

Out Doors Privacy Principles

Based on APP

The Australian Privacy Principles (APP) are principles-based law. Out Doors Inc. (Out Doors) has adopted these principles in relation to information handling practices and the diverse needs of individuals.

There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

APP1: Open and transparent management of personal information

What personal information is collected?

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

Out Doors collects the following data:

- an individual's name, signature, address, phone number and date of birth
- personal contacts, emergency contacts, mental health support person/support check contact, GP, Psychiatrist
- sensitive information* such as mental health/diagnosis, physical health, other disabilities, emotional/behavioural concerns, medication and allergies.
- Other information required to risk management and safety.
- employee record information if applicable
- photographs

What is sensitive data?

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- religious or philosophical beliefs
- sexual orientation or practices
- criminal record
- health or genetic information

Generally, sensitive information has a higher level of privacy protection than other personal information.

APP2: Anonymity and pseudonymity

Date of next review: October 2023

Authorised by: CEO
Written by: CEO
Page 1 of 5

This applies in circumstances where Out Doors is required by law or a court or tribunal order to deal with identified individuals. In this case, a personal identifier will be issued.

APP3: Collection of solicited personal information

Out Doors only collects your personal information that is reasonably necessary for us to do our work and support you to meet your goals.

Consent

Your consent is generally needed for the collection of your sensitive information or to use or disclose your personal information for a purpose other than the purpose it was collected for.

Out Doors seeks consent in the following circumstances:

- for QDC, Department of Health Quarterly Data Collection Form
- for Support check (case manager, GP, Psychiatrist, support person, etc)
- for photo to be taken and used for Out Doors promotional purposes
- to be part of Out Doors' evaluation
- for external Auditing and Certification purposes

Opt-out option/withdraw

You can withdraw your consent or opt out at any time by contacting email, mail or via a phone call. It is important to be aware and understand the possible consequences of withdrawing your consent. For example, opting out or withdrawal of Support Check means that from you may no longer have access to a service.

APP4: Dealing with unsolicited personal information

All unsolicited personal information received by Out Doors, that could not have been collected under APP 3 will be destroyed or de-identified if it is lawful and reasonable to do so.

APP5: Notification of the collection of personal information

At the assessment stage, Out Doors collects your personal information and the relevance is explained during this process.

Out Doors will notify you of any changes in the way your personal information is collected and stored within a reasonable time frame. In circumstances where there is a breach or potential breach of unauthorised access to your personal information, Out Doors will notify you with 24 hours from the time the organisation becomes aware.

APP6: Use or disclosure of personal information

Australian privacy law prevents Out Doors in using or disclose your personal information unless an exception applies which includes:

- you have consented for an external organisation or agency to use your personal information for a secondary purpose,
- your personal information will be disclosed in medical emergency circumstance to assist with best treatment and support,
- your personal information will be disclosed to the Police if a criminal act has been committed, and

- an authorised agency or enforcement body (eg. Police) under an Australian law, or court or tribunal order requires the information without your consent.

APP7: Direct marketing

Out Doors will not use or disclose personal information for direct marketing purposes. In some circumstances, Out Doors will mail/email by using your name and address or email for:

- Newsletters
- Training opportunities
- Shop merchandise available
- General Out Doors related communications, eg, on Out Doors events like Mental Health Month, programs, AGM, etc.

Your personal information can also be collected from other sources and used to send you direct marketing. For example, from:

- a membership list,
- an online, paper or phone survey or competition,
- an online account that shows your purchase history or browsing habits, or
- a mail order or online purchase.

How to opt out of direct marketing

The best ways you can opt out of receiving direct marketing include:

- clicking an 'unsubscribe' link in an email or,
- replying to an email or contact Out Doors.

APP8: Cross-border disclosure of personal information

All personal information is stored on line and only Australian based third-party providers are used. This ensures that the data is protected under the Australian laws.

When you communicate with us through a social network service such as Facebook or Twitter, the social network provider and its partners may collect and hold your personal information overseas.

APP9: Adoption, use or disclosure of government related identifiers

Out Doors does not collect government related personal identifier information. In some circumstances, you will be required to provide your Medicare Number (personal identifier) in emergency circumstances however, this information will not be stored.

APP10: Quality of personal information

Out Doors must take reasonable steps to ensure that the personal information it collects is accurate, up to date and complete. You also must ensure that the reasonable steps are taken to ensure the information you provide or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP11: Security of personal information

Out Doors collects and stored your personal information in the cloud. The organisation implemented the *Essential Eight Strategies* advised by the Australian Signals Directorate's

(Strategies to Mitigate Cyber Security). For a copy of Out Doors Network Security Checklist or Cyber Security policy, please contact us.

Out Doors has an obligation to store your personal data for 7 years after you have ceased accessing our service. After that time, the information will be destroyed or de-identified.

APP 12: How to request access

You will need to contact Out Doors to request access. Only you or another person you have authorised, such as a legal guardian or authorised agent, can make the request. Out Doors must be satisfied that the request came from you or a person you authorised.

You may be asked to put your request in writing and for information that identifies you. If so, include:

- your name and contact details
- the personal information you want to access
- how you would like access to the personal information (such as receiving a copy by email or post, or if you just want to look at the information)
- if you authorise a person or organisation to access the personal information on your behalf.

Out Doors can refuse your request if it has reasons to believe that:

- access may endanger the life, health or safety of any individual, or endanger public health or safety
- giving you access would have an unreasonable impact on the privacy of other individuals
- your request is frivolous or vexatious
- your personal information is part of existing or anticipated legal proceedings between you and Out Doors.

Generally, if Out Doors refuses you access to your personal information under Australian privacy law, we must respond to you in writing with the reason for the refusal and where you can make a complaint.

APP 13: Correct your personal information

If you think the personal information Out Doors holds about you is incorrect, please contact us to amend it. Only you or a person you authorise, such as a legal guardian or authorised agent, can request the correction of your personal information.

Out Doors must be satisfied that the request came from you or the person you authorised. You may be asked to put your request in writing or for information that identifies you.

How Out Doors will handle your request?

Out Doors will respond to a request to correct your personal information within a reasonable period. If it is via phone, it can be amended within 48 hours however, if it is via email/mail, it might take up to 14 business days.



Out Doors must consider the reasons your personal information is being held and then take reasonable steps to respond to your request. Reasonable steps may include:

- adding, changing or deleting your personal information
- refusing to correct your personal information because doing so would be unreasonable

Out Doors may have a legal need to keep particular information about you for a certain period and so they may not be able to amend or delete this information during this period.

History

Date	Version	Reason for revision
October 2020	1.0	Issue Version