Baptist Churches
of South Australia

Privacy Manual

an aid to handling
personal information in compliance
with the 2012 Privacy Amendment
(Enhancing Privacy Protection) Act

Baptist Churches of South Australia

Privacy Manual produced by Baptist Churches of South Australia Inc. March 2014

For more information contact:
The Privacy Information Contact Person
Baptist Churches of South Australia Inc.
35 King William Road, Unley SA 5061 (PO Box 432)
p: +61 8 8357 1755
info@sabaptist.asn.au
f: +61 8 8373 8000
http://sabaptist.asn.au

Contents

CButler/Privacy/BCSA Privacy Manual with key points V7 Mar 2014.pub

Section 1 : Introduction

All organisations collect personal information from people for a variety of reasons.

It is significant to recognise that privacy is very important to most people. It is an act of trust by an individual to provide personal information. In response, we need to take the process of upholding an individual's privacy very seriously.

The Privacy Act

In 2012 the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) was passed. This amendment Act introduces many significant changes to the Privacy Act of 2000 and will commence in March 2014.

The Privacy Amendment Act now applies to most private sector organisations. It has thirteen Australian Privacy Principles (APPs) which all have direct implications for our churches.

All organisations should take all reasonable steps to comply with the requirements of the amended Privacy Act.

If you require more information, please access The Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au/

Additional details regarding the 2012 Privacy Amendment (Enhancing Privacy Protection) Act can be obtained by accessing www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

For simplicity, the original act and all amendments due to commence in 2014 will be referred to as the Privacy Act.

About this Manual

This Manual is designed to help you understand the Privacy Act and what your church will need to do to ensure that it complies.

In **Appendix 1** you will see a copy of Baptist Churches of South Australia Inc. (BCSA Inc.) Privacy Policy. **Section 4** introduces the Australian Privacy Principle's aim to highlight the key points for implementation of each principle.

For a full copy of the Australian Privacy Principles, please access http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform/law-reform-resources

Where the term “church” is used in this Manual, it means the BCSA Inc. and any member Baptist church in South Australia. A church is an APP entity.

The Privacy Information Contact Person's role (see Section 2.1)

The key tasks of the Privacy Information Contact Person are:

- Introduce the Privacy Act and its implications to your church.
- Conduct an audit of how your church collects, collates, and uses personal information *(**refer to Appendix 3** of this Manual)* and identify areas that may need attention.
- Keep a Privacy Register *(**refer Section 6**).*
- Ensure all future collection of information adheres with the Privacy Act *(**refer Section 7**).*
- Handle any enquiries or complaints *(**refer** **Section 8**).*

The Privacy Information Contact Person does not need to personally view the information, simply to oversee the process.

Section 2 : What the church needs to do

1. • Appoint a Privacy Information Contact Person. (This position defaults to the Secretary if no-one is appointed.)

2. • The Privacy Information Contact Person and Pastor read the Privacy Kit and begin to familiarise themselves with the Act. Put the Privacy Act on the agenda of your next Church Leaders' meeting.

3. • Make available the Privacy Information brochures (make sure you have added your Privacy Information Contact Person's details on the brochure). See Appendix 5 for a copy of the Privacy Information brochure.

4. • Complete an Audit Information Sheet for each activity that your congregation does, which involves the collection of personal information. Store the Audit Information Sheets in a register with other privacy details.

5. • Put together an action plan detailing those tasks that your audit has identified that require further attention. This will ensure your congregation complies with the Australian Privacy Principles and the BCSA Privacy Policy. Store these action plans in your register.

6. • Train members of your congregation, who collect, use, store or destroy personal information.
   • Ensure any historically significant records that you do not wish to store are sent to the BCSA office.

Resources available from the OAIC website at
http://www.oaic.gov.au/news-and-events/privacy-awareness-week/resources#heading_1
include posters, an APP Quick Reference Tool and Training material.
These resources can assist in understanding and making your church aware of the new principles due to commence in 2014.

Section 3 : Information relevant to a church office

Church offices:

It is important that all staff (including volunteers) are familiar with the Principles of the Privacy Act.

Four simple things that you can do are:

1 . **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.

2. **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 that have carbon copies.

3. **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?"

4. **Emails –** when sending emails to multiple recipients, addresses should be placed in the BCC (blind copy) field.

5. **Details –** do not give out information of church members to callers.

Collecting information on paper:

Written consent is the best consent.
When information is collected, the following should be included on the form:

- the church identity and how to contact it;
- that the person can access the information;
- why the information is collected;
- to whom the information will be disclosed *(refer APP 6: Use or Disclosure of Personal Information);*
- any law that requires the particular information to be collected; and
- the consequences (if any) for the individual if the information isn't provided.

Whenever you collect information, the standard BCSA Inc. Privacy Information Brochure (copy enclosed in this kit) should be available for distribution.

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.

Collecting information via a website:

If information is collected online, the website must include a clearly identified privacy statement. This must be in a prominent position and users should not have to move through a number of pages to reach it.

Sharing information:

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

Storage and Back up:

All paper records should be kept in lockable storage in a central location, eg: a locked filing cabinet or cupboard. Records that must be kept include: Baptisms, Funerals and Memberships. The Register of Marriages should also be permanently held.
If a church does not wish to store historic church records (eg: membership roles, and records of baptisms and funerals), they should be sent to the BCSA Inc. office. This information will be forwarded to the Mortlock Library in Adelaide.
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. Back up files should also be held in a secure location.

Destroying records *(see also Storage and Back up)***:**

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.

Age of Consent:

Although the Privacy Act does not specify an age at 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 a congregation 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.

Record Keeping:

You should keep a record of all information you collect *(refer Section 6: Keeping a Privacy Register).*

Section 4 : An overview of the Privacy Principles

In 2012 the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) was passed with amendments. This Act introduces many significant changes to the Privacy Act and will commence in March 2014.

The Privacy Amendment Act now applies to most private sector organisations. It has thirteen Australian Privacy Principles (APPs) which all have direct implications for churches. A church is considered an APP entity. The Act sets out how we should collect, use, keep, secure and disclose personal information. It also gives individuals the right to know what information an organisation holds about him or her and the right to correct it if it is wrong. Additional information can be obtained through The Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au/

The Act has thirteen Australian Privacy Principles (APPs) under the following headings:

1 - Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

2 - Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

3 - Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of "sensitive" information.

4 - Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

5 - Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

6 - Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

7 - Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

8 - Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

9 - Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

10 - Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.

11 - Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

12 - Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

13 - Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

APP 1 — open and transparent management of personal information	organisations must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 1 outlines the steps an APP entity must take to manage personal information in an open and transparent way.

An APP entity must:

- take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
- have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.
- take reasonable steps to make its APP Privacy Policy is available free of charge and in an appropriate form (usually on its website).
- upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.

Your church should ensure your privacy policy is up-to-date. If your church does not have a privacy policy, please refer to Appendix 1: Privacy Policy—Baptist Churches of South Australia Inc. as a template for you to use.

Example: Please refer to the Appendices for a copy of the BCSA Inc. Privacy Policy and a Privacy Information Brochure .

> ***Please note:*** *you will need to add your local congregation's details and your church's designated Privacy Information Contact Person to your brochure before duplicating and distributing within your congregation.*

(A copy of the brochure template as a computer file can be obtained from the Baptist Centre.)

Privacy Information Brochure

The BCSA Inc. Privacy Information Brochure in Appendix 5 should be easily accessible to anyone enquiring about what your church is doing in regard to privacy. However, if you want to create your own brochure, the following must be included:

- the church's contact details;
  - the name of the church;
  - street and postal addresses;
  - the main telephone and fax numbers and appropriate email addresses;
  - the name of the church's Privacy Information Contact Person.
- the personal information the church is requesting to be held;
- 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 Information Contact Person;
- how the church handles requests for access to personal information.

APP 2 — anonymity and pseudonymity	organisations are required to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity.

- Anonymity means that an individual dealing with an APP entity cannot be identified and the APP entity does not collect personal information or identifiers.
- A pseudonym is a name, term or descriptor that is different to an individual's actual name.

An APP entity is not required to provide those options where:

- the entity is required or authorised by law, a court or tribunal order to deal with identified individuals, or
- it is impracticable for the entity to deal with individuals who have not identified themselves.

An APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

Unless a church has a good practical reason (which must be described at the time of collection, eg: "we want to send you information about our church") or legal reason to require identification, people must be given the opportunity to remain anonymous or be given the option of using a pseudonym. (A couple of exceptions apply.)

Example: Anthony Smith has recently moved into the local community. On his first visit to Awesome Baptist Church he is asked to fill out a visitor's form. The form states that the information requested is used to help the church pastorally care for all its members. Anthony politely passes up the opportunity to fill in the form. Although Anthony continues to attend worship services, the church must respect his right to remain relatively anonymous. Should Anthony fill out the form, or have his personal information collected in some other manner, it should be at Anthony's initiative and not at the church's request.

APP 3 — collection of solicited personal information	outlines when an organisation can collect personal information that is solicited. It applies higher standards to the collection of "sensitive" information.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 3 outlines when an APP entity may collect solicited personal information.

- An APP entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information.

APP 3 deals with when and how an APP entity can/must collect personal information.

For personal information (other than sensitive information), an APP entity that is:

- an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities;
- an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities.

Personal information must only be collected by lawful and fair means.

Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to agencies).

Sensitive Information

APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.

Example 1: The parents of a child planning to attend a 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".

Example 2: 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.

Example 3: During a counselling session, Betty Jones has confided in her minister that she has cancer.

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.

APP 4 — dealing with unsolicited personal information	outlines how APP entities must deal with unsolicited personal information.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information.

- Unsolicited personal information is information received by an APP entity where the entity has taken no active step to collect the information.

If an APP entity receives unsolicited information, it must decide whether it could have collected the information under APP 3 (collection of solicited personal information).

If the entity determines it could not have collected the information under APP 3, different rules apply according to whether or not the information is contained in "a Commonwealth record".

If the unsolicited personal information is contained in a Commonwealth record, APP 4 does not require it to be destroyed or de-identified.

Other unsolicited personal information that could not have been collected under APP 3 (collection of solicited personal information), must be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.

If an APP entity is not required to destroy or de-identify the unsolicited personal information under APP 4, the entity may retain the information but must deal with it in accordance with APPs 5-13.

What is unsolicited information?

While the Privacy Act does not specifically define the term "unsolicited", it can be generally understood to be information gathered through:

- misdirected mail received by an entity;
- correspondence to Ministers and Government departments from members of the community, or other unsolicited correspondence to an entity;
- a petition sent to an entity that contains names and addresses;
- an employment application sent to an entity on an individual's own initiative and not in response to an advertised vacancy;
- a promotional flyer containing personal information, sent to an entity by an individual promoting the individual's business or services.

Example: When the Office Manager of Awesome Baptist Church looks through the post received that morning, a letter for the neighbour is discovered. The Office Manager should either return the letter to the sender or pass it on to the neighbour without making a record of the postal details.

APP 5 — notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

An APP entity that collects personal information about an individual must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of certain matters.

The matters include:

- the APP entity's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- the APP entity's usual disclosures of personal information of the kind collected by the entity
- information about the APP entity's APP Privacy Policy
- whether the APP entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

Example: Rapture is the upper primary school youth group at Awesome Baptist Church. Whenever a new child joins the group, they are given an information sheet to be filled out by a parent/guardian.

The purpose for collecting the information needs to be clearly stated on the form, along with the contact details for the church. Youth leaders need to know why this information is being collected so they can answer any immediate questions, as well as having access to resources (Privacy Information Brochure) to give to the parent/guardian if requested.

APP 6 — use or disclosure of personal information	outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 6 outlines when an APP entity may use or disclose personal information.

An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the "primary purpose"), or for a secondary purpose if an exception applies.

The exceptions include where:

- the individual has consented to a secondary use or disclosure
- the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
- the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
- a permitted general situation exists in relation to the secondary use or disclosure
- the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
- the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or
- the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.

Example: The Awesome Baptist 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 Awesome Baptist 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: Ms Jac Doe.*

APP 7 — direct marketing	an organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 7 provides that an organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies.

Direct marketing involves communicating directly with an individual to promote goods and services.

Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:

- allow an individual to request not to receive direct marketing communications (also known as "opting out"), and
- comply with that request.

An organisation must provide its source for an individual's personal information, if requested to do so by the individual.

APP 8 — cross-border disclosure of personal information	outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

APP 9 — adoption, use or disclosure of government related identifiers	outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 9 restricts the adoption, use or disclosure of government related identifiers by organisations. APP 9 may also apply to agencies in some circumstances.

An identifier is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.

An identifier, including a government related identifier, is personal information that must be handled in accordance with the APPs.

Where other personal information is handled at the same time as the government related identifier, an organisation must handle the other personal information in in accordance with the APPs.

An organisation must not adopt a government related identifier of an individual as its own identifier of the individual, unless an exception applies.

An organisation must not use or disclose a government related identifier of an individual, unless an exception applies.

Example: The Awesome Baptist Church has prepared a database of its members.

The church can use its own ID (identification) codes to identify members of the church if it wishes. It cannot adopt a tax file or Medicare number as that ID code.

However, the registration form for the annual Rapture Easter Camp can request the Medicare number of the camper as long as the number is not used as an identifier of the child and the information is used in accordance with other APPs.

APP 10 — quality of personal information	reasonable steps must be taken to ensure the personal information collected, used or disclosed is accurate, up to date and complete, having regard to the purpose of the use or disclosure.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Example: The Awesome Baptist 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 recall all directories. However, any directories held in reserve should be updated, and no future directories should contain this information.

APP 11 — security of personal information	reasonable steps must be taken to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified. This requirement applies except where:

- the information is part of a Commonwealth record, or
- the APP entity is required by law or a court/ tribunal order to retain the information.

Example 1: 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.

Example 2: Churches may invite people to sign a visitor's book requesting contact information, and the book may be 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 put 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.

Example 3: Awesome Baptist Church runs the following activities: Kids Holiday Club, a youth group activity, Alpha, Support Groups, Adult Fellowship, Craft groups, Marriage Preparation Courses and a basketball team.

The church leadership group 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.

APP 12 — access to personal information	outlines the obligations when an individual requests to be given access to personal information held about them by the entity.

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access.

APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to information, including the Freedom of Information Act (FOI Act) that provides a right of access to information held by agencies.

Whether a request for access to personal information is better dealt with under APP 12 (including under an informal arrangement) or under the FOI Act may vary according to the circumstances and the wish of the individual seeking access.

Example: Jenny's parents are divorced and share joint custody of Jenny. Jenny's Youth 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 can provide this information to Jenny's father:

- as long as it is able to remove Jenny's mother's details from the document before it is released, or
- consent has been given by Jenny's mother to provide access to this information to Jenny's father.

Checklist for requests to view personal information:

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

1. **Ask for the request in writing**.
2. **Record the request in the Privacy Register** *(refer Appendix 2: Definitions).*
3. **Determine if an exception should be used**.

   If an exception is used, the Privacy Information 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.
4. **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.
5. **Authenticate the identity of the person seeking access** to the personal information (eg: photo ID).
6. **If the information needs to be corrected this should be done as soon as possible** *(refer APP 10: Data Quality).*
7. **If the individual is not happy with the outcome, contact the BCSA Inc's Privacy Information Contact Person** *(refer Section 8: Enquiries and Complaints).*

APP 13 — correction of personal information	outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals

To fully comply with this principle you should refer to the Australian Privacy Principles (Guidelines) at www.oaic.gov.au/*, however, in summary you should note the following:*

Key points

APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

This requirement applies where:

- the APP entity is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
- the individual requests the entity to correct the information.

APP 13 also sets out other minimum procedural requirements in relation to correcting personal information, including when an APP entity must:

- take reasonable steps to notify other APP entities of a correction
- give notice to the individual which includes reasons and available complaint mechanisms if correction is refused
- take reasonable steps to associate a statement with personal information it refuses to correct
- respond to a request for correction or to associate a statement, and
- not charge an individual for making a request, correcting personal information or associating a statement.

APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for agencies, the *Freedom of Information Act 1982* (FOI Act).

Whether a request for correction of personal information is better dealt with under APP 13 (including under an informal arrangement) or under the FOI Act may vary according to the circumstances and the wish of the individual seeking correction.

Example: Adam and Eve Smith are long time members of Awesome Baptist Church and have just welcomed their third child, Seth, into the world. On the first visit with their new baby the Office Administrator (after appropriate gooing and gaaing) suggests that Adam should update their details on the church family register. Adam agrees with this and gets a visitor card to fill out and returns it to the church office on their way out.

Section 5 : Conducting an audit

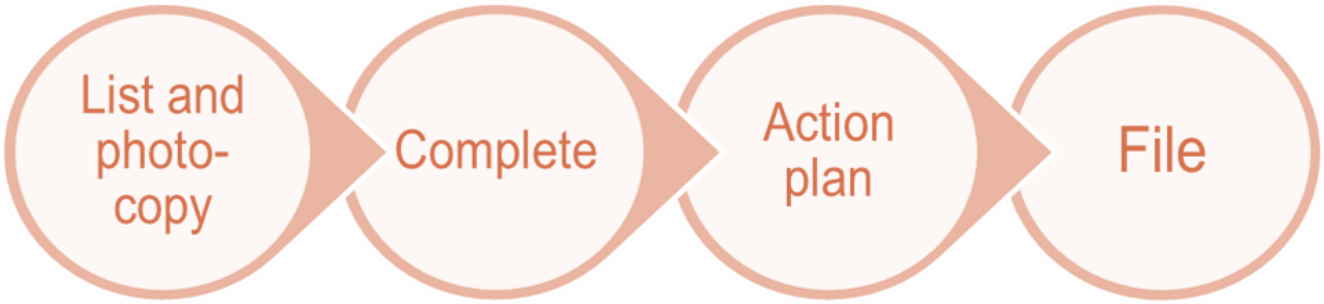
Conducting an Audit will allow you to assess what action (if any) needs to be taken.

You should audit any activity that involves the collection of personal information.

These may include:

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

Audit Checklist:



Make a list of the activities that your church runs that involve collecting information.

Photocopy an audit information sheet *(Appendix 3)* for each activity.

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. *(Refer Appendix 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, eg: directories.

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. *(Refer Section 6: Keeping a Privacy Register.)*

Section 6 : Keeping a Privacy Register

The church's Privacy Information 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 (eg: 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 Checklist;
- 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 Office of the Australian Information Commissioner to do otherwise.

After this time, Privacy Register records should be destroyed in the appropriate manner, eg: shredding, etc.

It should also be noted that some church records are required to be permanently held and not destroyed, eg: Baptisms, Funerals and Memberships (see Section 3: Information relevant to a church office).

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 (eg: membership roles, and records of baptisms and funerals) should be sent to BCSA Inc. who will forward them to the Mortlock Library in Adelaide.

Section 7 : Checklist for collection of information

In future, when you collect information you will need to adhere to the Privacy Act. It is best to request all information in writing. If information is collected verbally it should be verified for correctness.

This check list gives you 11 simple steps to follow.

If requesting **sensitive information,** you should state in what circumstances you will disclose it (eg: if your form includes a statement similar to "Please tell us if you have any medical conditions or allergies?" you should clarify that the information will only be disclosed in a medical emergency.)

1	Clearly state **who** is collecting the information (eg: Awesome Baptist Church on behalf of the Day Fellowship Group).
2	Be clear about **what** information is being collected (eg: name, address, phone number, and birthday).
3	State **clearly** the purpose you will use it for (eg: the annual Fellowship Directory).
4	Explain who the information will be **disclosed** to (eg: the directory will only be distributed to members of the fellowship).
5	Explain **how** it will be stored (eg: "We will also keep these details on our church database which is stored in a secure location").
6	Explain **who** is responsible for updating the information (eg: "The database is updated annually by the office administrator").
7	Explain that you will **destroy** the information when it is no longer required (eg: information about past members is not kept).
8	Include an "**opt out**" clause (eg: you do not have to complete this form, however, if you choose not to, you may limit the fellowship's ability to pastorally care for you).
9	If your form includes a print out of current data you need to state **where** you got that information from (eg: Below is a copy of the details printed in last year's fellowship directory. Please notify us of any changes or incorrect information).
10	Explain how they can **access** the information that has been collected about them (eg: if you wish to view the information we hold about you please contact our Privacy Information Contact Person).
11	Include the name and contact details of the **Privacy Information Contact Person** (eg: Awesome Baptist Church's Privacy Policy Information Contact Person is Ms Jac Doe).

Section 8 : Enquiries and Complaints

Enquiries

If an individual has a question about the information that the Church holds about them, they are to enquire with the church's Privacy Information Contact Person.

For more information look at the "Checklist for requests to view personal information" *(refer APP 12: Access to Personal Information). The church's Privacy Information Contact Person does not need to contact the BCSA Inc. office, unless they believe that the enquiry will lead to a complaint or dispute (see Complaints).*

Complaints

If there is a complaint or dispute, the complainant should detail their concerns in writing and forward them to BCSA Inc's Privacy Information Contact Person.

The BCSA Inc's Privacy Information Contact Person will record the correspondence and, together with the local Privacy Information Contact Person, deal with it as necessary.

Alternatively, the individual can complain direct to the Office of the Australian Information Commissioner (www.oaic.gov.au/).

When the Commissioner receives a complaint, in most cases it will be referred back to the church to give the congregation/BCSA Inc. the chance to resolve the complaint directly.

If the individual and the church cannot resolve the complaint between themselves, the Privacy Commissioner will become involved using letters and phone calls, or in some cases, face-to-face meetings. In the majority of cases the complaint is resolved this way.

As a last resort, the Commissioner can make a formal determination. If the church does not comply with the determination, either the Commissioner or the complainant can seek to have it enforced by the Federal Court.

A good way of both minimising complaints and keeping things simple is to only use and disclose information in the way that was described at the time of collection.

Appendices

Appendix 1 : Privacy Policy — Baptist Churches of South Australia Inc.

As from 1 March 2014 Baptist Churches of South Australia Inc (BCSA Inc.) made a commitment to adhere to the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act), and the Australian Privacy Principles that are contained in the Act, listed below:

APP 1 — Open and transparent management of personal information

APP 2 — Anonymity and pseudonymity

APP 3 — Collection of solicited personal information

APP 4 — Dealing with unsolicited personal information

APP 5 — Notification of the collection of personal information

APP 6 — Use or disclosure of personal information

APP 7 — Direct marketing

APP 8 — Cross-border disclosure of personal information

APP 9 — Adoption, use or disclosure of government related identifiers

APP 10 — Quality of personal information

APP 11 — Security of personal information

APP 12 — Access to personal information

APP 13 — Correction of personal information

Further information on the Principles is contained within the legislation, or from the Office of the Australian Information Commissioner (www.oaic.gov.au/).

The diverse range of activities of our churches also gives rise to numerous uses of personal information within the Church.

Personal information may be collected in a variety of ways including registration or enrolment forms, or in personal notes.

The information collected may include names, addresses, email addresses, telephone and fax numbers, medical details, family details (including spouses, children, guardians and parents' details), credit card and account numbers, and any notes taken for counselling purposes.

Churches only collect personal information which 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/disclosure is necessary to prevent threats to health, life or safety to any individual.

Personal information is not shared without the prior consent of the individual. It is not distributed to any organisation which is not associated with a Baptist Church.

In the Baptist Centre, all personal information is stored in secured cupboards, and where possible in secured premises. All personal data in an electronic form is stored in secured facilities. Churches should follow this model.

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

Individuals may access their personal data, which is held by BCSA Inc. or a church, by notifying BCSA Inc. or a church in writing of their request. BCSA Inc. or the church will acknowledge the request within 14 working days and arrange a time for viewing the data. Information which is out of date or incorrect, will be updated upon written request, or the applicant will be notified of the reason why the information will not be updated.

BCSA Inc. or a church may send out newsletters and other information including information from different associated bodies of BCSA Inc. from time to time. If an individual does not want to receive any of this type of information, they should notify BCSA Inc. or a church in writing of their desire not to receive any further information. Any correspondence of this nature should be addressed to the Privacy Information Contact Person.

Appendix 2 : Definitions

Anonymity	**Anonymity** means that an individual dealing with an APP entity cannot be identified and the APP entity does not collect personal information or identifiers.
Children and Youth	When a church seeks to collect information about an individual who is under 18 years, it must make every effort to ensure that the parent / guardian provides express consent to information being collected.
Church	The "**church**", as it relates to this policy, is the BCSA Inc. and its member churches or affiliate members.
Compliance	**Compliance** means doing what the Privacy Amendment Act 2000 and the Church's Privacy Policy says you should.
Consent	**Consent** means a voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the church. Consent is invalid if there is extreme pressure or coercion. Only a competent individual can give consent, although an organisation can ordinarily assume competency unless there is something to alert it otherwise.
Contractors	A **contractor** is an entity / organisation that enters into a relationship (contractual or otherwise) with the church where the entity / organisation: • supplies services to the church; or • supplies services to someone else on behalf of the church; and • the relationship involves the entity / organisation handling personal information in some way. This might be a Home Help agency, a health care service or a tradesman. When a congregation 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.
Disclosure	In general terms, the church discloses personal information when it releases information to others outside the part of the church that collected the information. It does not include giving individuals information about themselves.
Employee	An "**employee**" is a person paid to perform specific duties on behalf of the church. The application of this definition, as it relates to the Privacy Legislation, means a Pastor is to be treated as though they are an employee of the church.
Exemptions	Employee records are not covered under the Privacy Act, eg: employers have the right to collect personal and sensitive information about employees without their consent. This exemption does not include contractors, sub contractors and prospective employees. Prospective employees (applied for a job and or had a job interview) who do not enter into an employee relationship with the church have the same rights as any other individual with regard to making complaints under this Act.
Non-profit organisation	A **non-profit organisation** means an organisation that is a non-profit organisation, and engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes.

Appendix 2: *Definitions (contd)*

Opt out	An **opt out** statement offers an individual options concerning the continued use of their personal information. The following should be standard: • the chance to opt out is clearly stated and likely to be understood by the individual; • the individual is likely to be aware of the implications of opting out; • opting in or opting out is clearly shown and not bundled with other statements; • opting out involves little or no financial cost to, and little effort from, the individual; • the consequences of failing to opt out are harmless.
Personal information	**Personal information** is information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Personal information does not always need to include specifics such as an individual's name. It can be any information that can lead to the identification of an individual. ***Important:*** Information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy, and communications privacy.
Privacy information brochure	The **privacy information brochure** informs an individual how personal information collected about them is used and stored. It also lets the same individual know how to access and correct information held about them.
Privacy register	A **register** is a record of all matters relating to compliance with the Privacy Act in your church. It should include a copy of all audit sheets, a record of any disclosures, and any enquiries or complaints made to the Privacy Contact Person.
Pseudonym	A **pseudonym** is a name, term or descriptor that is different to an individual's actual name.
Sensitive Information	**Sensitive information** is information or an opinion about an individual's racial or ethnic origin; political opinion; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preference or practice; criminal record; that is also personal information; health information about an individual; or genetic information about an individual that is not otherwise health information
Third party	When the church obtains or discloses personal information to a person other than the individual concerned, that person is called a **third party**.
Use	In general terms, **use** refers to the handling of personal information within an organisation including the inclusion of information in a publication.
Volunteers	**Volunteers** have the same rights as any other private individual with regard to making complaints under this Act. Volunteers must also comply with the standards set out in this manual.

Appendix 3 : Audit Information Sheet

NOTE: There are no "right" answers. This form is designed to help you think through the issues and required actions. Please file this in your Privacy Register.

Name of activity: .....

question & example	answer	further action required	? task done
What type of information is collected? (*eg: contact details, family information, date of birth, medical details)* See also APP 1			
Does this information include "sensitive information?" *(eg: medical records, counselling notes)* See also APP 3			
Has consent been given to hold the information stated in the above answers? See also APP 1, 5			
Purpose of collection? *(eg: to ensure safety, pastoral care)* See also APP 6			
Is it relevant? Do we need to collect it? See also APP 3, 5		*Note: If you answer "no" you must delete this information.*	
Is the information we have correct? *(eg: don't know)* See also APP 10		*Note: If you answer "no" you must destroy or update your information.*	
How often is the information updated? *(eg: annually)* See also APP 10			
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.*	

Appendix 3: *Audit Information Sheet (contd)*

question & example	answer	further action required	? task done
How is it collected? (*eg: verbally or by written form)* See also APP 11			
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? See also APP 11		*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? See also APP 11		*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)* See also APP 11		*Note: If you answered "no" – you may need to rethink you distribution method.*	
What needs to be done next time we update this information? *(eg: training for personnel, distribute Privacy Information Brochure, add appropriate wording to registration forms, etc.)*			

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

.....	.....	.....
Privacy Information Contact Person's Signature	*Activity Co-ordinator's Signature*	*Date*

Appendix 4 : Audit Information Sheet Example

NOTE: This is an example. There are no "right" answers. This form is designed to help you think through the issues and required actions. Please file this in your Privacy Register.

Name of Activity: Awesome Baptist Church Youth Group

question & example	answer	further action required	? task done
What type of information is collected? (*eg: contact details, family information, date of birth, medical details)* See also APP 1	Name, address, phone numbers, email, birthday, school, parent's contact details, medical details, personal notes from youth worker, critical incident information forms, police check record releases.	Nil	✓
Does this information include "sensitive information?" *(eg: medical records, counselling notes)* See also APP 3	Yes – medical conditions, personal notes.	Nil	✓
Has consent been given to hold the information stated in the above answers? See also APP 1, 5	No	Seek written consent.	
Purpose of collection? *(eg: to ensure safety, pastoral care)* See also APP 6	General information – for communication. Medical safety. Personal notes – pastoral care.		
Is it relevant? **Do we need to collect it?** *(eg: Yes)* See also APP 3, 5	Yes, some of the personal notes made by youth worker may be questionable.	Check this matter with BCSA Inc. Privacy Officer. *Note: If you answer "no" you must delete this information.*	
Is the information we have correct? *(eg: don't know)* See also APP 10	Not sure how long since medical information was checked.	Check the date of collection and if unsure will confirm with each member. *Note: If you answer "no" you must destroy or update your information.*	
How often is the information updated? *(eg: annually)* See also APP 10	General – annually, with additions as new members join. Medical – not sure should be updated annually and when we hold camps.	Ensure Youth Worker implements this.	
Who is it collected from? *(eg: the individual or a third party?)*	Most comes from individuals. Some for word of mouth.	Check the word of mouth information to ensure relevance. Destroy information that is not necessary. *Note: If you answered "third party" consent should be sought from the individual.*	

Appendix 4: *Audit information Sheet Example (contd)*

question & example	answer	further action required	? task done
How is it collected? (*eg: verbally or by written form)* See also APP 11	Most verbally, some is gained from camp forms.		✓
Is the person who collects the information aware of the Privacy Act and its implications? *(eg: elder, minister, fellowship leader)*	Youth worker – sort of Other members of youth group – no	Need to train Youth worker and have a standard collection form. *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)*	Yes	Note we were planning to send stewardship invites to youth group members – need to include an "opt out" clause.	
Where is the information stored? **Is it secure?** See also APP 11	Youth worker's filing cabinet – no lock. Keeps in folder in back seat of his car. Church data base – at least 8 people know password. Minister's laptop – no password.	Arrange locks for filing cabinet. Arrange individual passwords. Arrange password security for minister's laptop. *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? See also APP 11	Yes. Changes above will fix current problems. Note: when we send group emails we must use BCC field to insert addresses.	Check that office administrator knows what BCC is (Blind Copy) *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)* See also APP 11	Yes – the youth group directory is given personally to each member by Youth Worker during a pastoral care visit.	*Note: If you answered "no" – you may need to rethink you distribution method.*	
What needs to be done next time we update this information? *(eg: training for personnel, distribute Privacy Information Brochure, add appropriate wording to registration forms, etc.)*	Include church's privacy statement on all material we use to collect information.	Include request for consent on all forms. Lapsed members need to be removed from general list. Check consent on Drivers and medical forms.	

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

Jac Doe	T Jones	21/03/2014
Privacy Information Contact Person's Signature	*Activity Co-ordinator's Signature*	*Date*

Baptist Churches
of South Australia

VISION:

to be a growing movement of healthy churches and ministries that are together in God's mission

OUR COMMITMENT TO THE PRIVACY POLICY

As from 14 March 2014, Baptist Churches of South Australia Inc. makes a commitment to adhere to the Privacy Act (2000) and Amendments, and the Australian Privacy Principles that are contained in the Act.

Baptist Churches
of South Australia

privacy

Baptist Churches of South Australia Inc.
Privacy Information Contact Person:

Glenn Dixon
Business & Systems Manager
Baptist Churches of South Australian Inc

35 King William Road, Unley SA 5061

PO Box 432, Unley SA 5061

p: +61 8 8357 1755

f: +61 8 8373 8000

info@sabaptist.asn.au

http://sabaptist.asn.au

… what the Privacy Act means to you …

THE LEGISLATION

An Act of Parliament 'Privacy Act 2000' was passed which sets out laws in relation to all personal information collected. This Act has been amended in 2013 with many significant changes effective in March 2014.

Baptist Churches of South Australia Inc. (Baptist Churches SA), including all member church congregations, need to comply with the law and the 13 Australian Privacy Principles that are contained in the Act and Amendments, listed below:

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information
- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Adoption, use or disclosure of government related identifiers
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

For more information about the Act and Australian Privacy Principles you can contact Baptist Churches SA Privacy Information Contact Person or visit the Office of the Australian Information Commissioner's website at www.oaic.gov.au

WHAT INFORMATION DO WE COLLECT?

Personal information may be collected in a variety of ways including registration or enrolment forms, or in personal notes.

The information collected may include names, addresses, email addresses, telephone and fax numbers, medical details, family details (including spouses, children, guardians' and parents' details), credit card and account numbers, and any notes taken for counselling purposes.

WHAT HAPPENS WITH YOUR INFORMATION?

Personal information is only collected if it is necessary for the mission and ministry of a Baptist Church.

Individuals will be notified of intended uses of personal information at the time of collection. Personal information is not shared without the prior consent of the individual.

Personal information will be securely stored and not disclosed to other parties without the individual's consent.

If you become aware that your congregation is holding personal information that is no longer required, incorrect, or out of date, please notify them so they can amend or destroy the information. This will be done in a secure and sensitive way.

Baptist Churches SA has formulated its own Privacy Policy and Privacy Manual that details its position on privacy. A copy is available on request.

YOUR RIGHTS

If you would like to view your personal information, or if you have any questions about the personal information the church has about you, you should contact your local congregational Privacy Information Contact person.

Church:

.....

Privacy Information Contact Person:

.....

Individuals may access data on themselves, which is held by Baptist Churches SA or a member church, by notifying Baptist Churches SA or the particular church in writing of their request. The request will be acknowledged within 14 working days and time will be arranged for viewing the data. Information which is out of date or incorrect, will be updated upon written request, or the applicant will be notified of the reason why the information will not be updated.

If your concern is not addressed to your satisfaction, then forward your concern to Baptist Churches SA Privacy Information Officer (see contact details on the reverse side of this brochure). If you still feel that your concerns have not been resolved, your complaint can be sent direct to the Office of the Australian Information Commissioner (an Australian Government Department) for their attention.

Baptist Churches of South Australia

Appendix 6 : Privacy Compliance Checklist

Privacy Compliance Checklist

Please tick the boxes below to confirm completion of the following tasks and file for your own records:

We have received and read our copy of the Privacy Manual.	☐
The congregation has been made aware of the Privacy Act.	☐
Copies of the Privacy Information Brochure have been made available to all members.	☐
Copies of the Privacy Information Brochure are easily available at our Church.	☐
We have conducted an audit of all the personal and sensitive information that we collect, hold, use, distribute and destroy.	☐
We have destroyed any information that we should not be keeping.	☐
Using the Privacy Manual as a guide, we have established a Privacy Register and taken other appropriate action as a result of the outcomes of our audit.	☐

Privacy Information Contact Person: _____

Signature: _____

Date: _____