Teen Missions Australia

Australian Company Number (ACN) 010 725 881
Australian Business Number (ABN) 25 010 725 881
A company limited by guarantee

Privacy Policy

1 Statement

(a) Under the Privacy Act 1988 (Cth) (**Privacy Act**), Teen Missions International Australia Limited (**Teen Missions**) is legally obliged to protect and manage Personal Information in accordance with a set of detailed rules called the Australian Privacy Principles (**APPs**).

(b) The Privacy Act imposes very serious penalties for breaching the APPs and any privacy breach could cause substantial damage to the reputation of the Teen Mission's brand and business. It is therefore important that as employees, you familiarise yourselves with the APPs and assist Teen Mission comply with its obligations.

(c) This document sets out some important guidelines and procedures that you need to follow.

2 Definitions

2.1 Personal Information

(a) Personal Information is defined in the Privacy Act as:

(i) information or an opinion;

(ii) about an identified individual (ie a natural person, not a corporation or business); or

(iii) an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information is recorded in a material form or not.

(b) This includes obvious types of information, eg:

(a) name;

(b) telephone numbers;

(c) addresses (postal, email, etc);

(d) gender; and

(e) age or date of birth.

(c) But it may also include less obvious examples, particularly if they are combined with other data:

(i) the IP address of a computer or other device; or

(ii) location data (eg from a mobile device's GPS).

(d) Examples of what is not Personal Information includes:

(i) a record of an individual's activities that is not linked to any identifying detail of the kinds described above (and provided their identity cannot reasonably be ascertained from the record itself); and

(ii) any set of aggregated data drawn from individuals' activities to the extent that it cannot be reverse-engineered to identify any of those individuals (eg, demographic information).

2.2 Sensitive Information

2.2.1 In certain circumstances, Teen Missions also collects Personal Information which is classified as "sensitive information" under the Privacy Act including:

(a) criminal records; and

(b) police checks.

2.2.2 Under the Privacy Act and the APPs, higher standards apply to information classified as sensitive information. This sensitive information should only be accessible by restricted staff within APP Entity and should only be disclosed to an entity (generally the relevant regulatory or government authority or agency) where we have a legal or regulatory requirement or obligation to do so.

3 How Teen Missions workers can ensure privacy is always protected

3.1 Some general rules

While exceptions do apply, in general when you are handling or collecting Personal Information you should always:

(i) only collect the Personal Information which is strictly necessary for the purpose you are collecting it for (ie do not collect more Personal Information than you need);

(ii) ensure that the Personal Information is necessary for one or more of the APP Entity's functions;

(iii) only use the Personal Information for the purpose for which it was collected (eg if we collect Personal Information for licensing and probity requirements, this Personal Information should not be used for the marketing and sale of APP Entity products and services); and

(iv) consider how the Personal Information will be destroyed or de-identified once the purpose for which it has been collected has been completed (taking into consideration any legal record keeping requirements).

3.2 Collection notice

(a) APP 5 requires Teen Missions to take reasonable steps to notify individuals of certain matters or otherwise ensure the individual is aware of those matters when APP Entity collects Personal Information about an individual. In some cases, APP Entity's privacy policy may be sufficient to meet the notification requirements. However, in certain circumstances it may be best practice to provide a specifically tailored collection notice.

(b) You should always consult the legal team before preparing a collection notice, or if you are unsure if one is required.

(c) More detail about the Australian Privacy Principles generally and specific guidelines on APP 5 can be found on the Office of the Australian Information Commissioner website.[1]

3.3 New projects

(a) Whenever you start work on a new initiative (eg offer a new system for ordering products online or rolling out a new service) which will involve the collection, use or disclosure of Personal Information, or if you are considering changes to the way Teen Mission currently collects, uses, discloses or stores any Personal Information (eg, engaging a new overseas IT contractor to perform data services APP Entity), it is essential that you get advice about the privacy implications of your proposal from legal.

(d) You may need to build in some extra processes or protections to ensure we comply with the Privacy Act, or we may need to update our privacy policy or other documentation to reflect new ways of handling Personal Information.

(e) You should contact the legal team as early as possible and brief them on your proposal. They will usually be able to advise you on the privacy issues themselves, but if the issues are complex, they may need to arrange external legal assistance.

3.4 What should you do if you think there may have been a data breach?

(a) If you ever become aware that there may have been a data breach at Teen Missions Australia, it is critical that you act quickly to bring this to the attention of the Base Coordinator at complaints@teenmissions.com.au . A data breach occurs when any information, including Personal Information and tax file numbers, held by Teen Missions is the subject of inadvertent or unauthorised disclosure, access, modification, misuse, loss or interference.

(b) It is important to note that:

(i) unauthorised or inadvertent disclosure can occur verbally;

(ii) loss and unauthorised disclosure may occur in relation to “paper” records which are not stored or disposed of correctly;

(iii) unauthorised disclosure or access may also be caused by a breach of Information and Communications Technology (**ICT**) security, allowing Personal Information to be exfiltrated from the APP Entity’s systems; and

(iv) loss of Personal Information may occur through ICT equipment being:

(A) lost (eg, laptops or USB sticks without encryption or password protection being left in a taxi or on public transport); or

[1] https://www.oaic.gov.au

(B) disposed of at the end of their life without proper precautions being taken to remove any Personal Information from devices; and

(c) Data breaches are not limited to situations where there have been malicious actions, such as theft or the "hacking" of ICT systems but may also arise from internal errors or failure to follow information handling policies.

(d) Even if you are not sure there has been a data breach, it is better to discuss it with someone and have them allay your concerns, rather than to ignore the issue and find out later that Teen Missions could have avoided serious consequences if you acted quickly.

(e) Under the Privacy Act, APP Entity is obliged to notify the Office of the Australian Information Commissioner and affected individuals of Eligible Data Breaches under the mandatory data breach notification scheme. An **Eligible Data Breach** is a data breach that meets three criteria:

(a) there has been unauthorised access to or disclosure of Personal Information, or Personal Information has been lost in circumstances where unauthorised access to or disclosure of the Personal Information is likely to occur;

(b) the above is likely to result in serious harm to an individual to whom the compromised Personal Information relates; and

(c) APP Entity has not been able to prevent the likely risk of serious harm with remedial action.

(d) If we fail to meet our obligations in relation to an Eligible Data Breach, we could receive significant fines, as well as suffering other significant loss, such as losing the trust of our customers.

(e) In the first instance, you should talk to your manager about the situation. Your manager will then report it to the Board of Teen Missions Australia, who will investigate further. If your manager is involved in the data breach, you can speak directly to the Managing Directors at complaints@teenmissions.com.au ATTN: Managing Directors.

3.5 What if you receive a complaint or inquiry?

(a) Sometimes an individual may contact you with concerns about how their Personal Information has been handled, or to get more information about Teen Missions use of that information.

(b) If you do not feel confident answering their questions, or if they are alleging that Teen Missions has breached its privacy obligations, you should bring this to the attention of our Base Coordinator at complaints@teenmissions.com.au as soon as possible.

(c) Our privacy policy sets out a process for how we will handle complaints, including the timeframes within which we will respond, so it is important that you bring these to the attention of the appropriate people immediately. We also have an internal process for recording all complaints and inquiries regarding Personal Information.

3.6 What if someone asks for access to their Personal Information?

(a) Under the Privacy Act, individuals generally have a right to access (and, in some circumstances, seek correction of) Personal Information that Teen Missions holds about them.

(d) Our privacy policy sets out a process for how we will handle access and correction requests. If you receive a request, you should refer it to our Base Coordinator, as soon as possible.

(e) If you wish to access Personal Information which Teen Mission holds regarding you. You should also contact our Base Coordinator at info@teenmissions.com.au

Important links and general information about privacy

(a) You can find more information about privacy and the protection of Personal Information on the Office of the Australian Information Commissioner website.

Version Table

Version	Date of review	Person who reviewed
2	June 2025	External Legal