

Contents

1.	Introduction	1
2.	Privacy Policy – Uniting Church, NSW Synod	2
3.	An overview of the Privacy Principles	3
3.1	The National Privacy Principle 1: Collection	4
3.2	The National Privacy Principle 2: Use and Disclosure	6
3.3	The National Privacy Principle 3: Data Quality	8
3.4	The National Privacy Principle 4: Data Security	9
3.5	The National Privacy Principle 5: Openness	11
3.6	The National Privacy Principle 6: Access and Correction	12
3.7	The National Privacy Principle 7: Identifiers	14
3.8	The National Privacy Principle 8: Anonymity	15
3.9	The National Privacy Principle 9: Transborder data flows	16
3.10	National Privacy Principle 10: Sensitive Information	17
4.	Conducting an audit	19
5.	Keeping a privacy register	20
6.	Check list for collection of information	21
7.	Enquiries and complaints	22
	Appendix 1 Definitions	23
	Appendix 2 National Privacy Principles	26
	Appendix 3 Audit Information Sheet Example	33

1. Introduction

Our congregations, presbyteries and Synod all 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 December 2000, the Federal Parliament passed the Privacy Amendment (Private Sector) Act 2000. This legislation amended the Privacy Act 1988, which had mainly covered public sector agencies. However, the Privacy Act now applies to most private sector organisations, and to the Uniting Church in Australia.

The Amendment 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.

The Act has ten National Privacy Principles (NPPs) which all have direct implications for the Church.

Further information about the Act and these principles is located at the Australian Privacy Commissioner's website at www.privacy.gov.au. Also refer to *Appendix 2*.

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 with this Act of Parliament.

In Section 2 you will see a copy of the Synod of NSW's Privacy Policy. This document applies to all of the church's inter-related councils: all our congregations, Presbyteries and the Synod.

The following pages (*Section 3*) introduce the National Privacy Principle's aim to highlight the key points for implementation of each principle.

The Privacy Contact Person's role

The key tasks of the Privacy Contact Person are:

1. Introduce the Privacy Act and its implications to your church (*Refer separate document titled NSW Synod Compliance with Privacy Legislation Kit sent out January 2002*)
2. Conduct an audit of how your church collects, collates, and uses personal information and identify areas that may need attention. (*Refer Section 4*)
3. Keep a Privacy Register (*Refer Section 5*)
4. Ensure all future collection of information adheres with the Privacy Act. (*Refer Section 6*)
5. Handle any enquiries or complaints. (*Refer Section 7*)

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

2. Privacy Policy – Uniting Church, NSW Synod

We are an innovative, growing church proclaiming Jesus Christ, empowered by the Spirit to transform God's world. The corporate trustee and legal entity of the Uniting Church in NSW (the "Church") is the Uniting Church in Australia Property Trust (NSW). The Church is made up of three inter-related councils: Congregations (local), Presbyteries (regional) and Synod (state).

The Church conducts religious, outreach and community activities including religious services, fellowship, weddings, funerals, baptisms, counselling and caring for members of the community.

As from 21 December 2001, the Uniting Church in NSW has made a commitment to adhere to the Privacy Act (2000), and the National Privacy Principles that are contained in the Act, listed below:

- Collection
- Use and disclosure
- Data quality
- Data security
- Openness
- Access and correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive Information

Further information on the principles are contained within the legislation, or from the Privacy Commissioner's Office.

The diverse range of activities of our Church 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 & parents' details), credit card and account numbers, and any notes taken for counselling purposes.

The Church only collects personal information which is necessary for its activities, and in particular only collects sensitive information where it is consented to by the individual, or their parent or guardian. Sensitive information is only shared where the Church has a belief that it's 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 the Uniting Church.

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.

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 data, which is held by the Church on themselves, by notifying the Church in writing of their request. 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.

The Church may send out newsletters and other information including information from different associated bodies of the Church from time to time. If an individual does not want to receive any of this type of information, they should notify their relevant congregation, presbytery, Synod or associated body of the Church in writing of their desire not to receive any further information.

For further information please contact the Synod Privacy Officer at GPO Box A2178 Sydney South NSW 1235. Phone number: (02) 8267 4200. Fax number: (02) 9264 4487. Email: bfp@nsw.uca.org.au

3. An overview of the Privacy Principles

In December 2000, the Federal Parliament passed the Privacy Amendment (Private Sector) Act 2000.

This legislation amended the Privacy Act 1988. The Amendment 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. The Act has ten National Privacy Principles (NPPs) under the following headings:

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.

2. Use and disclosure

A 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.

3. Data quality

The Church will 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

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

5. Openness

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

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).

7. Identifiers

The Church must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government agency (eg Tax file number, Medicare number).

8. Anonymity

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

9. Transborder data flows

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

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.

For further information please contact the Synod Privacy Officer at GPO Box A2178 Sydney South NSW 1235. Phone number: (02) 8267 4200. Fax number: (02) 9264 4487. Email: bfp@nsw.uca.org.au

3. 1 The National Privacy Principle 1: Collection

Summary: **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.**

Practical example:

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

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

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

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

What information can we collect?

- Information includes data collected on forms and informal notes taken by a Minister or church member.
- It also includes material that has been come across by accident or has not been asked for directly.
- You should only collect information that is relevant to the purpose for which it is being collected. Eg baptism, marriage, funeral, church camp, craft group, kids' club, community course.
- When personal information is obtained from a "third party" (*Refer Appendix 1: Definitions*), 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. This is called an "opt out" clause. (*Refer Appendix 1: Definitions*).

Collecting information on paper

- Written consent is the best consent.
- When information is collected, the following dot points below should be included on the form.
 - the identity of the Church 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 Section 3.2 Use and Disclosure Principle*)
 - any law that requires the particular information to be collected; and
 - the consequences (if any) for the individual if the information isn't provided.
- An alternative, is to use the standard Privacy Information Brochure (*copy enclosed in this kit*) and distribute it whenever you collect information.

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

- Church offices are usually staffed by a team of volunteers. It is important that they are familiar with the principles of the Privacy Act.
- Three simple things that you can do are:
 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 with 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?*”

Collecting information via a website

- If collected on-line, the website must include a clearly identified privacy statement. This must be prominent and users should not have to move through a number of pages to reach it.

Age of Consent

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

Contractors

- When 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. Note: contracts should be between The Uniting Church in Australia Property Trust (NSW) on behalf of “Congregation Name” and the contractor, as the former is the sole legal entity for the Church. (*Refer Appendix 1: Definitions*)

Practical example:

XYZ UCA decides to employ a stewardship consultant to assist in the biennial stewardship program. When the congregation enters into a contract with the consultant it should ensure that the agreement includes compliance with the Privacy Act.

This will ensure that the consultant won’t divulge personal information to any third party.

Record Keeping

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

3. 2 The National Privacy Principle 2: Use and Disclosure

Summary: **A 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.**

Practical Example:

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

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

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

An example of an “opt out clause” is:

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

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

There are a number of situations where it is appropriate to disclose information:

- When it is required by law or by 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); or
- 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 Section 3.10 Sensitive Information*).

Serious threats to life, health or safety

- Personal information may be given out where it is believed that there is a serious and imminent threat to the life or health of the person concerned or to a third party.
- Where personal information is disclosed in these circumstances, it is very important that a record of the disclosure be kept.

Practical example:

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

In this instance there are two types of threats: the first to Charlie himself and the other to the ambulance personnel and hospital staff. In this instance, it would be appropriate for the first aid volunteer to inform the ambulance staff about Charlie's condition so they can treat his cut both appropriately and safely. It is also very important that this information is given in a discrete manner.

Direct Mailing

- There may be occasions where the Church will use personal information for direct mailing purposes.
- Only non-sensitive personal information can be used for direct marketing.
- Recipients must be given the opportunity to "opt out". (*Refer Appendix 1: Definitions*)
- Information collected by the Church cannot be passed onto any other organisation so that the latter can use this 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 Synod's Privacy Officer should be contacted prior to making contact with a recognised 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.
- Where the use or disclosure of personal information is authorised by law, the Church can decide for itself whether to disclose the information or not.
- If a situation arises and the Privacy Contact Person is uncertain of what can be required or authorised by law, contact should be made with the Synod's Privacy Officer.

3.3 The National Privacy Principle 3: Data Quality

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

Practical Example:

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

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

To fully comply with this principle you should refer to the enclosed copy of the National Privacy Principles.

Correcting information

- 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 it is not accurate, complete and up-to-date.

3.4 The National Privacy Principle 4: Data Security

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

Practical Example:

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

To be compliant with the Privacy Act, this method of collection is no longer suitable. The ability of people to look at the names and contact details offers no security to the personal information of the latter party. Individual cards (eg pew cards or visitors forms) that can be handed to the door steward or into the offering bag are the best option. If, however, the visitor's book is only used for entry of names and a comment, then it is fine to continue with this practice provided that only names and comment details are sought and a sign clearly states public access eg "This book is on permanent display and security of personal information cannot be provided.

Practical Example:

Church directories should not be kept in the foyer for anyone to access. All surplus directories should be held in a secure location in the Church office, and made available upon request and in accordance with the policy of who should receive the directory.

To ensure security, each person should be told to keep the directory in a secure place when it is not being used.

Practical Example:

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

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

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

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

Storage and Back up

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

Destroying records

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

Sharing information

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

3.5 The National Privacy Principle 5: Openness

Summary: **The Church must have a document outlining its information handling practices and make this available to anyone who asks for it.**

Practical Example:

A copy of the Synod's Privacy Information Brochure is enclosed in this kit for your use.

You will need to add your local congregation's details before duplicating and distributing in your congregation.

If you need to tailor it to your own requirements (eg because you have a incorporated body that is associated with your church), you will need to refer to the check list below. Please lodge a copy with the Synod's Privacy Officer prior to distribution. The Privacy Officer can also give you a copy of the brochure template as a computer file.

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

- In most cases the enclosed Privacy Information Brochure will cover events and activities run by the church. However if you need to create your own document, the following must be included:
 - the Church's contact details;
 - the name,
 - street and postal addresses,
 - the main telephone and fax numbers and
 - appropriate e-mail addresses;
 - the kinds of personal information the Church holds;
 - the main purposes for which the Church holds the information;
 - how the information is collected;
 - how the Church stores or secures information (but it is not required to give specific details of security measures that would jeopardise the security of the personal information it holds.)
 - how the information will be used;
 - who the information will be disclosed to;
 - how to contact the Privacy Contact Person;
 - how the Church handles requests for access to personal information.

3. 6 The National Privacy Principle 6: Access and Correction

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

Practical Example:

Jenny's parents are divorced and share joint custody of Jenny. The divorce settlement, including custody arrangement, was a bitter process. As a consequence, Jenny's mother has told the congregation that she has a legally obtained 'no contact' order against Jenny's father for herself. Jenny's Day Camp registration has the contact details for both Jenny's mother and father. Jenny's father has made a request to access the personal details held about Jenny and himself.

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

Practical Example:

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

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

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

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

Checklist for requests to view personal information

- Prior to granting a person access to the information that the Church holds about them, the Privacy Contact Person should follow this basic checklist:
 1. Ask for the request in writing.
 2. Record the request in the Privacy Register. (*Refer Appendix 1: Definitions*)
 3. Determine if an exception should be used.
 - The only 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; or
 - the request is frivolous or vexatious.
 - If an exception is used, the Privacy Contact Person is required to give their reasons for denying access or refusing to correct personal information. However, this is not required where such a disclosure would prejudice an investigation against fraud or other unlawful activity.
 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 Section 3.3: Data Quality*)
 7. If the individual is not happy with the outcome, contact the Synod Privacy Officer. (*Refer Section 7: Enquiries and Complaints*).

3.7 The National Privacy Principle 7: Identifiers

Summary: **The Church must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government agency (eg Tax file number, Medicare number).**

Practical Example:

The presbytery has prepared a database of its members.

The presbytery can use its own ID (identification) codes to identify members of the presbytery if it wishes.

It cannot adopt a tax file or Medicare number as that ID code.

To fully comply with this principle you should refer to the enclosed copy of the National Privacy Principles.

3. 8 The National Privacy Principle 8: Anonymity

Summary: **Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do.**

Practical Example:

Anthony Smith has recently moved into the local community. On his first visit to the XYZ Uniting 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 initiative.

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

- 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.

3. 9 The National Privacy Principle 9: Transborder data flows

Summary: **The Church can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.**

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

- Before a Church sends any personal information internationally it must obtain the individual's consent and the individual's directions for secure transfer of the information.

3. 10 National Privacy Principle 10: Sensitive Information

Summary: **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 Example:

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.

Practical Example:

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

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

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

Practical Example:

Christine is part of XYZ Uniting Church congregation. Unfortunately, her uncle has just had a heart attack. Christine asks the person coordinating the prayer chain for people to pray for her uncle. Christine's uncle is an atheist. The uncle has no partner or carer.

The prayer wheel coordinator must first ask Christine if her uncle has given his consent for people on the prayer wheel to pray for him. Since the uncle is an atheist, and it is unlikely that he would have given his consent, news about his heart attack cannot be placed onto the prayer chain. If news about his heart attack was placed onto the prayer wheel and he found out about it, he would have cause to make a complaint against the congregation.

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

- "Sensitive information" is information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information.
- 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 a person cannot give consent due to some incapacity, consent can be obtained from the individual's guardian.
- If an individual does not give consent, the individual must be made aware of the consequences.

For further information please contact the Synod Privacy Officer at GPO Box A2178 Sydney South NSW 1235. Phone number: (02) 8267 4200. Fax number: (02) 9264 4487. Email: bfp@nsw.uca.org.au

- Sensitive information should not be collected on the off chance that it will be helpful to have it some time in the future.
- Sensitive information should be destroyed when no longer required.

Practical Example:

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

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

4. Conducting an audit

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

You will need to 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:

1. Make a list of the activities that your church runs that involve collecting information.
2. Photocopy an audit information sheet (*template enclosed*) for each activity.
3. In consultation with the co-ordinator/s for each activity, complete an Audit Information sheet. A sample of how to complete the form is enclosed. (*Refer Appendix 3*)
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.
5. File each Audit Information sheet in your Privacy Register. It is important that you keep this information so that you have a record of how you conducted your audit. (*Refer Section 5: Keeping a Privacy Register*)

5. Keeping a privacy register

- The Church's Privacy Contact Person should keep a register.
- A "register" is a record of all matters relating to compliance with the Privacy Act in your church. It should include:
 - A record of how the Privacy Act has been implemented in your church (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 Certificate;
 - A record of any enquiries or complaints made in relation to personal information.
 - A record of any disclosure of any personal information other than what consent has been gained for.
 - A record of all requests to "opt out."
- All records will be kept for a minimum of seven years unless directed by law or the Privacy Commissioner to do otherwise.

Other important information about church records

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

6. Check list 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.

1. Clearly state **who** is collecting the information. (Eg XYZ Uniting 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 Our 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 and to send you an annual birthday card.)
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 Contact Person.)
11. Include the name and contact details of the **Privacy Contact Person**. (Eg XYZ Uniting Church's Privacy Contact Person is MR C Member.)
12. If requesting **sensitive information**, you should state in what circumstances you will disclose it. (Eg If your form includes a statement like "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.)

7. 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 appropriate Privacy Contact Person.

For more information look at the “Checklist for requests to view personal information.” (*Refer Section 3.6 Access and Correction*).

The Privacy Contact Person does not need to contact the Synod office, unless they believe that the enquiry will lead to a complaint or dispute (see below).

Complaints

If there is a complaint or dispute, the complainant should detail their concerns in writing and forward them to the Synod Privacy Officer.

The Synod Privacy Officer will record the correspondence and, together with the local Privacy Contact Person, deal with it as necessary.

Alternatively, the individual can complain direct to the Commonwealth Government’s Privacy Commissioner.

When the Commissioner receives a complaint, in most cases it will be referred back to the Church to give the congregation / presbytery / Synod 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.

Appendix 1

Definitions

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 Uniting Church in Australia, NSW Synod. The Church is made up of three inter-related councils: Congregations (local), Presbyteries (regional) and Synod (state).

The corporate trustee and legal entity of the Uniting Church in NSW (the “Church”) is the Uniting Church in Australia Property Trust (NSW).

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 other) 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. Note: Contracts should be between The Uniting Church in Australia Property Trust (NSW.) on behalf of “Congregation Name” and the contractor, as the former is the sole legal entity for the Church.

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 Minister is 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.

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. It includes all personal information regardless of its source. Personal information only relates to a natural living person.

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.

Sensitive Information

“Sensitive information” is information about an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information.

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.

The Australian Privacy commissioner's website at www.privacy.gov.au contains helpful information about the Privacy Act.

This paper is extract from the "Guidelines to the National Privacy Principles (Sept 2001)" located at http://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:
 - (i) 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:
 - (i) 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:
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) 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;
- (iii) 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.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 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:
 - (i) 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:
 - (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - (ii) the disclosure is made for compassionate reasons; and
 - (c) the disclosure is not contrary to any wish:
 - (i) 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
 - (d) 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 unauthorised 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:
 - (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; 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 National Privacy Principles; 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 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 National Privacy Principles.

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:
 - (i) 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
 - (ii) 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 organisation 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.

Appendix 3 Audit Information Sheet Example

Name of activity: XYZ Uniting Church Youth Group

Question & Example	Answer	Further action required?	Task Done ?
<p>What type of information is collected?</p> <p><i>(Eg Contact details, family information, date of birth, medical details)</i></p> <p><i>Manual reference: 3.1</i></p>	<p>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.</p>	<p>Nil.</p>	<p>✓</p>
<p>Does this information include "sensitive information?"</p> <p><i>(Eg medical records, counselling notes)</i></p> <p><i>Manual reference: 3.10</i></p>	<p>Yes - medical conditions, personal notes.</p>	<p>Nil.</p>	<p>✓</p>
<p>Has consent been given to hold the information stated in the above answers?</p> <p><i>Manual reference: 3.1</i></p>	<p>No.</p>	<p>Seek written consent.</p>	
<p>Purpose of collection?</p> <p><i>(Eg To ensure safety, pastoral care)</i></p> <p><i>Manual reference: 3.1</i></p>	<p>General information - for communication. Medical - safety. Personal notes - pastoral care.</p>		
<p>Is it relevant? Do we need to collect it?</p> <p><i>(Eg? Yes.)</i></p> <p><i>Manual reference: 3.1; 3.2</i></p>	<p>Yes. Some of the personal notes made by youth worker may be questionable.</p>	<p>Check this matter with Synod Privacy Officer.</p> <p><i>Note: If you answer "No" you must delete this information.</i></p>	
<p>Is the information we have correct?</p> <p><i>(Eg Don't know)</i></p> <p><i>Manual reference: 3.3</i></p>	<p>Not sure how long since medical information was checked.</p>	<p>Check the date of collection and if unsure will confirm with each member.</p> <p><i>Note: If you answer "No" you must destroy or update your information.</i></p>	

Question & Example	Answer	Further action required?	Task Done ?
<p>How often is the information updated? (Eg annually)</p> <p>Manual reference: 3.3</p>	<p>General - annually, with additions as new members join.</p> <p>Medical - not sure. Should be updated annually and when we hold camps.</p>	<p>Ensure Youth Worker implements this.</p>	
<p>Who is it collected from? (Eg the individual or a third party?)</p> <p>Manual reference: 3.1</p>	<p>Most comes from individuals. Some from word of mouth.</p>	<p>Check the word of mouth information to ensure relevance. Destroy information that is not necessary.</p> <p>Note: If you answered "third party" consent should be sought from the individual.</p>	
<p>How is it collected? (Eg verbally or by form)</p> <p>Manual reference: 3.1; 3.3</p>	<p>Most verbally, some is gained from camp forms.</p>		✓
<p>Is the person who collects the information aware of the Privacy Act and its implications? (Eg Elder, minister, fellowship leader)</p> <p>Manual reference: 3</p>	<p>Youth worker - sort of Other members of youth group - no</p>	<p>Need to train Youth worker and have a standard collection form.</p> <p>Note: If you answered "no" - do you need to offer training?</p>	
<p>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)</p> <p>Manual reference: 3.2</p>	<p>Yes.</p>	<p>Note we were planning to send stewardship invites to youth group members - need to include an "opt out" clause.</p>	
<p>Where is the information stored? Is it secure? (Eg church office, foyer, individual's home)</p> <p>Manual reference: 3.4</p>	<p>Youth worker's filing cabinet - no lock. Keeps his folder in back seat of his car. Church data base - at least 8 people know password. Minister's Laptop - no password.</p>	<p>Arrange locks for filing cabinet. Arrange individual passwords. Arrange password security for minister's laptop.</p> <p>Note: If you answered "no" - you will need to make it secure.</p>	
<p>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)</p> <p>Manual reference: 3.4</p>	<p>Yes. Changes above will fix current problems. Note: When we send group emails we must use BCC field to insert addresses.</p>	<p>Check that Office Administrator knows what BCC is (Blind Copy)</p> <p>Note: If you answered "no" - you may need to limit access.</p>	

Question & Example	Answer	Further action required?	Task Done ?
<p>Is the distribution method of collected information appropriate?</p> <p><i>(Eg pigeon holes and foyer table are open to anyone to access)</i></p> <p><i>Manual reference: 3.4</i></p>	<p>Yes -The youth group directory is given personally to each member by Youth Worker during a pastoral care visit.</p>	<p><i>Note: If you answered "no" – you may need to rethink your distribution method.</i></p>	<p>✓</p>
<p>What needs to be done next time we update this information?</p> <p><i>(Eg distribute Privacy Information Brochure, add appropriate wording to registration forms)</i></p> <p><i>Manual reference: 3.5; 3.6; 6</i></p>	<p>Include church's privacy statement on all material we use to collect information.</p>	<p>Include request for consent on all forms. Lapsed members need to be removed from general list. Check consent on Drivers and medical forms.</p>	

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

C. Member
21/12/2001
 Privacy Contact Person's Signature

T Jones
 Activity Co-ordinator's Signature

Date