

## **Katoomba Christian Convention Privacy Policy**

**Katoomba Christian Convention Ltd** ABN 86 000 153 560 (**KCC**) appreciates that privacy is very important. KCC adopted this Privacy Policy as we recognise the right of people to keep their personal information private. As a Small Business under the Privacy Act (annual turnover of \$3 million or less in the previous financial year), KCC is currently exempt from the legislation. However, KCC intends, as far as possible, to comply with the legislation. Accordingly, the Privacy Policy covers KCC's treatment of all private and personal information that we collect or hold.

### ***Privacy Policy Statement***

#### ***Introduction***

*Your privacy is important to us. It is KCC's policy to respect the confidentiality of information and the privacy of individuals. The KCC Privacy Policy Statement will be reviewed from time to time to take account of new laws and technology, changes to our operations and practices, and to make sure it remains appropriate to the changing environment. We are committed to being open about how we use personal information. Where our documents ask for personal information, we will endeavour to state the purpose for its use and to whom it may be disclosed.*

#### **Purpose of Collecting Information**

KCC aims to "run conventions that magnify every Christian's desire to live up to their true calling: holiness". Personal information collected by us is primarily used in the registration process for each convention. We seek to maintain a relationship with delegates over the long term, rather than on a convention by convention basis. As such, personal information about people who are involved with and attend the conventions of KCC is also used to maintain contact with those people in order to minister to them effectively.

#### **What Information is Held?**

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

- Name;
- Address;
- Contact details; and
- Details of registrations for and attendance of our conventions.

We obtain most of this information directly from our delegates through registration forms and from maintaining records of information provided in the course of ongoing ministry. This information may be collected at our conventions, from responses to our communication to you, or from other public sources. Given that we are dealing with large numbers of delegates 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) these will not be any Commonwealth Government identifiers (e.g. 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 delegates, especially if we have delegates with similar names, and no current address information. If an individual makes a financial payment to KCC then other information such as bank account details and credit card information may need to be collected. 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 whom may we disclose it to?**

While we may send you information regarding the activities of KCC from time to time that we think may be useful to you, we are conscious of the need to respect your privacy. We will not disclose information regarding you without your prior consent. The personal information you give to us may be made available to KCC employees, key volunteers and senior leaders at the discretion of the Board and Executive Director. This is in keeping with our stated purpose for the collection of the information:

- The nature of the information being collected;
- The purpose of the collection;
- The nature of the distribution of the list;
- An avenue for people to not have their information listed.

#### **Sensitive information is subject to greater restrictions**

Some personal information we hold is 'sensitive'. 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.

As part of our Privacy Policy we hereby undertake to collect only the following information that is deemed to be 'sensitive information':

- *Membership of religions*  
The form of information collected will be restricted to the denomination, location and name of the church that the individual may attend.
- *State of health, medical history*  
On occasions, we may seek to collect this information, when we consider that the collection is helpful to assist in appropriately managing risk to life and/or health of delegates. For example, when we are dealing with children who for a stated and agreed reason will be absent from their parents and under our care. In such a case, a separate form will be provided for the collection of such information. This form will include (but is not limited to):
  1. The nature of the sensitive information being collected;
  2. The purpose of the collection;
  3. How the information will be stored and used;
  4. How long the information will be stored for;
  5. An avenue for people to not have their information collected – and the consequences of us not being able to collect such information.
- *Criminal record and sexual preferences*  
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 only be held according to the guidelines set down 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**

KCC seeks to train its employees and volunteers who handle personal information to respect the confidentiality of members' information and the privacy of individuals. KCC regards breaches of your privacy very seriously. 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, email, over the internet, or other electronic media. We hold personal information in a combination of secure computer storage facilities and unauthorised 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. KCC endeavours to ensure that the personal information it holds is accurate and up-to-date. We realise that this information changes frequently with changes of address and other personal circumstances. We can update your information over the telephone.

### **Request/s to view and make amendments**

Any individual can at any time view or amend the information that is held on them by KCC. Requests to view or amend personal information can be made by contacting our Privacy Officer:

Privacy Officer  
Katoomba Christian Convention  
PO Box 156  
Burwood NSW 1805

Ph: 1300 737 140  
Fax: 1300 737 145  
Email: [privacy@kcc.org.au](mailto:privacy@kcc.org.au)

## Summary of Privacy Principles

(See [www.oaic.gov.au](http://www.oaic.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 and 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 reasonable 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 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.