NZ Privacy Policy

INTRODUCTION

We, as Gospel workers, elders and friends are a 'body of persons' and are therefore considered to be an 'Agency' under the Privacy Act 2020, because we collect and hold personal information about other people. Under the Privacy Act there are thirteen information privacy principles, and this policy describes how we meet these principles.

Personal information is any information that tells us something about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address. This means that all sorts of things can contain personal information, including notes, emails, recordings, photos, and scans, whether they are in hard copy or electronic form.[1]

PERSONAL INFORMATION THAT IS COLLECTED

We collect personal information directly from an individual and/or from someone acting on the behalf of an individual. The personal information we collect could include name, home address, mailing address, email address, phone number, gender and date of birth.

We only collect personal information for lawful purposes connected with our functions and activities, and only where the collection of such information is **necessary** for those purposes.

We also generate personal information about individuals in the course of our activities. The personal information we may generate about a person includes name, address, correspondence between us and the person or us and other agencies, memoranda, file notes and minutes of meetings.

Individuals can choose not to provide their personal information to us. However, this will limit the activities we can provide to that person. If individuals do not provide us with necessary personal information, we may not be able to provide certain information to them (eg if we don't know their email address). In terms of convention attendance, if an unknown person arrives at a convention property and they refuse to give us their name, they will not be allowed to enter. Regarding child safety, exclusion of some information may mean that we are unable to provide the support outlined in the NZ Child Safe Policy.

METHOD OF COLLECTION OF PERSONAL INFORMATION

We will only collect personal information by lawful and fair means and not in a way that may be unreasonably intrusive. Wherever possible, we collect personal information directly from the individual (or someone acting on behalf of an individual) when a person provides information to us (such as when a person completes a form in hard copy or via our website). We may also collect personal information from third parties where the individual has authorised the relevant collection such as any authorised representatives. We may also collect personal information from publicly available sources.

Individuals will give consent to use their personal information. Prior to giving consent, we will ensure that the request for consent is given in an intelligible and easily accessible form and includes the purpose for data collection.

[1] https://www.privacy.org.nz/responsibilities/your-obligations/

We will take reasonable steps to ensure that the person is aware that the:

(a) information is being collected;
(b) purpose for which the information is being collected;
(c) intended recipients of the information;
(d) name and address of the agencies that are collecting and holding the information;
(e) collection of the information is authorised or required by or under law, and if so
    (i) the particular law; and
    (ii) whether the supply of information is voluntary or mandatory;
(f) consequences of not providing the information; and
(g) rights of access to and correction of information

PURPOSES OF COLLECTING, HOLDING, USING AND DISCLOSING PERSONAL INFORMATION

We may collect, hold, use and disclose personal information to:

(a) Determine who is attending what convention, and their accommodation preferences;
(b) Meet catering and health & safety requirements, including emergency response ;
(c) Facilitate a rapid sign in/sign out process;
(d) Identify and respond to risks concerning child safety;
(e) Communicate with individuals;
(f) Work with other organisations; and
(g) Comply with relevant laws and regulations.

We may send out communications via text messages or email. Individuals will have the option to 'opt out' of receiving communications at any time by advising their elder and/or worker in their field.

DISCLOSURE OF PERSONAL INFORMATION

We will not disclose personal information except in accordance with the Privacy Act. We may disclose personal information to the convention coordinator, or people that hold overall responsibility for food, accommodation, health and safety, sign-in personnel and or convention property owners and if necessary, to any other authorised persons or entities, in accordance with legal obligations.

We will responsibly manage personal data of individuals. We may disclose personal information, in a manner consistent with the purposes for which it was collected, to:

(a) our related entities;
(b) agents and contractors that provide services to us or perform functions on our behalf, including its legal advisers, investigators, website managers and providers of internet, data storage and data access services;
(c) anyone else whom the individual authorises us to disclose personal information to; and
(d) anyone else required or authorised by law.

We will ensure that where personal information is disclosed to any person or entity referred to in subparagraph (a) to (d) above will be contractually bound to use the personal information that is shared with them only to perform the services they have been instructed by us to provide.

PROTECTION OF PERSONAL INFORMATION

We use such security safeguards as reasonable in the circumstances to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We take precautions including:

(a) restricting access to held/stored personal information;
(b) imposing confidentiality requirements on its users;
(c) requiring that its contractors and agents take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure;
(d) implementing electronic security systems, such as firewalls;
(e) ensuring that systems containing individuals' information have security measures such as password protection; and
(f) taking reasonable steps to protect "unique identifiers" from being misused. (Unique identifiers are individual's numbers, names or other forms of identification allocated to people by organisations eg driver's license and passport numbers.)

We use both manual and cloud-base storage.

Where it is necessary for us to give a person the personal information of another in connection with services provided to us, we will do everything reasonably within our power to prevent unauthorised use or disclosure of the information.

ACCURACY OF PERSONAL INFORMATION

We aim to ensure that the personal information we keep is accurate, up-to-date, complete, relevant and not misleading.

ACCESS AND CORRECTION OF PERSONAL INFORMATION

Individuals have a right to access and seek correction of personal information that we hold about the person, in accordance with the Privacy Act.

Where information is held in such a way that it can be readily retrieved by us, we will, on request, provide the information to the individual, in accordance with the Privacy Act.

We will not charge the individual for the making of the request or to correct or update the personal information.

If the individual would like to access or correct personal information, the individual may contact our Privacy Officer via the contact details listed below. We will respond to the request within **20 working days**. We may decide to grant or refuse access to, or correction of, personal information. However, if we refuse to provide access to or correct the information, we will notify the individual of the reasons for refusal. We may also add a 'statement of correction' to our files that clearly shows that the individual asked to have the information changed or corrected.

VERIFICATION OF AN INDIVIDUAL

Before any personal information can be given to an individual requestor, that person must provide their identification details to the Privacy Officer. The person's name, date of birth and address will be verified via the person providing a certified copy of their passport or NZ driver's licence and address document (eg. rates notice, utilities bill, mobile phone bill).

A person may not request information about another person, unless they have the authority to do so and a certified copy of authority is provided to us (eg. enduring power of attorney). In this case, the person requesting the information and the individual would both need to be verified.

RETENTION OF INFORMATION

We will not keep personal information for longer than it is required for the purposes for which the information may be lawfully used.[2]

If personal information is no longer required, or for any reason authorised under NZ law, it will be destroyed.

DISCLOSING INFORMATION OVERSEAS ("CROSS-BORDER DISCLOSURE")

Personal information may only be disclosed to an overseas agency if that agency has a similar level of protection to New Zealand, or the individual is fully informed and authorised the disclosure.

We must undertake the necessary due diligence of overseas agencies **before** making a cross-border disclosure of personal information.

We may only participate in a cross-border disclosure if the offshore agency meets the following criteria:

1. Is subject to the Privacy Act because the agency does business in New Zealand; or
2. Is subject to privacy laws that provide comparable safeguards to the Privacy Act, or they agree to protect the information in such a way e.g. by using model contract clauses; or
3. Is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, we may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

CLOUD STORAGE

We may send information to an overseas organisation to hold or process on our behalf as our 'agent'. This will not be treated as a disclosure under the Privacy Act. For example, an overseas company providing cloud-based services for a New Zealand organisation. We will be responsible for ensuring that any agent – the overseas company – handles the information in accordance with the New Zealand Privacy Act.

[2] Recommendation 83 of the Abuse in Care, Royal Commission of enquiry recommends that records relating to CSA are kept for 75 years.

URGENT DISCLOSURES

We may need to make a cross-border disclosure in certain, urgent circumstances where it would not otherwise be allowed. Information privacy principle 12 (IPP 12) allows cross-border disclosure when it is necessary to maintain public health or safety, to prevent a serious threat to someone's life or health, or for the maintenance of the law.

PRIVACY COMPLAINTS

If an individual believes that we have breached the Privacy Act, the individual may contact our Privacy Officer via the contact details listed below. We may request that the individual puts the complaint in writing. We will endeavour to resolve the complaint in a reasonable time frame (usually within 20 working days) and may contact the individual to obtain further details in order to provide the individual with a full and complete response. If the individual is not satisfied with the way we have handled the complaint, the individual can lodge a complaint with the Office of the Privacy Commissioner at www.privacy.org.nz.

BREACHES

PRIVACY BREACH

A privacy breach in relation to personal information held by us means:

(i) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
(ii) an action that prevents us from accessing the information on either a temporary or permanent basis.

This includes whether or not the breach was caused by someone inside or outside our fellowship, or whether or not it is ongoing.

NOTIFIABLE PRIVACY BREACH

If we have a privacy breach that has caused *serious harm* to someone (or is likely to do so), we must notify the Office of the Privacy Commissioner as soon as practicable. Breaches must be lodged via NotifyUs at www.privacy.org.nz.

If a notifiable privacy breach occurs, we should also notify any person that is affected as soon as possible after the breach occurs, unless relying on permitted exceptions set out in s116 of the Privacy Act.

When assessing whether a privacy breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach, we must consider the following:

(a) any action taken by us to reduce the risk of harm following the breach:
(b) whether the personal information is sensitive in nature:
(c) the nature of the harm that may be caused to affected individuals:
(d) the person or body that has obtained or may obtain personal information as a result of the breach (if known):
(e) whether the personal information is protected by a security measure:
(f) any other relevant matters.

Any privacy breaches, whether notifiable or not, will be summarised in the attached form – 'Annexure 2, Breach and Incident Report'. This form will be kept by the Privacy Officer.

CRIMINAL OFFENCES

It is a criminal offence:

- for a person to mislead us by impersonating someone, or pretending to act with that person's authority, to gain access to their personal information to have it altered or destroyed.
- for us to destroy a document containing personal information, knowing that a request has been made for that document.

PRIVACY OFFICER CONTACT DETAILS

To access or correct personal information, to notify us of an alleged breach of the Privacy Act or if there is any privacy related inquiry, please contact:

The Privacy Officer
privacyofficernz@gmail.com

GOVERNANCE

This policy shall be reviewed at least every 3 years.

Next review due 31st July 2028. Review by the Overseer and Designated Person/s for Child Safety.

Annexure 1 – Privacy Principles *(referenced from www.privacy.org.nz)*

The Privacy Act 2020 has 13 privacy principles that govern how you should collect, handle and use personal information.

Principle 1 – Purpose for collection

You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

Principle 2 – Source of information – collection from the individual

You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source.

Principle 3 – What to tell the individual about collection

When you collect personal information, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information.

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

Principle 4 – Manner of collection

You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

Principle 5 – Storage and security of information

You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

Principle 6 – Providing people access to their information

People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy.

Principle 7 – Correction of personal information

A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

Principle 8 – Ensure accuracy before using information

Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

Principle 9 – Limits on retention of personal information

You must not keep personal information for longer than is necessary.

Principle 10 – Use of personal information

You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

Principle 11 – Disclosing personal information

You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law.

Principle 12 – Disclosure outside New Zealand

You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

Principle 13 – Unique identifiers

A unique identifier is a number or code that identifies a person in your dealings with them such as driver's licence number or passport. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.

Annexure 2 – Breach and Incident Report

Breach and Incident Report

The Privacy Officer must be notified of all Breaches and Incidents immediately.

Information Required	Details
Name of individual affected:	
Date:	
Date Breach occurred	
If Breach was not reported on the same day it occurred state the reason for the delay:	
Was it a notifiable privacy breach?	
What happened? (Summary of Breach)	
Significance of Breach	
Was the Breach a “material” Breach?	
Was this the result of a systemic problem?	
Was this the result of human error?	
Date Breach was resolved, or date Breach will be resolved	
What action has been/will be taken to rectify the Breach?	
What action has been/will be taken to ensure the Breach does not occur again?	
Timing of action	
Other comments Report completed by	
Signature	
Reviewed (Privacy Officer)	
Has the breach been reported to the NZ Overseer? Reason Y or N:	
Has the Breach been reported to the Privacy Commissioner? State date reported.	
Does the individual need to be notified? Yes, if a notifiable privacy breach and not a permitted exemption (refer Privacy Policy).	
Name:	
Signature:	
Position (NZ Overseer):	