording for Church Directories

"In accordance with the Privacy Policy of The Baptist Union of Victoria any information contained in this directory will be used only for the ministry of this church and activities related to this church. The information will not be released to any organisation outside of this church".

Suggested wording for Care or Prayer Cards

"In accordance with the Privacy Policy of The Baptist Union of Victoria, any information collected on this card will be used only for the ministry of this church and activities related to this church. You are free not to complete any part of this card but this may limit our ability to respond to your request. It is also a requirement of our Privacy Policy that any information given on behalf of another person is done so with their consent. If you are seeking prayer on behalf of a third person please use only first names.

Checklist for Collection of Information

In the future when your church collects information it should adhere to the Privacy Act.

It is best to request all information in writing. If information is collected verbally then it should be checked for correctness.

Here are 11 simple steps to follow:

1. Clearly state who is collecting the information, e.g., Happy Valley Baptist Church on behalf of Tuesday Craft group.

2. Be clear about what information is being collected, e.g., name, address & phone number.

3. State clearly the purpose you will use the information for, e.g., the church directory.

4. Explain to whom the information will be disclosed, e.g., the directory will only be distributed to attendees of the church.

5. Explain how the information will be stored, e.g., we will store the information on our church computer database that is stored in a secure location.

6. Explain who is responsible for updating the information, e.g. the office administrator updates the database annually.

7. Explain that you will destroy the information when it is no longer required.

8. Include an “opt out” clause, e.g., you do not have to complete this form. If you choose not to, you may limit the church’s ability to care for you pastorally.

9. If your form includes a print out of current data you need to state where you got the information from, e.g., below is a copy of the details printed in last year’s church directory. Please notify us of any changes or incorrect information.

10. Explain how people can access the information that has been collected about them, e.g., if you wish to view the information we hold about you, please contact our Office Administrator.

11. If requesting sensitive information, you should state in what circumstances you will disclose it, e.g., if you have a form collecting medical information in case of an emergency, the form should make it clear that the information will only be disclosed in the event of a medical emergency.

NATIONAL PRIVACY PRINCIPLES

Privacy Act 1988 Schedule 3 – National Privacy Principles

THESE FULL EXPLANATIONS OF THE National Privacy Principles are extracted from a paper located at the following web address;
www.privacy.gov.au/publications/nppgl_01.doc

1. **Collection**

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. **Use and disclosure**

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) both of the following apply:

the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing: it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure–the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:

the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

the disclosure is not contrary to any wish:

expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is responsible for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3. **Data quality**

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4. **Data security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5. **Openness**

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. **Access and correction**

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information–providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information–providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

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

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

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7. **Identifiers**

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an identifier.

8. **Anonymity**

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. **Transborder data flows**

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the NPPs.

10. **Sensitive information**

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

is physically or legally incapable of giving consent to the collection;
or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation–the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual;
and

(b) the information is collected:

(i) as required by law (other than this Act); or

in accordance with rules established by competent health or medical
bodies that deal with obligations of professional confidentiality which
bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organization discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

TABLE OF CONTENTS

Introduction … … … … … 1

Privacy Policy of the Baptist Union of Victoria … 2

National Privacy Principles Summary … … 4

NPP 1: Collection … … … … … 5

NPP 2: Use and Disclosure … … … 7

NPP 3: Data Quality … … … … 9

NPP 4: Data Security … … … … 10

NPP 5: Openness … … … … … 11

NPP 6: Access and Correction … … … 12

NPP 7: Identifiers … … … … … 13

NPP 8: Anonymity … … … … 13

NPP 9: Transborder Data Flows … … … 13

NPP 10: Sensitive Information … … … 14

Conducting a Privacy Audit … … … 15

Audit Checklist … … … … … 15

Audit Information Sheet … … … … 16

Keeping a Privacy Register … … … 18

Disclosure and Collection Statements … … 19

Checklist for Collection of Information … … 20

National Privacy Principles – Full Explanations … 21