

SUEU Policy on Handling and Use of Private Information

Dated 8th June 2009

Preamble

The Commonwealth Government's [Privacy Act](#) (1988) covers the operation of private sector organisations, however Small Businesses (those with an annual turnover of \$3million or less in the previous financial year) are exempt from the legislation. As a result, the SUEU are currently exempt from the legislation.

However, the Sydney University Evangelical Union (SUEU) intends, as far as possible, to comply with the legislation. Accordingly the following is the SUEU policy on the handling of all private and personal information.

Since the SUEU is a registered club with the University of Sydney Union Clubs & Societies Program (USU), and is affiliated with the Australian Fellowship of Evangelical Students (AFES), this Privacy Policy has taken into consideration the SUEU's relationships with these two entities. Of further consideration is that the SUEU also approves staff to work alongside the SUEU from the EU Graduates Fund. There is an ongoing and close relationship between these two entities, and some sharing of information is therefore appropriate.

Introduction

Your privacy is important to us. The following statement outlines the SUEU policy on how we manage the personal information we hold about our members and associates. It is SUEU policy to respect the confidentiality of information and the privacy of individuals.

The SUEU Privacy Policy will be reviewed from time to time to take account of new laws, technologies, and changes to SUEU operations and practices. This is done in order to ensure the Privacy Policy remains appropriate to the changing social and legal environment. Any information we hold will be governed by the most current SUEU Privacy Policy Statement.

We are committed to being open about how we use personal information. Where our documents ask for personal information, we will generally state the purpose for its use and to whom it may be disclosed.

Purpose of Collecting Information

The SUEU are committed to helping those whom they come in contact with understand the Christian gospel, as described in the Bible. This commitment for understanding will take place in the context of personal relationships and may extend over many years. We would hope that where possible a continuing association between our members and associates takes place even after they have left the University context. As such, personal information about people who are involved with and attend the activities of the SUEU is collected primarily for the purpose of maintaining contact with people in order to minister to them effectively.

What Information is Held?

Because of the nature of the ministries provided, we ask for a range of personal information. The type of information we may collect can include (but is not limited to):

- name
- address
- contact details
- course and year of study
- and the type, name and date of meeting attended.

From time to time we may also collect images of you during the course of SUEU ministry activities. This includes but is not limited to photographs, video footage or audio recordings.

We obtain most of this information directly from our members or associates through response slips and from maintaining records of information provided in the course of ongoing ministry. We will endeavour to seek consent wherever possible. This information may be collected at public meetings, smaller group meetings, from responses to our communication to you, or from other public sources.

Given that we are dealing with large numbers of members and associates and as we need to identify you within our record keeping, we may seek to collect a piece of personal information from you that is in some way unique to yourself. Under the Privacy Principles (as listed in the following attachment) this will not be any Commonwealth Government identifiers (eg Medicare number). We may seek to ask you for only the day and month of your birth. This will help us keep your records unique from other members, especially if we have members with similar names, and no current address information.

If an individual makes a financial payment to the SUEU then other information such as bank account details and credit card information may need to be collected. We will always endeavor to provide a mechanism whereby the individual will be able to give anonymously. However in some cases if payment information is not provided, then such a payment may not be able to be correctly carried out. We will store this financial information for only as long as is necessary for us process the desired transaction.

At some of our activities we may ask for sensitive information to be collected. For more details see the section entitled 'Sensitive Information is subject to greater restrictions'.

How do we use this information and to whom may we disclose it?

From time to time we may send you information about SUEU activities that we think may be useful to you, but we remain conscious of the need to respect your privacy. As such these communications will typically be infrequent. You may also request that your name be removed from SUEU mailing lists.

The personal information you give to us may be made available, where necessary, to the SUEU executive, volunteer leaders, EU Graduates Fund pastoral staff, trainee staff, and employees at the discretion of the SUEU Executive. This is in keeping with our stated purpose for the collection of the information.

We will not disclose information regarding you without your prior consent. We may offer to give your information to other Christian ministry organizations. If you consent to this offer then we will keep a record of your intention as well as pass on the information you have indicated to the nominated organization/s. Such an offer might be made if you were moving to another campus, another university, graduating, or wished to join another Christian group at the University of Sydney.

If you apply for formal membership to SUEU, your access card details and student ID will be passed onto the University of Sydney Union for the purpose of their membership records. This will be explained explicitly on any membership form. This is a condition of our affiliation with the USU Clubs and Societies Program.

The contact information that you give us may be used to contact you to provide you with information regarding SUEU activities, events and ministry opportunities. This includes but is not limited to letters, phone calls, emails and SMS text messaging. As technology develops we will develop opportunities for you to 'opt-out' of various modes of communication at your choice.

We may employ third party providers to utilise technology not currently available to the SUEU itself. We would do this in accordance with our stated purpose for collecting information. This could require us to provide the third party with some of your personal information, such as a mobile phone number. Before doing this, the SUEU Executive will satisfy themselves that the third party provider's privacy policy is consistent with the SUEU Privacy Policy. An example of this third party situation is SMS Messaging. If we were to use a third party SMS-provider, we will post the details of the service that we are using on our website. If you do not consent to your details being passed on to a third party provider, or wish to opt out of the service, you may do so at any time by contacting us using the details below

The EU has a strong online community presence. While you may wish to engage with the EU Community online, no personal information will be revealed in an official capacity, unless you specifically agree to it, and then only on a case by case basis. Photos, video, sound and text recorded of you at events or conferences may be replicated and used for advertising and review, both in videos and presentations offline and online. Examples of websites which present online content at the time of writing include the EU Website, Facebook, YouTube and Twitter. If you object to the use of your comments, photos, or /videos in any EU Media please make this clear to the Privacy Officer

If the SUEU wished to distribute a list of the names of current members to members and associates of the SUEU, we would produce a separate application form to collect information for such a list. This form will state:

- The nature of the information being collected

- The purpose of the collection
- The nature of the distribution of the list
- That filling out the form is voluntary.

Sensitive Information is Subject to Greater Restrictions

Sensitive information relates to a person's:

- Racial or ethnic origin
- Membership of political bodies, religions or trade unions
- Sexual preferences or activities
- Criminal record
- State of health
- Medical history

Some personal information we hold is 'sensitive'. We will not be seeking to collect information regarding membership of political bodies, trade unions, or information regarding sexual preferences or activities. As part of our Privacy Policy we hereby undertake to collect only the following information that is deemed to be 'sensitive information';

Racial or ethnic origin.

Information collected may include country of origin or ethnicity.

Membership of political bodies, religions or trade unions

The form of information collected will be restricted to the denomination, location and name of the church that a person attends.

State of health, medical history

On occasions we may seek to collect this information, when we consider that the collection is necessary to prevent or lessen a serious and imminent threat to life or health of an individual. This is most likely to be in the context of conferences the SUEU may run in conjunction with Evangelical Union Christian Conferences (EUCC).

In such a case, a separate form will be provided for the collection of such information. This form will state:

- The nature of the sensitive information being collected.
- The purpose for collecting the information.
- How the information will be stored and used.
- How long the information will be stored for.

- An avenue for people to not have their information collected – and the consequences of us not being able to collect such information.

Criminal record

During the course of collecting and processing information for the Working with Children Check (under the *Child Protection Act*) it may be made apparent that an individual has a criminal record. This information will be held in accordance with the guidelines established in the *Child Protection Act*. Under circumstances other than the collection of information pertaining to the Child protection Act sensitive information regarding criminal records will not be collected.

Management of Personal Information

The SUEU seeks to train its students, EU Graduate Fund pastoral staff, trainee staff and employees who handle personal information to respect the confidentiality of members' information and the privacy of individuals. The SUEU considers that breaches of your privacy are very serious matters. We have appointed a Privacy Officer to ensure that the management of your personal information is in accordance with this statement.

Safeguarding the privacy of your information is important to us, whether you interact with us personally, by phone, mail, over the internet, or other electronic media. We hold personal information in a combination of secure computer storage facilities and paper based files and other records, and take steps to protect the personal information we hold from misuse, loss, unauthorized access, modification or disclosure.

We may need to maintain records for a significant period of time. However, when we consider information is no longer needed, we will remove any details that will identify you or we will securely destroy the records regarding you.

Because of the unique working relationship between the SUEU and the EU Graduates Fund, the SUEU will pass details of its members to the EU Graduates Fund upon a student graduating from their degree at University, and from them ceasing to be an active on-campus member of the SUEU. EU Graduates Fund use of this information will be governed by their Privacy Policy.

The SUEU endeavours to ensure that the personal information it holds is accurate and up-to-date. We realize that this information changes frequently with changes of address and other personal circumstances. We can update your information over the telephone. In the near future we hope to implement a system which allows members and associates to update their own information.

Request/s to View and Make Amendments

Any individual can at any time view or amend the information that is held on them by the SUEU. Requests to view or amend personal information can be made by contacting our office;

Ph: c/- (02) 9351 7496

Email: secretary@sueu.org.au

EU Secretary (Privacy Officer)

SUEU

c/- Holme Building

Sydney University NSW

6 March, 2009

Summary of Privacy Principles

(for more information see www.privacy.gov.au for more information about the Privacy Act)

1. Collection

1.1 An organisation should generally collect only the personal information it needs for its legitimate functions and activities. The organisation should collect the information in a fair and lawful way.

1.2 Where reasonably practicable an organisation should collect personal information directly from the individual. The organisation should usually take reasonable steps, when collecting information, to ensure that the individual knows why the information is being collected, who the information will be given to and how the information will be used or disclosed, as well as how to contact the organisation and that the individual may access the information. This is the case whether the organisation collects personal information from the individual or from someone else.

1.3 An organisation should usually ensure it has the consent of the individual to collect sensitive information. Sensitive information is information or an opinion about a person's -

- religious or philosophical beliefs and affiliations,
- racial or ethnic origin,
- political opinions or membership of a political association,
- membership of professional or trade associations or a trade union,
- sexual preferences or practices,
- criminal record, or
- health.

2. Use and disclosure

An organisation should usually only use or disclose personal information for -

- the primary purpose for which it was collected,
- a related purpose which the individual would reasonably expect, or
- with consent.

3. Data quality

An organisation should take reasonable steps to introduce systems to ensure that personal information it holds is accurate, current and complete.

4. Data security

4.1 An organisation should implement measures to protect personal information from misuse, loss and unauthorised access, changes or disclosure.

4.2 An organisation should usually destroy or permanently de-identify personal information when the organisation no longer needs it.

5. Openness

An organisation should be open about how it manages personal information. If asked, an organisation should provide information about its approach to privacy.

6. Accessing and correcting personal information

6.1 Usually, when asked, an organisation should give an individual access to their personal information unless there is a reason why the organisation cannot do so. An organisation may deny a request for access if it reasonably believes any of the following circumstances apply -

- it would pose a serious and imminent threat to the life or health of any person, or if health information, would pose a serious threat to the life or health of any person,
- the privacy of others would be unreasonably affected,
- the request is frivolous or vexatious,
- the information relates to existing or anticipated legal proceedings with the person who is the subject of the information and would not be accessible in those proceedings,
- providing access would prejudice negotiations with the person who is the subject of the information by revealing the organisation's intentions regarding those negotiations,
- providing access would be unlawful or denying access is required or authorised by law,
- providing access would be likely to prejudice an investigation of possible unlawful activity,
- providing access would be likely to prejudice law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body,
- an enforcement body performing a lawful security function requests denial of access to protect national security, and
- where evaluative information generated by the organisation in making a commercially sensitive decision would be revealed by providing access. In this situation the organisation may provide an explanation for the commercially sensitive decision instead.

6.2 The organisation should usually correct personal information if the individual to whom it relates can establish that the information is not accurate, current and complete.

6.3 An organisation should not impose an excessive charge for access by an individual to their personal information.

7. Identifiers

An organisation should generally not adopt, use or disclose Commonwealth government identifiers unless specifically permitted to do so. Identifiers include tax file numbers or social security numbers, but not an ABN.

8. Anonymity

If reasonably possible, an organisation should give others the option of dealing with it anonymously.

9. Transborder data flows

An organisation should generally obtain consent to transfer information overseas unless otherwise permitted to do so.

10. Sensitive information

An organisation should generally obtain consent to collect sensitive information unless otherwise permitted to do so.