
POLICY TITLE:	PRIVACY POLICY
POLICY NUMBER:	IT-BP-PR1
CATEGORY:	BOARD POLICY
CLASSIFICATION:	INFORMATION & TECHNOLOGY
STATUS:	ADOPTED, AUGUST 2008

This policy document may not be current as SUA regularly reviews and updates its policies. The latest version can be found in the Policies section of SUA's website or obtained from the National office.

1. PURPOSE

The Policy aims to ensure that information held by Scripture Union Australia (SUA) about people is handled responsibly. It also gives people some control over the way information about them is handled by SUA.

Specifically, this Policy determines how SUA will deal with private and personal information of individuals who participate in, support the activities of, or deal with Scripture Union Australia Inc, in order to respect those persons legal and reasonable rights to privacy.

As a networking service arm working on behalf of the Australian States and Territories, SUA deals with the transfer of information between movements as core business. Special care therefore needs to be taken to ensure that information is correctly handled, stored, transmitted, protected and disposed of when no longer required.

This policy adopts and reflects the tenor of Privacy Act 1988 (Cth) as amended by the Privacy Amendment (Private Sector) Act 2000 which applies to private sector 'organisations' including non-profit organisations with an annual turnover of more than \$3 million. It adopts the 10 National Privacy Principles stated within the Act and contextualises them for SUA.

2. SCOPE

This policy pertains to all SUA operations and applies to all SUA employees and volunteers. It is not binding on other SU state and territory movements, however it is expected that those movements would have in place similar policies in response to jurisdictional privacy regulations.

The material scope of this policy is drawn from that of the Privacy Act 1988 (Cth), the salient points of which are:

- It does not apply to employee records of an individual if an act or practice directly relates to a current or former employment relationship between the employer and the individual;
- It covers personal information and has special protection for personal information that is also sensitive information;
- It only applies to information that is recorded in some form. That recording need not involve paper, it can include data in an electronic record.

It is worth noting that each Australian State and Territory has differing regulatory regimes with respect to Privacy. Whilst these all at present have roots in the Commonwealth platform and NPPs, SUA must exercise due caution when dealing across State and Territory boundaries in case of compliance differences.

It is also notable that the Australian Law Review Commission has in August 2008, delivered recommendations following from an extensive review of Privacy legislation in Australia and this is likely to lead to significant changes to the Privacy Act 1988 (Cth), over the coming year or so (<http://www.austlii.edu.au/au/other/alrc/publications/reports/108/>).

3. POLICY STATEMENT

SUA will develop and maintain protocols for protecting the private and personal information of individuals, consistent with the Privacy Act 1988 (Cth) as amended by the Privacy Amendment (Private Sector) Act 2000.

In doing so, SUA:

- Adopts the ten National Privacy Principles (NPP's) that are set out within the Privacy Act 1988 (Cth);
- Notes that at this point in time, SUA does not fall within the scope of the Act;
- Explicitly chooses NOT to formally “opt in” to coverage by the Act as allowed for within it.

4. PRINCIPLES

This policy adopts the 10 National Privacy Principles, which in summary are:

NPP 1 - Collection

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

NPP 2 - Use and Disclosure

An organisation should only use or disclose information for the purpose it was collected 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,

or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

NPP 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.

NPP 4 - Data Security

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

NPP 5 - Openness

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

NPP 6 - Access and Correction

Generally speaking, an organisation must give an individual access to personal information it holds about the individual on request.

NPP 7 - Identifiers

Generally speaking, an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth Government agency.

NPP 8 - Anonymity

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

NPP 9 - Transborder Data Flows

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

NPP 10 - Sensitive information

An organisation must not collect sensitive information unless the individual has consented, it is required by law or in other special specified circumstances, for example, relating to health services provision and individual or public health safety.

This summary is based on information obtained from the Office of the Federal Privacy Commissioner's website at www.privacy.gov.au

Contextual notes for the application of each Principle to SUA are included in Appendix A.

5. DEFINITIONS

Collection

An organisation collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when an organisation keeps personal information it has come across by accident or has not asked for.

Consent

Consent means 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 organisation. Consent is invalid if there is extreme pressure or coercion.

Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise. Competence means that individuals are capable of understanding issues, forming views based on reasoned judgments and communicating their decisions. The general law about competence and incapacity will apply to the issue of consent.

Personal information

Information or an opinion 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 relates to a natural living person. A natural person is a human being rather than, for example, a company, which may in some circumstances be recognised as a legal 'person' under the law.

Sensitive information

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.

Use

In general terms, use of personal information refers to the handling of personal information within an organisation including 'the inclusion of information in a publication.

6. RESPONSIBILITY

This policy is to be implemented by all SUA volunteers and staff.

7. REFERENCES

Policy Owner:	Chair of Board of SUA
Contact Officer:	CEO of SUA
Endorsed by:	Nil
Final Approval:	Board of SUA
Date to be revised:	Full review every 2 years after approval – Aug 2010
Related Policies:	Nil

Related Publications: Nil
Reference documents: Privacy Act 1988 (Cth)
Office of the Privacy Commissioner
<http://www.privacy.gov.au/>

8. VERSION CONTROL & HISTORY

PR1 Privacy Policy, approved December 2002
IT-BP-PR1 Version Adopted August 2008

APPENDIX A – POLICY TEMPLATE

(NPP 1) Collection of Information

SUA collects information from, amongst others:

- Active, past and potential volunteers;
- Potential and prospective employees;
- Donors, sponsors, supporters, and staff;
- Other movements of SU International and local;
- Other organisations with which SUA is a partner;
- Resource customers – wholesale, and retail.

The type of personal information collected, used, and stored by SUA regarding individuals may typically include the following:

- Names;
- Addresses (including email addresses);
- Telephone and facsimile numbers;
- Date of Birth;
- Gender;
- Nationality;
- Education and training;
- Details about next of kin including spouse, parent's and children's names;
- Health information;
- Occupation and employment history;
- Membership and professional associations;
- Religious or philosophical beliefs;
- Criminal history;
- History of Involvement in SU activities;
- Financial details including bank account access authorities
- Purchasing history;
- Photographic images, video clips and sound recordings.
- Credit card details and signatures.

SUA will only collect personal information necessary for one or more of its legitimate functions or activities.

SUA will collect the personal information only by lawful and fair means and not in an unreasonably intrusive way. Whenever SUA collects personal information about an individual, SUA will take reasonable steps to ensure that the individual is aware of:

- Who SUA is;
- The fact that he or she is able to gain access to all personal information held about them by SUA;
- The purpose for which the information is collected;
- The consequences for the individual if the information is not provided;
- Any organisations to which SUA usually discloses the information being sought;

- Any laws that require SUA to collect the information.

Where possible, SUA will collect personal information about an individual only from that individual. If, however, this information is collected from someone else, SUA will act reasonably to ensure the individual is or has been made aware of the matters listed above.

The purposes for which SUA uses personal information it collects include::

- To consider volunteer applications and record participation in SUA activities;
- To consider potential employee's applications for employment by SUA;
- To administer donations and sponsorship of SUA activities;
- To provide services to wholesale and retail customers;
- To administer contractors of the organisation;
- For promotion, marketing, and retail initiatives such as events, and fund raising.

In relation to "Online" or internet based Privacy:

- SU may collect personal information through the SUA website and the website may also collect information which may or may not be personal information;
- For each website visitor, the server may automatically recognise and store:
 - The visitor's address (eg the domain name or internet protocol address);
 - The type of internet browser used by the visitor;
 - Address of the site which "referred" the visitor;
 - Clickstream data.
- In addition, the website may use "cookies" to track website usage and statistics. Visitors may set their browsers to refuse cookies, which may limit access to some functions. Tracking will be conducted in such a way to ensure the anonymity of visitors;
- The SUA website may contain links to third party websites. SUA is not responsible for the privacy practices of these sites.

(NPP 2) Use and Disclosure

SUA will not use or disclose personal information about an individual other than for its primary purposes, except where:

- The individual has consented to the use or disclosure; or
- SUA has gathered the information on behalf a state movement in which case only nominated staff of the movement will have access; or
- A mailing house has been contracted to pack and despatch SUA materials; or
- SUA has reason to suspect that unlawful activity has been, 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
- SUA reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or to public health or safety.

Where the personal information is not sensitive information, SUA may use the information for its own direct marketing purposes including where:

- It is impractical for SUA to seek the individual's consent before that use;
- The individual has not made a request not to receive direct marketing.

SUA will provide individuals with options not to receive direct marketing material by:

- Including in each direct marketing communication the option of informing SUA if they do not wish to receive further direct marketing communications;
- Including in each direct marketing communication SUA's business address and telephone number and, if the communication is made by fax or email or other electronic means, a number or address at which SU can be directly contacted electronically.

(NPP 3) Data Quality

SUA will take reasonable steps to make sure that the personal information it collects, uses, or discloses is accurate, complete and up to date and will regularly provide opportunities to individuals to revise and update their personal information.

(NPP 4) Data Security

SUA will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. This includes physical security, computer and network security and personnel security.

These steps will generally include:

- Hardcopy personal records will be kept in locked storage;
- Access to personal records is restricted to the National Director, or to others expressly authorised by or in the company of the National Director;
- Electronic personal records will be secured by password;
- Personal records will not be left on unattended computer screens or in view of non-authorised persons;
- Personal information will not be disclosed except in the normal course of operation.
- Where the records are collected on behalf of a state or territory movement, SUA accepts no responsibility for the misuse of that information within that movement.

SUA will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed. In instances where information is archived, SU will take reasonable steps to ensure the security of this information.

(NPP 5) Openness

SUA will publish a Privacy Statement on its Internet site. That statement will outline this policy, provide contact details for a nominated SUA Privacy Officer, and describe a complaint handling process. The Privacy Officer will be made available

to investigate and resolve the complaint internally through mediation with the individual.

(NPP 6) Access and Correction

As a general rule, SUA will, on request by an individual, provide him or her with access to his or her personal information. SUA may, however, choose not to provide individuals with access to such information.

This will include cases where:

- Providing access would have an unreasonable impact on the privacy of other individual's; or
- The request for access is frivolous or vexatious; or
- The information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings; or
- Providing access would reveal the intentions of SUA in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Providing access would be unlawful; or
- Providing access would be likely to prejudice an investigation of possible unlawful activity.

If a person can show that SUA holds information that is incorrect, incomplete or out of date, SUA will take reasonable steps to correct the information.

There will be no fee charged for a *request* for access or correction, and the fee for *supplying* access will not exceed the cost to SUA of providing that access.

(NPP 7) Identifiers

SUA will not adopt an identifier in respect of personal information that is the same as an identifier used by the Commonwealth Government.

(NPP 8) Anonymity

Wherever it is lawful and practical, SUA will allow individuals the option of not identifying themselves when entering into transactions with it.

(NPP 9) Transborder data flows

SUA will only transfer personal information about an individual to a third party movement in specified circumstances. This would include:

- Where the individual consents to the transfer; or
- Where SUA, in gathering and transmitting of the information, was acting as an agent of that movement; or
- Where SUA has taken reasonable steps to ensure that the information which has been transferred will not be held, used or disclosed by the recipient of the information inconsistently with the NPPs.

(NPP 10) Sensitive Information

Some information SUA collects or holds may be “sensitive” information. This may include information or an opinion about an individual's:

- Religious beliefs, affiliations or philosophical beliefs;
- Health;
- Criminal record;
- Financial details including bank account access authorities;
- Credit card details and signatures.

SUA will only collect sensitive information when the collection:

- Is undertaken with the person's consent; or
- Is required by law; or
- Is necessary to prevent or lessen a serious and imminent threat to the life or health of the person; or
- Is necessary in respect of a legal claim; or
- Is necessary for the fulfilment of a particular service provided by SUA.