THE UNITING CHURCH IN AUSTRALIA
NSW SYNOD

COMPLIANCE WITH PRIVACY LEGISLATION KIT

UPDATED AS AT MAY 2002

Uniting Church in Australia – NSW Synod
Board of Finance & Property
Level 3, 222 Pitt Street, Sydney 2000
(PO Box A2178, Sydney South NSW 1235)
Ph: 82674300 Fax: 92644487

To Heads of all Uniting Church Organisations

THE UNITING CHURCH IN AUSTRALIA NSW SYNOD
THE NEW PRIVACY POLICY LEGISLATION

Dear Colleagues,

The Federal Government passed the *Privacy Amendment (Private Sector) Act No 155 of 2000* in December 2000, which comes into effect on 22 December 2001. This act is binding on all Australian businesses as well as the Non Profit Sector.

This Act amends the current and long standing Privacy Act 1988 and gives the Australian public greater comfort, assurance of their rights and recourse in the handling and storing of personal and/or sensitive information acquired from them by businesses and other Organisations, in their day to day business dealings. It also makes such organisations more accountable to the public.

The Uniting Church in Australia (UCA) is committed to be obedient to both its mission and the laws of Australia and therefore seeks to abide by this new act. As with GST wherein the UCA's approach to compliance was to register as a "GST Religious Group", The Synod likewise considers the Privacy Act as also being a "UCA Group" compliance issue or activity, both morally and legally.

Accordingly, all UCA Organisations must undertake an informal Privacy audit of its current operations to ensure they are compliant with the basic principles of this new legislation. These are called the "10 Privacy Principles". How this is done is explained in the Privacy Manual attached.

Unlike GST, there is nothing difficult or confusing about these 10 principles as they apply a common sense approach or "good practice" in the collection, use, release and storage of an individual's private and/or sensitive information and once realised and practiced, they should become part of an organisation's culture.

These new principles are operative from 21 December 2001. By and large, all that is required by an organisation is to take better care with private and/or sensitive information acquired from the public for their own operational needs. As a rule of thumb, whenever a question arises *is this private or sensitive information?* Or *how to I handle such information?* the first question to ask yourself is *does the getting of this information really meet the primary purpose of my organisation? ie, does my organisation really need this information to fulfill its spiritual, pastoral, social, educational and administrative functions?*

To assist and guide you in your understanding of these principles, we refer you to the article "Privacy in Australia" issued by the Office of the Federal Privacy Commissioner in September 2001, which can also be obtained from their web site **www.privacy.gov.au**. This is the Privacy Commissioner's own guidelines to explain what the act is and does, to be understood and followed by all organisations. The web site is updated regularly.

The attached policies and associated information should cover most if not all UCA Organisations and their systems in their compliance with the Privacy Act and their handling of private and/or sensitive information.

What you need to do

Please find attached 5 self explanatory documents, as part of the Synod's compliance with the Privacy Act. The actions, which we require, you to take are also detailed below. Please follow the instructions in the order indicated to gain a better appreciation and more effective implementation of the Privacy Policies in your organisation.

1. The UCA Privacy Policy

This is the NSW Synod's generic Privacy Policy or the "rules". The main document, as approved by the Council of Synod at its meeting on 22-23 November 2001. However, it is just the Policy and not the detailed procedures, which is contained in a 2nd document (Privacy Policy and Procedures – Insert into the Manual – see 2 below).

Please use this policy as your own. If you wish, you can insert your UCA organisation's name, name of the Privacy Officer and contact details. You can even transcribe it under your letterhead.

Place this policy in a prominent public place, at the entrance to your premises, in your Congregation's directory (at the front introductory page), when collecting private and/or sensitive information from your members, constituents, etc, in your correspondence. It is intended to be visible.

We stress that apart from this Policy, your organisation also needs to develop its own in house policy and procedures in the handling of private and/or sensitive information. The attached Manual (see 2 below) will assist you in this even though the examples used largely draw on information or examples from the life of Congregations.

2. Privacy Policy and Procedures Insert into the Manual

This is the detailed policy and procedures, which can be inserted into your manual. In due course it will be contained in the Synod's own Policy and Procedures Manual as a distinct chapter. This is the main document, which you and your privacy Officer will refer to most of the time. It will also be the document most regularly updated by Synod. The Manual can also be used as the basis of formulating your own "in house" Privacy Policy procedures (see step 4 below).

3.Privacy Officer Duties and Responsibilities (in each UCA organisation)

This is self explanatory and again, can be printed under your organisation's letterhead. Please assign the duties of Privacy Officer to someone that will understand what's required and will best suit your organisation's needs.

4. Privacy Officer Declaration for Compliance

Consistent with the duties of the Privacy officer, he or she needs to complete this declaration and return to the NSW Synod office as soon as possible.

The P.O. once nominated by each UCA Organisation is to carry out a self audit of all the possible privacy issues in your organisation, sign the declaration and return it to Synod (head) office (to the address on the letterhead). The feedback we seek is quite informal with an honest general description or answer against each question. You shouldn't need the services of a solicitor or professional to complete this declaration. One could even call this exercise a "stock take" of your current handling of Private or Sensitive information in your organization.

5. Frequently Asked Questions or FAQ's

Together with the Policy and Procedures Manual mentioned in 2 above, these questions should also be filed in the Manual as they form the basis of relevant information on situations that may arise that are common to most organisations. They can be considered "what if type" situations.

All these documents, 1 to 5 can also be located on the UCA Web site at www.uca.org.au

Action Steps:-

Step 1 The head of your organization unilaterally or in conference with your management or Committee of Management reads, appreciates and understands what the Privacy Policy is and how it could potentially impact on your organisation.

Step 2 Decide who is going to be your Organisation's Privacy Officer or P.O.

Step 3 Once appointed, ask your P.O. to read the attached and also gain an appreciation of the Privacy issues within your organization.

Step 4 Ask your P.O. to conduct your in house Privacy self audit, answer the questions in document 4 and sign the declaration. Return the results to us as soon as possible. If we have any questions or concerns we will contact you. This action will become an annual declaration.

Step 5 Your P. O. (solely or with the assistance of others) will need to develop your own organisation's unique Privacy Policy and Procedures. You can use The Manual insert (as mentioned in 2 above) as your guide, but at the end of the day, you alone know where you store all your information (computer, hard copy in a filing system/cabinet, off site, in the CEO's or Ministers manse, etc) and how to document their use and maintenance. These procedures do not need to be long, just a page or two, using the Synod's Policy document as the background paper.

Step 6 Report the results of your self audit to your Organisation's Management Committee, Council or Board as an example of good Governance.

How are the attached forms to be used?

The attached forms are to be used by each UCA Organisation in the way prescribed in the aforementioned steps. The rule of thumb is one set of these forms are to be issued to and completed by each UCA organisation with its own ABN entity.

However, unlike the use of ABN's, if you feel that there are other sub entities or organisations, committees or other structures which would require their own identity and hence their own Privacy Policy guidelines, Procedures and Privacy Officer, please copy the attached and give it to the respective head of this other organisation(s), remembering that they in turn will require their own Privacy Officer, Operating procedures and Self Audit and Declaration.

The Synod, however, feels that for better or more effective compliance and central control of the task at hand, it is better that there be fewer Privacy Officers and recommend one only in each organisation (ie, one for each grouped organisation), coordinating all of the various functions of sub entities by the main organisation, even if these sub entities are geographically scattered. This is better than delegating the responsibilities to lots of people or lots of privacy Officers.

The Synod will not be keeping a central register of all UCA Organisations who have individually complied with the Privacy Legislation and sees this as a self audit exercise. However, it will have some record by annually seeking from every UCA Organisation, similar to the annual Insurance declaration, an assurance that the Privacy Principles are also being adhered to and effectively maintained. The Insurance declaration could therefore be amended in the future to include this additional compliance requirement.

One could therefore surmise that the person signing the annual Insurance declaration could very well be the Privacy Officer also, although this is purely an internal organisation decision.

Do you require further assistance?

Immediate – Help Desk

If you have followed the necessary steps mentioned above and find you still need more assistance or information that is not covered by the instructions contained in this kit, please contact the following persons:-

For enquiries dealing with Congregations, Presbyteries and Missions- contact the Board of Finance and Property at any of the contact details below:-

Kegan Kashian (02) 8267 4341 or kegank@nsw.uca.org.au

Natalie Waters (02) 8267 4410 or nataliew@nsw.uca.org.au

For UC Records & Historical Society – Daryl Lightfoot on 9683 3147 (Mon/Tues only) or PO Box 2395 North Parramatta 1750

You can also look up our web site on www.uca.org.au (Click on 'Synods', then Click on 'Synod of NSW' and look for and Click on the words 'Privacy Legislation'.

Longer Term

The Board of Finance and property will be visiting all Presbyteries in 2002 to conduct seminars on matters contained within the new Synod Policy and Procedures Manual. Naturally, this will include Privacy as topic.

1. Other special or unique enquiries

The Synod through the expertise of Dibbs Barker and Gosling (DBG), commissioned to assist in the development of the Synod's Privacy Policies, have sought widespread input from the various Synod organisations and programmes in compiling the attached policies and feels satisfied that they have legally covered all practices by the Church and provide adequate coverage to all Privacy issues.

For those unique Church organisations that have lodged separate submission detailing their unique problems or areas of concern, DBG have dealt with these separately and devised more specific instructions and policies to guide their situations. There have not been many of these, for example, The Uniting Church Trust Association, which acts as a non-bank financial institution. Financial Institutions under the Privacy Act require more stringent observance of privacy policies in the handling of their customer base (example depositors and borrowers).

If you feel you have a unique or special situation that requires legal opinion or special line of enquiry, please contact Dibbs, Barker and Gosling on (02) 8233 9500 and speak to either Tony Spajic or Peter Ludemann.

Conclusion

Remember, as with GST, the compliance with the Privacy Policy has been instigated by the Federal Government. All corporately responsible organisations need to abide by this new legislation.

They are not a Synod initiative, but the Synod needs to obey the Government laws, particularly as the UCA, as with other denominations, by their very nature of activities deal in personal and sensitive information on a daily basis and thus need to take extra care and duty of responsibility in the handling of such information.

Don't Panic!

Unlike Y2K or GST, there is no general alarm or panic associated with the introduction of this new legislation, hence the low key media approach so far, however, there is also no room for complacency, as in time the general public will become aware of their rights and your obligations and may approach you to test how their private and/or sensitive information is being used and stored by your organisation.

The attached polices will cover most if not all UCA Organisations privacy issues and subject to your Privacy Officer's responses, we feel there will be very few if any problem areas, which cannot be resolved by the adoption of the attached guidelines.

What if you already have a Privacy Policy in place? (called second generation policy)

To ensure that the Church across its many organisations has a consistent or uniform Privacy Policy, reflective of its Mission, we ask that if you have put in place your own Privacy Policy before now, that you now send us a copy for authorisation by the Synod's Privacy Officer.

If you wish to dispense with your "second generation" policy and adopt the attached official Synod policy, this is quite acceptable and no further action is needed by you.

Our best wishes to you in this task and thank you for your continued cooperation.

Kegan Kashian
Finance Manager
Uniting Resources
NSW Synod

THE UNITING CHURCH IN AUSTRALIA NSW SYNOD

PRIVACY LEGISLATION

THE UCA – NSW SYNOD PRIVACY POLICY

NOVEMBER 2001

THE UNITING CHURCH IN AUSTRALIA
THE PRIVACY POLICY OF (Your Organisation's name)

This policy has been adopted by the Organisation in order to comply with the requirements of the Privacy Amendment (Private Sector) Act No 155 of 2000.The policy should be read together with the National Privacy Principles (NPPs) set out in the Privacy Act. A copy of the NPPs is attached.

1. In this policy, a reference to

- "Church" means The Uniting Church in Australia;
- "Organisation" means the organisation of the Church which has adopted this policy.

2. The Organisation will comply with the NPPs. If there is any inconsistency between this policy and the NPPs, then the NPPs prevail.

3. Subject to paragraph 4, the Organisation will only use personal information for the primary purpose for which it is collected. In most cases, the purpose will relate to the spiritual, pastoral, social educational and administrative functions of the Organisation.

4. Those functions include maintaining personal information for the purpose of analysing the role of the Church in society and recording the family histories of its members. The information may be disclosed to scholars studying the Church and to relatives of Church members.

5. The Organisation will only use personal information about an individual for a secondary purpose (i.e. something beyond the scope of the primary purpose) if that individual has consented or the use is otherwise permitted by the NPPs.

6. The Organisation will take reasonable steps to keep personal information secure and will, subject to the NPPs, comply with any request from a person to correct or remove his or her information. The Organisation will appoint a Privacy Officer who will be responsible for storing, correcting and giving people access to personal information collected about them. The Organisation may charge fees for access to personal information.

7. Personal information collected by the Organisation may be sensitive information for the purpose of the NPPs (e.g. information about a person's religious beliefs). As a non-profit organisation, the Organisation is permitted to collect sensitive information without a person's express consent. However, the Organisation will endeavour to seek consent from a person if sensitive information is sought for something other than the primary functions of the Organisation described in paragraph 3.

8. The operating procedures (whether or not they are formalised in a manual) of the Organisation will comply with this policy and the NPPs.

9. The Organisation will appoint a Privacy Officer who will be empowered to receive and deal with any complaint that the Organisation has not complied with this policy or the NPP's.

If you have any questions about this Policy, please contact the Organisation's Privacy Officer.

The Privacy Officer for this organisation is ----------who can be contacted on ----------.

Privacy Officer
date

THE UNITING CHURCH IN AUSTRALIA
NSW SYNOD

PRIVACY LEGISLATION

MANUAL INSERT OF
POLICY AND PROCEDURES

NOVEMBER 2001

Uniting Church in Australia NSW Synod
Privacy Procedures and Instructions
to be inserted in Policy Manual

Introduction

The guidelines set out below will assist you in implementing and answering enquires about the Uniting Church's privacy policy and the National Privacy Principles (NPPs) under the Privacy Act.

The policy and NPPs govern the way in which the Uniting Church deals with "personal information" and "sensitive information". Copies of the policy and the NPPs are attached.

This guide is general in nature and does not touch upon every aspect of policy and the NPPs. In due course you will need to develop a brief procedures document unique to your organisation, explaining how private and sensitive information needs to be handled and stored. This guide can be used in developing your own procedures.

The new principles operate from 21 December 2001. They require organisations to take better care of private or sensitive information acquired for their own operational needs. As a rule of thumb, if information sought by your organisation may be personal or sensitive; the first question to ask should be "*Is the collection of this information really necessary for the functions or activities of my organisation?* That is, *does my organisation really need this information to fulfil its spiritual, pastoral, social, educational and administrative functions?"* If the answer is "*No*", then the solution is not to seek such information from your constituents.

The Act covers personal information contained or stored on paper, digital, video, audio or any other form or means of storage.
The Act also covers information held anywhere in your organisation, even if you didn't request it but you or your staff happen to keep it.

As well, the Act covers any private and/or sensitive information you outsource, so be sure any contracts you have with outsourcing organisations in turn have proper procedures in place to observe the privacy legislation. All contracts and agreements you may have (including those entered into without the knowledge of Synod's Property Trust) should be looked at to check if they should include privacy compliance provisions.

Background

The Federal Government passed the *Privacy Amendment (Private Sector) Act No 155 of 2000* in December 2000. It comes into effect on 21 December 2001. The Act is binding on many Australian businesses as well as the non profit sector.
This Act amends the current and long standing Privacy Act 1988 and gives the Australian public greater comfort and assurance of their rights in the handling and storing of personal and/or sensitive information acquired from them by businesses and other organisations,. It also makes such organisations more accountable to the public.
The Uniting Church in Australia (UCA) is committed to being obedient to both its mission and the laws of Australia and therefore seeks to abide by the new Act. As with GST where the UCA's approach was to register as a "GST Religious Group", the Synod likewise considers the Privacy Act as also being a "UCA Group" compliance issue or activity, both morally and legally.

Accordingly, each UCA Organisation should undertake a privacy self-audit of its current operations to ensure they are compliant with the NPPs. How this is done is explained below.

To assist and guide you in your understanding of the NPPs, we refer you to the article "Privacy in Australia" issued by the Office of the Federal Privacy Commissioner and also refer you to their web site www.privacy.gov.au for further information as it is updated. This manual will cover most if not all UCA Organisations privacy issues and questions and subject to your Privacy officer's responses, we feel there will be very few if any problem areas, which cannot be resolved by the adoption of these guidelines.

What is your entity structure ?

One set of forms attached, as part of this kit is to be issued to and used by each UCA organisation, which has its own ABN. However, unlike the use of ABN's, if you feel that there are other sub entities or organisations, committees or other structures which have their own identity and hence require their own Privacy procedures and Privacy Officer, please copy the attached and give it to the respective head of that other organisation(s), remembering that they in turn will require their own Self Audit and Declaration.

For better and more effective compliance and central control of the task at hand, the Synod would prefer that there not be too many Privacy Officers and recommend one only in each organisation (ie, one for each grouped organisation), coordinating all the sub entities.

The Synod will keep a record of compliance by its organisations by annually seeking from them a Privacy declaration, similar to the current annual Insurance declaration. The Insurance declaration may be amended to include this additional compliance requirement. The person signing the annual Insurance declaration could be the Privacy Officer also, although we leave this decision to you.

What if you already have a Privacy Policy in place?

To ensure that the Church across its many organisations has a consistent privacy policy, we ask that if you have already put in place your own Privacy Policy, you send us a copy of it for authorisation by the Synod.

If you wish to dispense with your own policy and adopt the policy approved by the Synod, you need not submit your earlier policy.

Guidelines (with examples drawn from the activities of Congregations)

Preface

In your dealings with your congregation members, residents of our aged care centres, staff, community services staff, the families they work with, children in our child care centres and their parents, and any member of the public with whom you have any dealings, you need to be very clear about your intentions as to the use of their private and sensitive information. The attached policies guide you as to what you need to do and they include such simple things as stating in writing in your correspondence, signs around the counter, in roll books, registers, in fact any public record, what exactly is your Organisation's Privacy Policy. Some examples of suggested phrases are shown below.

Employee Records

Staff or employee records (staff files, payroll records) are excluded from the privacy legislation. However, rules governing the handling, storing and disposal of such records still require appropriate security measures. Furthermore, they are not to be used outside their normal intended purpose. In storing such records, you need a well secured environment, for example, locked filing cabinets and passwords on computer files to name two. As a further example, the CV of a successful applicant to a vacant position once filled should be stored securely as part of the staff file, however, the CV's of the unsuccessful applicants must be disposed of properly and not kept if there is no purpose for keeping them.

Personal information

Personal information is information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. The information or opinion need not be true or recorded in material form. If the identity of an individual is not apparent or cannot be reasonably ascertained from the information, then the information is not personal information and is not relevant for our purposes.

Personal information may include opinions, reports or records, whether true or not, relating to a client, member of a Congregation, resident, volunteer or visitor under your care.

By way of example, the following information about an individual is not personal information, if this information is alone collected:

Male, 210cm tall, brown eyes

The following information is personal information:

[name or address], male, 210cm tall, brown eyes

Some personal information is "**sensitive information**" (see below).

What personal information does your Congregation collect and for what purpose?

Information collected by Congregations includes members' names, addresses, ages, birth dates, occupations, phone numbers, email addresses, etc. The information is often used to compile a Congregation directory or roll, rosters (morning tea duty, cleaning church, bible reading, welcoming committee, deliveries) etc. It could also be contained in minutes, newsletters, correspondence, emails, notices on boards, in fact any means of communication or record keeping.

Congregations often keep such personal information on data bases (manual and/or computerised) for use in directories or to be used and/or shared by key church members or amongst the general Church membership for the Congregation's spiritual, pastoral, social, educational and administrative functions. The privacy legislation allows this where its use is for these functions or activities.

Sensitive information

Sensitive information is information or an opinion 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 Congregation would have to tread more carefully when determining why sensitive information needs to be collected and stored, to ensure that it serves the functions and activities as mentioned above, in relation to Personal information.

Collection of personal information

The Church collects personal information about individuals in order to fulfill the spiritual, pastoral, social, educational and administrative functions of the Church.

The Church will also, depending upon the circumstances, collect personal information for other reasons. For instance, the Church's financial investment arm (UCA Investment Services) or UCTA will collect personal information for the purposes of considering and approving applications for commercial loans or opening deposit accounts.

Wherever a UCA organization collects personal information, it must be able to justify the collection on the grounds that the collection is related to its functions or activities.

Whenever the Church collects personal information (or sensitive information), the Church must provide the following information to the person from whom the information is collected:

- how to contact the Church (and even the name and contact details of the UCA Organisation's Privacy Officer);
- the purposes for which the information is collected;
- the organisations (or types of organisations) to which the organisation usually discloses information of that kind;
- any law that requires the information to be collected; and
- the main consequences, if any, for the individual if all or part of the information is not provided.

The following statement should be made at the point of collection of personal information. Such a statement can be accompanied by your (Synod's) "Privacy Policy" as sent to you in this kit.

*"**Privacy**: The Uniting Church (add your organisation's name – "the XYZ Congregation or Centre") requires the information provided by you in this form in order to [identify purposes of collecting personal information]. If you do not provide all the relevant information, then [identify consequences, if any, of not providing the personal information]. Please also note that the Uniting Church may provide your personal information to a third party [identify third party] in order to [identify purpose of disclosure]. Generally speaking, you can access your personal information by contacting [identify contact – the head of the organisation or Privacy officer].*

If you wish to access your information or have any queries in relation to the manner in which the Uniting Church handles your personal information, please visit our privacy policy on our web site (optional) or contact our Privacy Officer on [telephone number and e-mail]."

This information is known as 'NPP 1.3 information'.

We suggest notices of this kind be clearly displayed at the point of collection of personal and/or sensitive information. For instance, with regard to Congregations:-

- at the beginning of your members directory,
- at the start or somewhere noticeable in your visitors book
- at the start or by way of a menu display on your web site
- any other place where personal or sensitive information is collected

Release of personal information to other organisations

You may be queried on how another organisation separate from the Church came to hold a person's personal information.

The Church's privacy policy on this is that where the person has consented to the disclosure, then the disclosure may be made.

However, in some instances consent may not be needed. For example, if the disclosure is related to the original purpose of collection, that is, to fulfill the spiritual, pastoral, social, educational or administrative functions of the Church and the person concerned would reasonably expect the information to be disclosed to the other organisation, consent is not required.

If a person indicates a desire for their personal information to remain within the Church then that request should be considered and, where appropriate, the consequences of that choice explained to the person.

Sometimes it might not be reasonable to provide information to another organisation. A good example would be if a UCA childcare centre gave the names and contact details of the parents or guardians of children attending the centre to a Congregation for the purpose of the Congregation gaining membership or participation in church services. Such a parent or guardian may query how the Congregation acquired such contact details, supplied originally to the Childcare centre as private information for entirely different purposes.

It would be quite acceptable for the Director of the child care centre to invite the parents or guardians of the children at the centre, to attend the Congregation's services, particularly family services.

Personal or sensitive information cannot generally be released to other Organisations without the knowledge or consent of the person concerned. There are exceptions, for instance where the use or disclosure is required or authorised by or under law.

Members' personal or sensitive information cannot be supplied to other organisations for the purposes of marketing or soliciting such members to acquire or purchase a particular product or service (eg, to mailing houses, other Charities or call centres) unless marketing is the primary purpose of collection and you have informed the individual at the point of collection that the information will be used for those purposes or you have obtained the consent of the person to use the information for those purposes.

Use of personal information for a secondary purpose

The Church may use and disclose personal information for a secondary purpose (any purpose other than the primary purpose of collection) if the use is related to the original purpose of collection, that is, to fulfill the spiritual, pastoral, social, educational or administrative functions of the Church and the person concerned would reasonably expect the information to be used for the secondary purpose.

The Church can seek consent to use personal information for a secondary purpose. If a person indicates a desire for their personal information to be used only for the primary purpose of collection then that request should be considered and, where appropriate, the consequences of that choice explained to the person.

For example, if the Congregation in its pastoral role discovered that one of its members (through voluntary admission) had a particular gambling, drinking or drug related problem and needed help and the Congregation (its Minister or other authorised member) sought the permission of the individual to refer his or her problems to a third party for what is a secondary purpose, e.g to seek professional outside help, then this is legally allowable.

Alternatively the Congregation could simply give the affected individual contact details of outside professional help.

Collection of sensitive information

The Church's policy is that where necessary, it will seek the consent of the person concerned before it collects, uses or discloses such information. The consent to collect use and disclose sensitive information should be in writing. A declaration to the following effect should be permanently displayed on the means of collection (eg letter, form, web site):

"In providing the sensitive information sought in this form (or letter, web site etc) you consent to the use and disclosure of that information by the Church for [identify purposes and disclosures]. If you have any queries about the use and disclosure of the sensitive information provided by you please contact the Privacy Officer.

However, because the Church is a non-profit organisation it is permitted to collect sensitive information without consent where:

- the sensitive information relates to members of the Church or to a person who has regular contact with the Church in connection with Church activities and
- at or before the time the Church collects the sensitive information, the Church undertakes to the person concerned not to disclose the sensitive information without the person's consent.

There are legitimate reasons for the collection of sensitive information by a particular Congregation. For example, health information (information about allergies and medication needed for a particular illness) concerning a child may be needed if the child is attending a Church camp or youth event. In such instances you should seek such health information from the child's parent or guardian.

The Congregation would need to clearly state why it needs to collect such sensitive information, as detailed above.

Great care needs to be taken in the collecting, maintaining, storing, using, disclosing and disposing of such sensitive information.

Use of sensitive information for a secondary purpose

The use and disclosure of sensitive information for a secondary purpose is permitted where:

- the secondary purpose is *directly* related to the primary purpose of collection and
- the individual would reasonably expect the Church to use the sensitive information for the secondary purpose.

We refer to point 5 above.

How personal and sensitive information is secured

The Church's policy is to take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. Each agency of the Church will need to implement procedures to achieve these aims. Such procedures will range from keeping information locked away in secure storage to the use of encryption technology for information transmitted over the Internet. A basic precaution is to permit access to information only to those who have a 'need to know'.

The Church will also destroy or de-identify (ie remove a person's name and other identifying characteristics) from a record of personal and sensitive information it no longer uses or needs.

The destruction of personal and sensitive information should also take place in a secure manner. For instance, it may not be sufficient to destroy such information through normal waste disposal. Instead, such material should be shredded.

Access to personal and sensitive information

Subject to the conditions set out in the NPPs, the Church will permit a person to access and, where appropriate, correct their personal or sensitive information. The Church will correct personal information where that information is established to be inaccurate, incomplete or out of date. If agreement cannot be reached as to whether information is inaccurate, incomplete or out of date, then the Church will upon request take reasonable steps to associate with the information a statement claiming that the information is inaccurate, incomplete or out of date.

In most instances, the Church will not charge a person for access to, or the correction of, their personal or sensitive information. Sometimes a fee will be charged. For example, access to archival material for research purposes is subject to the payment of a research fee. The Church will not impose a fee that is excessive or charge for lodging a request for access.

If a person wishes to access their personal information or correct it, they should contact the Privacy Officer.

Accurate recording of personal and sensitive information

The Church's policy is to maintain accurate, complete and up-to-date personal information. It does this by verifying the integrity of information at the point of collection (eg production of drivers licence where necessary) and by updating information at regular intervals or where appropriate.

A person wishing to update their personal information should contact the Privacy Officer.

Other privacy issues

- The Uniting Church does not, for the purposes of the Privacy Act, transfer personal information overseas.

- Wherever lawful and practicable an individual may deal anonymously with the Uniting Church.

- **Identifiers** - The Uniting Church does not use official identifiers (e.g. tax file numbers) to identify individuals. An individual's name or Australian Business Number is not an identifier for the purposes of the Privacy Act and hence may be used to identify individuals.

- **Minutes of meetings** – Most UCA Congregations make decisions through a Committee, Board or other meeting process, eg, Elders Council, Church Council, Finance Committee, Property Committee, or various Sub Committee or groups.

One member of the relevant group (usually the Secretary) takes minutes of the meetings. All care must be observed that, when minutes contain personal or sensitive information of any individual or groups of individuals, the procedures referred to above are followed.

Where possible, minutes should not include personal or sensitive information. Equally, great care must be observed in the circulation, storing and archiving of minutes and minute books. The Congregation should also be very clear and document what happens with minutes (who stores them, how long they are kept, how are they disposed of, etc). If you have a policy of pinning minutes on to a notice board, ensure that they do not contain personal/sensitive information.

- **Correspondence – letters, emails, notices, newsletters, etc.** Again, all care must be taken when acquiring, using, sharing, storing and disposing of such information if it contains personal or sensitive information.

- **Private diary notes made by Ministers –** same rules apply as above

Conclusion

The next step is for your Organisation to use the input gained from this manual to put together your own in house, "day to day" operating procedures, so that you and your key members are aware:-

- of the contents of this manual and associated documents contained in this kit

- who is authorised to acquire personal and sensitive information

- what happens to the personal and sensitive information (usage, circulation, storage)

- what security or control measures you have in place to protect personal and sensitive information

- how long should you keep personal and sensitive information

- where personal and sensitive information is archived (assume Church Records and Historical Society)

- if not stored or archived, how you dispose of such information

- who has the responsibility of keeping such personal/sensitive information up to date (additions, alterations and deletions from records)

Kegan Kashian
Synod Privacy Officer
29 November 2001

THE UNITING CHURCH IN AUSTRALIA NSW SYNOD

PRIVACY LEGISLATION

COMPLIANCE WITH LEGISLATION BY THE UCA ORGANISATION'S PRIVACY OFFICER

NOVEMBER 2001

UNITING CHURCH IN AUSTRALIA (NSW SYNOD)
PRIVACY COMPLIANCE DECLARATION

The Privacy Officer
……..……..
(UCA Church Organisation)

Dear Privacy Officer

Congratulations on the appointment to the very important role as your organisation's Privacy Officer.
So we can audit compliance with the National Privacy Principles, we need to work out what sort of personal information your organisation collects, holds, uses and discloses. "Personal Information" means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. The information or opinion need not be true or recorded in material form. If the identity of an individual is not apparent or cannot be reasonably ascertained from the information, then the information is not personal information and is not relevant for our purposes.

By way of example, the following information about an individual is not personal information, if this information is alone collected:

Male, 210cm tall, brown eyes

The following information is personal information:

[name or address], male, 210cm tall, brown eyes

Some personal information is "sensitive information". This is information or an opinion about an individual's racial or ethnic origin, political opinions, memberships of a political association, sexual preferences or practices, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, criminal record or health information.

Please return your response to the attached questionnaire as soon as possible. It will help us gauge the level of compliance with the National Privacy Principles.

Yours sincerely

Kegan Kashian
Synod Privacy Officer
NSW Synod
29 November 2001

PRIVACY COMPLIANCE DECLARATION

FROM……
(Name of your Organisation)

Item 1: We collect the following types of personal information and/or sensitive information:
Response:
Item 2: We collect this information through the following means: (Eg. standard forms, surveys, questionnaires.)
Response:
Item 3: We store this information in the following forms: (Eg. in a single database, filing cabinet or spread across the organisation in a number of sites.)
Response:
Item 4: The following authorised persons have access to personal information and/or sensitive information:
Response:
Item 5: The following measures are in place to protect personal information and/or sensitive information from unauthorised access:
Response:
Item 6: We collect personal information and/or sensitive information for the following primary reason:
Response:

Item 7: We collect personal information and/or sensitive information for the following secondary reasons:
Response:
Item 8: We disclose personal information and/or sensitive information to the following organisations for the reasons stated, all of whom are external to [the Church or the organisation]:
Response:
Item 9: We contract out the following functions or activities involving personal information and/or sensitive information and take the following measures to protect the confidentiality of this information:
Response:
Item 10: When we collect personal information and/or sensitive information we inform individuals of: 1. Who we are and how to contact us, 2. The intended uses and disclosures of this information, 3. How to access this information, and 4. the main consequences if the information is not provided in the following manner:
Response:
Item 11: We keep personal information and/or sensitive information accurate, complete and up-to-date in the following ways:
Response:

Item 12: We permit individuals access to their personal information and, where appropriate, to correct the information, in the following ways:
Response:
Item 13: Individuals have the option of dealing with us anonymously in the following instances:
Response:
Item 14: When we collect sensitive information from an individual who is not a member of the Church, we obtain consent to collect and use the information in the following manner:
Response:
Item 15: When we collect sensitive information from an active member of the Church we assure the member that we will not disclose that information without consent in the following manner:
Response:

Completed and signed by:

……
Privacy Officer

Dated:

If there is insufficient space above please attach additional comments to the back of this declaration.

Thank you for completing this declaration.

Send it to:-
The Privacy Officer
NSW Synod
PO Box A2178
Sydney South NSW 1235

THE UNITING CHURCH IN AUSTRALIA NSW SYNOD

PRIVACY LEGISLATION

FREQUENTLY ASKED QUESTIONS OR FAQ'S

NOVEMBER 2001

Uniting Church Privacy Policy
Frequently Asked Questions or FAQs

2. What you must do when you collect personal information

Personal information is information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

When the Uniting Church ("the Church") collects personal information from an individual it must take reasonable steps at that time (or as soon as is practicable thereafter) to provide the individual with the following information:

(a) how to contact the Church;

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

(c) the purposes for which the information is collected by the Church;

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

(e) any law which requires the particular information to be collected by the Church; and

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

3. What you must do when you collect sensitive information

Sensitive information is information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- health information;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- sexual preferences or practices;
- membership of a trade union;
- criminal record; and
- health information about an individual.

The information referred to in paragraphs 1(a)-(f) should also be provided to the individual at the point of collection of sensitive information or as soon as practicable thereafter.

4. After the personal or sensitive information is collected it should be securely stored

Personal or sensitive information should be securely stored by those persons who:

- have authority or control over the record in which the personal information appears;
- use the personal information on a regular basis;
- are responsible for its storage.

Similarly, access to personal and sensitive information should be restricted to those persons who:

- have authority or control over the record in which the personal information appears;
- use or disclose the personal information on a regular basis; or
- are responsible for the storage of the personal information.

5. What do you do if a request is made to access or correct personal or sensitive information?

- You should ensure that the person who has made the request is in fact the subject of the personal information;
- You should consult National Privacy Principle 6 and determine whether or not an exception to access and correction applies. You can obtain the National Privacy Principles from the Privacy Officer;
- If it is established that the personal information is not accurate, complete and up-to-date the Church must take reasonable steps to ensure that the personal information is made accurate, complete and up-to-date;
- If the Church and the individual are unable to agree on whether the personal information is accurate, complete and up-to-date then the Church must take reasonable steps to associate a statement with the personal information to the effect that the personal information is not accurate; and
- Any charges for access must not be excessive. The Church cannot charge a person for merely making an application for access.

6. Why does the Church collect personal information?

The Church collects personal information about individuals in order to fulfil its spiritual, pastoral, social, educational and administrative functions.

For example, dates of birth and marriage are collected by the Church for pastoral and administrative functions.

Such information may also be provided to Church archivists and used to document the social and cultural history of the Church. Personal information may also be disclosed to researchers and historians of the Church.

7. Does the Church use personal information for secondary purposes?

The Church's policy is to confine its use of personal information to the primary purpose for which it was collected. This means the Church will primarily use personal information in order to fulfil its spiritual, pastoral, social, educational and administrative functions (the primary purposes).

The Church may use personal information for a secondary purpose (any purpose other than a primary purpose) if it has obtained the consent of the person concerned.

The Church will use personal information for a secondary purpose where consent is not required by the NPPs. Consent is not needed where the secondary use is related to the original purpose of collection, that is, to fulfil the spiritual, pastoral, social, and administrative functions of the Church and the person concerned would reasonably expect the information to be used for the secondary purpose.

8. Does the Church release personal information to other organisations/persons?

The Church's policy is to confine its disclosure of personal information to the primary purpose for which it was collected. This means the Church will primarily disclose personal information in order to fulfil its spiritual, pastoral, social, educational and administrative functions (the primary purposes).

The Church may disclose personal information for a secondary purpose (any purpose other than a primary purpose) if it has obtained the consent of the person concerned.

The Church will disclose personal information for a secondary purpose where consent is not required by the NPPs. Consent is not needed where the disclosure is related to the original purpose of collection, that is, to fulfil the spiritual, pastoral, social, educational and administrative functions of the Church and the person concerned would reasonably expect the information to be disclosed for the secondary purpose.

The Church does not provide or sell personal information for the purposes of direct marketing. However, if the Church uses or wishes to use the personal information it collects for the purpose of direct marketing, it may be appropriate to obtain consent or make it clear at the point of collection that the information is sought for that purpose.

9. Why does the Church collect sensitive information?

The Church collects sensitive information about individuals in order to fulfil its spiritual, pastoral, social, educational and administrative functions.

The Church's policy is that where necessary, it will seek the consent of the person concerned before it collects, uses or discloses such information. The consent to collect use and disclose sensitive information should be in writing.

However, because the Church is a non-profit organisation it is permitted to collect sensitive information without consent where:

- the sensitive information relates to members of the Church or to a person who has regular contact with the Church in connection with Church activities and
- at or before the time the Church collects the sensitive information, the Church undertakes to the person concerned not to disclose the sensitive information without the person's consent.

10. Does the Church use sensitive information for a secondary purpose?

The Church's policy is to confine its use of sensitive information to the primary purpose for which it was collected. This means the Church will primarily use sensitive information in order to fulfil its spiritual, pastoral, social, educational and administrative functions (the primary purposes).

The Church may use sensitive information for a secondary purpose (any purpose other than a primary purpose) if it has obtained the consent of the person concerned.

Consent to use sensitive information for a secondary purpose is not required where:

- the secondary purpose is *directly* related to the primary purpose of collection and
- the individual would reasonably expect the Church to use the sensitive information for the secondary purpose.

11. Does the Church release sensitive information to other organisations/persons?

The Church's policy is to confine its disclosure of sensitive information to the primary purpose for which it was collected. This means the Church will primarily disclose sensitive information in order to fulfil its spiritual, pastoral, social, educational and administrative functions (the primary purposes).

The Church may disclose sensitive information for a secondary purpose (any purpose other than a primary purpose) if it has obtained the consent of the person concerned.

However, the Church will disclose sensitive information for a secondary purpose where consent is not required by the NPPs. Consent is not needed where the disclosure is:

- *directly* related to the original purpose of collection and
- the person concerned would reasonably expect the information to be disclosed for the secondary purpose.

Privacy Officer
NSW Synod
29 November 2001

THE UNITING CHURCH IN AUSTRALIA
NSW SYNOD

PRIVACY LEGISLATION

PRIVACY OFFICER
STATEMENT OF DUTIES
AND RESPONSIBILITIES

NOVEMBER 2001

UNITING CHURCH IN AUSTRALIA (NSW SYNOD)
PRIVACY OFFICER OF CHURCH ORGANISATION
STATEMENT OF DUTIES & RESPONSIBILITIES

As the Privacy Officer of your organisation within the Church you will be expected to understand and apply the National Privacy Principles under the Privacy Act (NPPs) and *your organisation's / the Synod's general* privacy policy. Copies of the NPPs and the policy are attached as part of this mail out.

If you require any assistance in interpreting the NPPs or the policy please contact the relevant Synod Privacy Officer for your organisation group, depending on your organisation's line of enquiry. These contact names and phone numbers are contained in the "Privacy Policy and Procedures Manual" also attached.

As the Privacy Officer of your Organisation, on a day-to-day basis, you will be expected to:

- understand the types of personal information and sensitive information collected by your organisation;
- advise your colleagues on how to collect, use and disclose personal information and sensitive information;
- ensure that your organisation complies with the NPPs and the privacy policy;
- complete annually a declaration concerning your organisation's compliance with the NPPs;
- advise Church members and, where appropriate, members of the public on how your organisation collects, uses and discloses personal information and sensitive information;
- assist individuals to access, update and correct personal information and sensitive information held by your organisation; and
- deal with complaints, if any arise, from members of the public as it affects your organisation, for breach of privacy by your organisation.

The Privacy Officer can be any senior staff member or worker who is familiar with the organisation. In a Congregation, this would ideally be the Secretary. However, it could equally be the Treasurer/Accountant or Chairperson. Each organisation is unique and needs to appoint a Privacy Officer suitable to its structure or situation.

Title and Name of Privacy Officer of Organisation

Position Title
29 November 2001