



MercyWorks

SISTERS OF MERCY
IN AUSTRALIA & PAPUA NEW GUINEA

PRIVACY POLICY

Policy Number:	07	Version:	2
Updated by:	Anthony Pool	Approved by Board on:	28 October 2020
Reason of Review:	Review to include ACFID CAS/ACNC and CPSL guidelines	Scheduled review date:	As per schedule

INTRODUCTION

Mercy works Limited (MWL) promotes social justice through local and overseas relief and development activities that are part of the mission and vision of the Sisters of Mercy in Australia and Papua New Guinea.

The programs engage in partnerships with communities to promote justice, self-reliance and to support peoples and communities who are displaced or denied access to basic resources such as education, health and social welfare.

1. PURPOSE

The purpose of this Policy is to ensure that MWL manages personal information in an open and transparent way and complies with the Privacy Act 1988 (Cth), the National Australian Privacy Principles, and the Payment Card Industry Data Security Standard. It is also designed to confirm compliance with the Privacy Amendment (Notifiable Data Breaches) Act 2017 (subject to the conditions prescribed in the Privacy Act). MWL acknowledges the responsibilities it holds as an Australian Privacy Principles (APP) entity.

The purpose of this Policy is also to ensure observance with the Australian Council for International Development (ACFID) Code of Conduct Principles, in particular:

- Commitment 6.2 - We collect and use information ethically; and
- Commitment 7.2 - We meet our legal and compliance obligations; and
- Commitment 7.3 - We are accountable to our stakeholders.

Any exemption to this Policy must be applied for in writing, for approval by the Executive Director. Any exemption granted by the Executive Director must be in writing.

2. SCOPE

This Policy provides guidance to Workers (see definition 3.10) in relation to their work with/for MWL.

This Privacy Policy explains:

- a) the scope of our Privacy Policy;
- b) why we collect personal information;
- c) what personal information we collect;

- d) how we collect and use personal information;
- e) how we disclose personal information, including to overseas recipients;
- f) your right to access personal information;
- g) your right to correct personal information;
- h) how we protect the integrity of personal information;
- i) the right to make a privacy complaint;
- j) how to contact us regarding privacy concerns; and
- k) how we deal with breaches.

3. DEFINITIONS & ACRONYMS

Terms used in this Policy are:

3.1 Australian Privacy Principles (APP) - As laid out in Schedule 1 of the Privacy Act 1988 (Cth).

3.2 Australian Privacy Principles (APP) Entity - Is an agency or organisation.

3.3 Notifiable Data Breach (NDB) Scheme - Any organisation or agency subject to this scheme must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

3.4 Health information - Includes *personal information* collected from you in order to provide a health service. There are greater restrictions that apply to our collection, storage, use and disclosure of sensitive information under the Privacy Act 1988 (Cth).

3.5 OAIC – Office of the Australian Information Commissioner

3.6 Personal Information - Information or an opinion about an identified individual or an individual who is reasonably identifiable:

- a. whether the information or opinion is true or not; and
- b. whether the information or opinion is recorded in a material form or not.

As defined in the Privacy Act 1988 (Cth).

3.7 Payment Card Industry Data Security Standard – This standard was created jointly in 2004 by four major credit card companies: Visa, MasterCard, Discover, and American Express. It is a widely accepted set of policies and procedures intended to optimise the security of credit, debit and cash transactions to protect cardholders against misuse of their personal information.

3.8 Primary Purpose - Under the Privacy Act 1988 (Cth), an APP Entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose', or for a secondary purpose if an exemption applies as defined by the Act).

3.9 Sensitive information - Is a special category of *personal information* and includes, but is not limited to, information about your health, race or ethnic origin, political or religious beliefs, membership of a trade union or association, or criminal record.

3.10 Workers – refers to all MWL Board Directors, committee members, employees, contractors and volunteers.

4. APPLICATION

4.1 Collection of personal information

We collect *personal information* from you for the following purposes (Primary Purpose):

- a) to lawfully carry out our functions and activities;
- b) to deliver the services that you requested, or to deal with donations;
- c) to provide you with further information about the services that you requested or about donations;
- d) to personalise and customise your experiences with us;
- e) to help us review, manage and enhance our services;
- f) to develop insights used in reports or other content developed by us;
- g) to communicate with you;
- h) for administration purposes, including charging, billing and collecting debts;
- i) to promote and market those of our other services which we consider may be of interest to you;
- j) when considering making offers to job applicants and prospective employees or for employment purposes; and
- k) to receive services from you or the organisation which employs you.

In addition to the Primary Purpose, we may use the *personal information* we collect and you consent to us using, to:

- a) provide you with news about any services or donation matters;
- b) send you marketing and promotional material that you may be interested in;
- c) communicate with you, including by email, telephone and mail;
- d) manage and enhance services or your experience on our Website and domains;
- e) conduct surveys or promotions;
- f) verify your identity;
- g) investigate any complaints about, or made by you, or if we have reason to suspect you have breached any relevant terms and conditions; and
- h) as required or permitted by any law.

Unless otherwise provided by law, we will not collect, hold, use or disclose *sensitive information* without your consent.

4.2 The Type of personal information we collect

The nature and extent of *personal information* we collect varies depending on your particular interaction with us and the nature of our functions and activities.

Personal information that we commonly collect from you would include (but is not limited to):

- a) your name, position, date of birth;
- b) your address, email address, telephone numbers, gender, driver's licence number, passport number;
- c) your financial information including credit card and banking information, business references, details about your business, Australian Business Number;
- d) nature of services being sought;
- e) insurance details, rates and fees; and
- f) your occupation, career history and references.

We also collect information that is not *personal information*, such as data relating to your activity on our Website.

If you feel that the *personal information* that we are requesting at any point is not information that you wish to provide, please feel free to raise this with us.

4.3 How we collect personal information

Generally, *personal information* is collected by us from a variety of sources, including when dealing with members of the public or customers, when dealing with individuals, undertaking marketing initiatives, or when recruiting.

For example, we may collect *personal information* from you in the following circumstances:

- when you are dealing with donor services, fulfilling your registrations to events, webinars, participating in surveys or purchasing/accessing services;
- when you deal with us as an independent contractor; or
- when you apply for a job.

Personal information may be provided by you using our Website or by telephone, business cards, contracts, applications, survey entries, mail or email, registration forms, face-to-face or in writing, whether verbally, in hardcopy or electronic format.

Where possible, we collect your *personal information* directly from you. In some circumstances, we may obtain *personal information* from a third party.

If you provide *personal information* about another person to us, we require that you:

- inform that person you have done so and provide them with a copy of this Policy; and
- confirm to us that you have that person's consent to provide such information for the purpose specified.

If we receive unsolicited *personal information* about you that we could not have collected in accordance with this Privacy Policy and the Privacy Act, we will within a reasonable period, destroy or de-identify such information received.

4.4 Website and Google Analytics

Information we collect may include:

- a) the Internet Protocol address and a component of the domain name used (e.g. .com or .net);
- b) the type of browser and operating system you used;
- c) the date and time you visited our Website;
- d) the web pages or services you accessed at our Website;
- e) the time spent on individual pages and our Website overall;
- f) which files you downloaded; and
- g) information about your computer and Internet connections using cookies.

We use Google Analytics Demographics, and Interest Reports to obtain a more detailed understanding of our Website users and their potential needs. We do not collect *personal information* by such methods; only aggregate data is used for planning purposes.

4.5 Social Media

Authorisation will be obtained before posting a person's photos on social media. Personal phone numbers and email addresses will not be made available on social media.

4.6 Use of your personal information

We will only use and disclose your *personal information*:

- for purposes which are related to the Primary Purpose; or

- if we otherwise get your consent to do so, in accordance with this Privacy Policy and the Privacy Act.

This will include:

- maintaining accurate records of fundraising
- establishing and maintaining donor relationships and networks
- establishing and maintaining membership of Friends of MWL
- communicating the services of MWL online and through publications
- ensuring that programs of MWL are appropriate and effective
- meeting professional and legal requirements related to government funding, where the use or disclosure is required or authorised by law.

We will not use your *personal information* for any purpose for which you would not reasonably expect us to use your *personal information*. Additionally, we will not disclose your sensitive information without your consent, unless there is a need to disclose such information in accordance with the Privacy Act or to comply with any other regulatory requirement.

We take special care with your card payment details as we must under the Payment Card Industry Data Security Standard

We will only use or disclose your *personal information* for the purposes of direct marketing if:

- we collected the information from you;
- it is reasonable in the circumstances to expect that we would use or disclose the information for direct marketing purposes;
- we provide you with a simple means to 'opt-out' of direct marketing communications from us; and
- you have not elected to 'opt-out' from receiving such direct marketing communications from us.

You may opt-out of receiving such communications by:

- a) clicking a link on the email communications sent to you; or
- b) contacting our Office by telephone on 02 9564 1911 or
- c) at mercyworks@mercyworks.org.au ; or
- d) writing to us at Mercy Works, Sally Bradley, Executive Director, PO Box 2023, North Parramatta, NSW 1750.

You are not obliged to give us your *personal information*. If you would like to access any of our services on an anonymous basis or using a pseudonym, we will take reasonable steps to comply with your request. However, we will require you to identify yourself if:

- we are required by law to deal with individuals who have identified themselves; or
- it is impracticable for us to deal with you if you do not identify yourself or elect to use a pseudonym.

Please also be aware that your request to be anonymous or to use a pseudonym may affect our ability to provide you with the requested goods and/or services and the range of options available to you or the organisation as a member may be limited.

For example, we may not be able to provide the full range of services or allow you or your organisation to participate in functions, seminars or events if you do not provide your *personal information*.

For the purposes referred to above in this Privacy Policy, you acknowledge and agree that we may disclose personal information and you consent to us disclosing such *personal information* to:

- a) our Affiliated Entities;
- b) third parties engaged by us to perform functions or provide services or deal with donations on our or their behalf such as mail-outs, marketing or advertising;
- c) third parties that sponsor or promote us;
- d) third party contractors engaged to provide online credit card account processing and related services. When you pay your accounts online, a secure server is used which encrypts the information you send through our Website. We make no warranty in respect of the strength or effectiveness of that encryption, and we are not responsible or liable for events arising from unauthorised access of the information you provide;
- e) your referees and former employers;
- f) credit agencies;
- g) our professional advisors, including our accountants, auditors and lawyers;
- h) persons authorised by you to receive information held by us; and
- i) any persons as required or permitted by any law.

We will not rent, sell or exchange your information without your consent.

We do not send personal information overseas.

5.6 Access to personal information

If you require access to your *personal information*, please contact the MWL Executive Director. You are required to put your request in writing and provide proof of your identity.

We are not obliged to allow access to your *personal information* if:

- a) we reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or public health or public safety;
- b) giving access would have an unreasonable impact on the privacy of other individuals;
- c) the request for access is frivolous or vexatious;
- d) the information relates to existing or anticipated legal proceedings between you and us and would not ordinarily be accessible by the discovery process in such proceedings;
- e) giving access would reveal our intentions in relation to negotiations with you in a way that would prejudice those negotiations;
- f) giving access would be unlawful;
- g) denying access is required or authorised by or under an Australian law or a court/tribunal order;
- h) we have reason to suspect that unlawful activity, or misconduct of a serious nature relating to our functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- j) giving access would reveal internal evaluative information in connection with a commercially sensitive decision-making process.

If you make a request for access to *personal information*, we will:

- respond to your request within a reasonable period; and
- if reasonable and practicable, give access to the information in the manner requested.

If we refuse to give access to the *personal information* because of an exception or in the manner requested by you, we will give you a written notice that sets out at a minimum:

- our reasons for the refusal (to the extent it is reasonable to do so); and
- the mechanisms available to complain about the refusal.

We reserve the right to charge you reasonable expenses for providing access to *personal information*, for example, a fee for photocopying any information requested by you.

Nothing in this Privacy Policy replaces other informal or legal Policies by which you can be provided with access to *personal information*.

4.7 Correction of personal information

We request that you keep your *personal information* as current as possible. If you feel that information about you is not accurate or your details have or are about to change, you can call us on 02 9564 1911, and we will correct or update your *personal information*.

If you make a request to correct your *personal information*, we will:

- respond to your request within a reasonable period; and
- if reasonable and practicable, correct the information in the manner requested.

If we refuse a request to correct *personal information*, we will:

- give you a written notice setting out the reasons for the refusal and how you may make a complaint; and
- take reasonable steps to include a statement with your *personal information* we refuse to correct.

We reserve the right to charge you reasonable expenses for making a correction to your *personal information*, for example, a fee for photocopying relevant information.

Nothing in this Privacy Policy replaces other informal or legal Policies by which you can correct *personal information*.

4.8 Integrity of personal information

We will take reasonable steps to:

- ensure that the *personal information* that we collect is accurate, up to date and complete;
- ensure that the *personal information* that we hold, use or disclose is, with regard to the relevant purpose, accurate, up to date, complete and relevant; and
- secure your *personal information* while it is being held by us.

We will take reasonable steps to protect *personal information* from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

Electronic information is protected by various security measures (including encryption and password protection), and physical paper files are stored in a secure location. *Personal information* is de-identified, where appropriate. Data protection includes the use of password access areas and secure servers.

You acknowledge that the security of communications sent by electronic means or by post cannot be guaranteed. We cannot accept responsibility for misuse, loss or unauthorised access to your *personal information* where the security of information is not within our control. If you suspect any misuse or loss of your *personal information*, please contact us immediately.

We will take reasonable steps to destroy or de-identify any *personal information* held by us if we no longer need to hold the information for the purpose it was collected and we are not otherwise required by law to retain the information.

4.9 Notifiable Data Breaches (NDB)

The Privacy Act states a data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

Some examples are:

- When a device containing personal information is lost or stolen;
- When a database containing personal information is hacked; or
- When personal information is mistakenly provided to the wrong person.

Data breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow MWL's information handling policies that cause accidental loss or disclosure. The NDB scheme requires entities to notify individuals and the Australian Privacy Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur); and
- This is likely to result in serious harm to any of the individuals to whom the information relates; and
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

MWL will also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

MWL notifies the Australian Privacy Commissioner whenever MWL has reasonable grounds to believe that an eligible data breach has happened; or when directed to do so by the Australian Privacy Commissioner.

In the event of a suspected data breach, MWL will perform the following steps:

Step 1: Contain the breach and complete a preliminary assessment;

Step 2: Evaluate the risks associated with the breach;

Step 3: Notify the affected individual(s);

Step 4: Notify the Australian Privacy Commissioner/OAIC following the Notifiable Data Breach (NDB) Scheme as required; and

Step 5: Review processes and procedures to prevent future breaches.

5 BREACH

A breach of this Policy may result in disciplinary action that may involve severance from the organisation.

6 AUTHORITY

This Policy is approved and reviewed by the Board.

7 RELATED POLICIES/DOCUMENTS

Other organisational policies, legislation, and codes etc. that should be read in conjunction with this Policy and with MWL's ethical value principles include:

- Code of Conduct Policy
- Management of Concerns, Complaints and Commendations Policy
- Fundraising and Development Policy
- Risk Management Framework

- Social Networking Policy
- ACFID Code of Conduct - Commitment 6.2, 7.2 and 7.3
- Privacy Act 1988 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Payment Card Industry Data Security Standard

8 CONTACTS

Complaints about how we collect, use, disclose, manage or protect personal information, or otherwise consider that there may be a breach of the Privacy Act or the Australian Privacy Principles, can be made to:

Sally Bradley RSM
Executive Director
Mercy Works Ltd
Level 3, 6 Victoria Road
Parramatta NSW 2150
02 9564 1911
mercyworks@mercyworks.org.au

9 REVIEW

Review of this Policy, related forms and resources will be undertaken every three years by the Executive Director and approved by the MWL Board.


10 REVISION/MODIFICATION HISTORY

Date	Version	Current Title	Summary of Changes	Approval Date	Commencement Date
21 October 2015	1	MWL Privacy Policy	New	21 October 2015	22 October 2015
28 October 2020	2	Privacy Policy	Rewritten Policy to ACFID Requirements	28 October 2020	29 October 2020

11 APPROVAL DATE/REVISION SCHEDULE

Approved by: Board, Mercy Works Limited
Date: 28 October 2020

To be Revised: 28 October 2023

Board Chair Signature	
Date	10.11.2020