

STEER INCORPORATED

PRIVACY POLICY

Steer Incorporated (Steer) respects and honours its ministry partners, friends and contacts, and their right to be treated courteously and fairly, and to have their privacy protected. Steer is committed to complying with the Australian Privacy Principles contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and amendments.

1. Collection and Use

- 1.1. Names, contact details and other information provided by ministry partners and interested friends are collected by Steer, 1 Vision Drive, Burwood East, Victoria 3151, for the purpose of maintaining its database of contacts.
- 1.2. Ministry partners who become involved in one of Steer's programs for the purpose of supporting mission and outreach work in Australia and overseas also provide personal information which is used by Steer in its administration of the programs and its arrangements with the ministry partners. Personal information collected from ministry partners by Steer may be sensitive information for the purposes of the Australian Privacy Principles (ie information about a person's religious beliefs and commitments, etc).
- 1.3. Steer is willing to deal with individuals who contact it on an anonymous basis, or using a pseudonym. However, individuals who become Steer ministry partners must identify themselves and provide the necessary personal information required by Steer to administer its programs, because it is impracticable to operate these programs without the relevant personal information.
- 1.4. Unless requested otherwise, Steer provides the names and addresses of ministry partners to mission and outreach agencies which receive funds from Steer resulting from distribution suggestions made by the ministry partners concerned. These agencies may be located in Australia or in an overseas country, depending on the ministry partner's suggestions. The information is provided so that the agencies may acknowledge the funds. However, ministry partners may request that funds are distributed anonymously without their identities being disclosed to recipient agencies.
- 1.5. When ministry partners make distribution suggestion involving an overseas mission or outreach agency, and have not requested that the funds are distributed anonymously, Steer will inform them that their names and addresses will be provided to the overseas agencies concerned. If the ministry partners consent to this, then Sub-clause 8.1 of the Australian Privacy Principles preventing the transfer of such information overseas will not apply to the disclosure of the individual's personal information to overseas agencies by Steer.
- 1.6. Apart from the above, Steer will not provide details of its contact database, or details of individual contacts or ministry partners, to anyone without first obtaining the consent of the person or persons concerned. Steer will not sell, rent or trade mailing lists to another organisation or person for any purpose.

2. Data Quality and Security

- 2.1. Steer will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure, and will ensure that personal information is kept secure and confidential. Steer will also take reasonable steps to ensure that all personal information collected and used by it is accurate, complete and up to date.

2.2. With the exception of the purpose set out in 1.4 above, only Steer staff and those who perform services on Steer's behalf, who are authorised to handle personal information, will have access to such information.

3. Access and Correction

3.1. Individuals are invited to advise Steer of any change to personal details to ensure that Steer's records are complete and up to date.

3.2. Individuals may ask to see personal information about themselves and Steer will provide access to the information as soon as it is reasonably able, and in the manner requested by the individual if it is reasonable to do so. If the personal information held is not accurate, complete and up to date, Steer will take reasonable steps to correct the information. This right is subject to some exceptions, for example access may not be provided to information relating to existing or anticipated legal proceedings, or where it would breach the confidentiality pertaining to the personal information of others.

3.3. Steer staff will clearly identify themselves when making contact with individuals, and all correspondence and publicity materials will contain Steer's contact details.

4. Complaints

4.1. If you have a complaint about a breach by Steer of this Privacy Policy or the Australian Privacy Principles, you should contact the National Director of Steer Incorporated in writing as set out below. The National Director will investigate the complaint and take all reasonable steps to rectify any such breach.

5. Notifiable Data Breach Scheme

The Privacy Amendment (Notification of Data Breaches) Act 2017 ("NDB scheme") came into effect on 23 February 2018.

The NDB scheme applies to Steer and Steer has an ongoing obligation to take reasonable steps to handle personal information in accordance with Australian Privacy Principles. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification and disclosure.

The Office of the Australian Information Commission (OAIC) is the key regulator responsible for functions that are conferred by the Privacy Act. OAIC has issued a summary fact sheet outlining the NDB scheme. Headings used therein are adopted herein and some content has been replicated to explain the application of the NDB scheme to Steer.

The NDB scheme imposes mandatory reporting requirements on Steer when collecting personal information, including such things as identity details, residency and contact details.

The fundamental purpose of the NDB scheme is to allow ministry partners to undertake corrective procedures in circumstances when their personal information has been compromised.

5.1 Suspected or Known Data Breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, that an entity holds. Steer's employees are required to immediately record a data breach on the Steer Incident Report and simultaneously notify the Privacy Officer.

5.2 Contain

Steer is required and will undertake, to first contain a suspected or known data breach and take immediate steps to limit any further access or distribution of the affected personal information, or other compromise of other information.

5.3 Assess

Steer will next undertake an assessment of the data breach. The NDB scheme is intended to capture “eligible” data breaches. Steer will create a procedure to conduct an assessment and will follow OAIC’s suggested three-stage process, namely Initiate, Investigate and Evaluate to identify an eligible data breach. The Privacy Officer will lead and take responsibility for this assessment and in doing so will apply the criteria below: An “eligible data breach” is deemed to have occurred if either:

An unauthorised access to, or disclosure of, the relevant information, and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or

The relevant information is lost in circumstances where unauthorised access to or unauthorised disclosure of that information might occur, and if it did, a reasonable person would conclude that it would be likely to result in serious harm to any of the individuals to whom the information relates.

The Privacy Officer, in undertaking this assessment, should also consider remedial action. The assessment should be expeditious and , generally, within 30 days and should be documented.

5.4 Notify

Where serious harm is likely, Steer must prepare a statement for the OAIC Commissioner that contains:

- Steer’s identity and contact details
- A description of the breach
- The kind (s) of information concerned
- How Steer will respond to the breach
- Recommended steps for individuals

Steer must also notify affected individuals and inform them of the content of the statement.

There are three options of notifying:

- Notify all individuals
- Notify only those individuals at risk of serious harm
- If neither of these options are practical, then, Steer can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach

Notification exceptions can apply to mandatory reporting obligations. The most notable exception is in the event that Steer has taken necessary remedial actions upon discovering a data breach before serious harm has occurred. In this instance, Steer is not required to report the breach to the OAIC or to affected individuals.

5.5 Review

Steer will implement a review process after or during the relevant assessment by the Privacy Officer. The Privacy Officer will take the lead in the process and review the incident and take action to prevent future breaches. These preventative actions may include:

- Investigate and understand the cause of the breach
- Develop a prevention plan
- Conduct audits to ensure the prevention plan is implemented and being adhered to
- Update relevant policies and procedures and practices, including frequency and nature of staff training

Where necessary, Steer will consider reporting the incident to other relevant bodies.

6. Changes to this Privacy Policy

6.1. It may be necessary for Steer to review and revise its Privacy Policy from time to time. An up to date version will be posted on Steer's website at www.steer.org.au. You are invited to visit the website regularly to keep up to date with any changes.

7. Contact Us

7.1. If you would like any further information, or have any queries, problems or complaints in relation to Steer's Privacy Policy, or its information handling practices in general, please contact the National Director of Steer Incorporated at:

Email: steer@steer.org.au
Address: P O Box 211, Box Hill Vic 3128