

Privacy Policy

5 December 2022

Purpose

The purpose of this policy is to outline our privacy practices including how we collect and manage your personal information, why we collect it, how you may access and correct records containing your personal information and how you can make a complaint about the way we have handled your personal information.

In this policy, **you** and **your** refers to any person whose personal information we collect (excluding staff).

Scope

This policy applies to the personal information we collect or handle about people who interact with The Benevolent Society and any entity that is controlled by The Benevolent Society (**we, us, our**).

All Directors, Committee members, staff, contractors and volunteers of The Benevolent Society and any entity that is controlled by The Benevolent Society must adopt practices and actions to ensure compliance with this policy. Any practice or action which results in a deviation to this policy must be reported to the responsible Executive, privacy officer and Group General Counsel as soon as reasonably practicable.

This policy does not deal with personal information relating to staff. Personal information about staff is an “employee record” and will be used in conjunction with the management of staff.

Policy Statements

1. We are committed to respecting your right to privacy. In doing so, we recognise the importance of and are committed to protecting your personal information.
2. We comply with:
 - 2.1. the *Australian Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (**APPs**);
 - 2.2. any contractual obligations relevant to a contracted service provider for a Commonwealth contract or as a NDIS registered provider;
 - 2.3. human rights laws as they relate to and are relevant to us;
 - 2.4. contractual or legislative obligations under relevant state-based privacy laws, where we are a contracted service provider for a State contract; and
 - 2.5. other laws that exist to protect specific types of personal information arising from our service delivery, for example, personal information of children, older people and those who receive our mental health, health and disability services
(Australian Privacy Laws).
3. We take reasonable steps to implement practices, procedures and systems that will ensure we comply with Australian Privacy Laws and to deal with related enquiries and complaints, including mandatory training for all our staff.
4. Australian Privacy Laws require us to include specific matters in this privacy policy. These are addressed and set out in Appendix A below.
5. This privacy policy along with Appendix A constitute the 'Privacy Management Plan' for the purposes of section 33(2) of the *Privacy and Personal Information Protection Act 1998* (NSW).
6. We may, from time to time, review and update this privacy policy to take into account changes in laws and technology, changes to our operations and practices and to ensure it remains appropriate to the changing environment we operate in. We will post the updated version of the policy on our websites.
7. We acknowledge and support your right to complain if you believe your privacy has been breached in any way. The procedure for making a complaint and how we deal with a complaint is outlined in Appendix A below.
8. If you have any queries, concerns or feedback about this policy, you may contact us as follows:

The Benevolent Society
PO Box 257
Broadway NSW 2007
t 02 8262 3400
privacy@benevolent.org.au

Responsibilities and policy owner

- The policy owner is the Board.
- The policy is maintained by the Group General Counsel on behalf of the Board.
- The CEO has overall responsibility for the compliance of this policy.
- The Executive Directors have responsibility for the compliance of this policy in their directorate.

Consultation and approval

The following were consulted in the development of this policy:

- the CEO
- Executive Directors
- Privacy Committee
- Risk, Quality and Safety Committee

This policy has been approved by:

The Board of The Benevolent Society

Appendix A

This section should be read in conjunction with specific privacy collection notices that we have created for people from whom we regularly collect personal information.

1. What is your personal information?

In general terms, personal information is any information about you. If we can't tell that information is about a particular person, e.g. because it has been de-identified, it may not be 'personal information'.

Generally, if the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

2. What personal information do we collect and hold?

We may collect the following types of personal information:

- Name
- Mailing or street address
- Email address
- Telephone number
- Facsimile number
- Age or birth date
- Profession, occupation or job title
- Any information about you that you provide to us through our websites or online presence (e.g. pages you visit, language preferences, your interactions, searches you make).

If you are a client or prospective client (**client**), we may also collect your health information (e.g. details of vaccination status against COVID-19, allergies and/or disabilities, medical reports and names of doctors, information about referrals to and from government and non-government agencies, counseling reports, health care card numbers, health fund details and Medicare number, driver licence details and court orders) and other sensitive information.

If you are a job applicant, volunteer or contractor, we may also collect information on your job application, professional development history, salary and payment information, including superannuation details, medical information (e.g. details of disabilities and/or allergies, medical certificates), and workplace surveillance information. If you are a volunteer or contractor who is given one of our work email addresses, we may also hold information about your use of our ICT resources, including emails and internet use.

For other people who come into contact with us, such as donors, we will collect your personal information as necessary for the purpose of contact with us, or managing your relationship with us.

We record telephone conversations for quality, compliance and training purposes. If you do not wish for your conversation to be recorded, please let our staff know.

3. How do we collect your personal information?

We may only collect your personal information when it is reasonably necessary for, or directly related to, our functions or activities.

In some circumstances we may also collect sensitive information about you when you consent, or when the collection is authorised or encouraged by law or when the collection is otherwise allowed under privacy laws.

How

When collecting personal information from you, we may collect in various ways including:

- through your access and use of our websites and online presence
- during correspondence between you and our representatives, or
- when you complete an application form or purchase order.

Who from

We collect your personal information (and in particular, any sensitive information such as health information and probity checks) directly from you unless it is unreasonable or impracticable to do so.

We may also collect personal information from third parties including from your carer, guardian or authorised representative, government or non-government agencies, law enforcement agencies and medical and/or health professionals who have either worked with you or are currently working with you.

Where we receive information about you from someone else, we will take reasonable steps at the time of or before the time of collection (or as soon as practicable after collection) to let you or your authorised representative know that we have collected your personal information and the circumstances of the collection.

4. What happens if we can't collect your personal information?

If you do not provide us with the personal information we ask for, we may not be able to:

- provide the requested services to you, either to the required standard or at all
- provide you with information about the services that you want
- engage you as our employee, contractor or volunteer
- maintain our relationship with you
- improve our service to meet our clients' needs
- meet our funding, professional and legal obligations
- respond to your complaint
- tailor the content of our websites to your preferences and your experience of our websites may not be as enjoyable or useful.

There are limited circumstances where you can deal with us anonymously or by pseudonym. We will let you know if this is the case, and will provide you with an ID number if it is reasonably necessary.

5. For what purposes do we collect, hold, use and disclose your personal information?

We collect, hold, use and disclose your personal information so that we can provide services to our clients and perform our business activities and functions. This includes keeping our records and your contact details up-to-date, processing and responding to any complaint made by you and complying with any law or a court/tribunal order, or for co-operating with a regulator, authority or government department.

If you are a client or prospective client, we also collect, hold, use and disclose your personal information for the following purposes:

- providing you with information and updates about our services
- assessing your eligibility (or eligibility of a person in your care) for our services and determining how we can best help you
- providing our services to you or the person in your care and in some instances, this will include health services
- researching, monitoring and evaluating our services so we can continue to improve the quality and outcomes of our services as well as develop new services
- advocating for the improvement of service quality and outcomes
- meeting our funding, professional and legal obligations (including our duty of care) in providing you with our services
- processing and responding to any complaint made by you
- providing information to third parties as authorised or required by law
- unless you tell us not to, sending you our newsletters
- unless you tell us not to, sending you information and updates about other services of The Benevolent Society.

If you are a job applicant, volunteer, contractor or donor, we also collect, hold, use and disclose your personal information to establish and maintain our relationship with you and to fulfill our duties under this relationship.

Your personal information will not be shared, sold, rented or disclosed other than as described in this policy.

6. Do we send you direct marketing materials?

We may send our clients, donors and other stakeholders direct marketing communications and information about our services that we consider may be of interest to them. These communications may be sent in various forms, including mail, text message, facsimile and email, in accordance with applicable privacy and marketing laws, such as the Spam Act 2003 (Cth). If you indicate a preference for a method of communication, we will endeavor to use that method whenever practical to do so. In addition, at any time you may opt-out of receiving marketing communications from us by contacting us (see details below) or by using opt-out facilities provided in the marketing communications and we will ensure your name is removed from our mailing list. We do not provide your personal information to other organisations for the purposes of direct marketing.

7. To whom may we disclose your personal information?

We may disclose your personal information to our employees, volunteers, contractors, suppliers, service providers, affiliates, subsidiaries and other related companies and our auditors, funders and regulators, where it is necessary to provide a service to you, establish your eligibility to receive a service from us, manage our relationship with you, and comply with the law.

If you are a client, we may also disclose your personal information to:

- government and/or non-government agencies
- medical and/or other health providers (including members of your treatment team, such as health providers involved in your diagnosis, care or treatment for any particular episode of care)
- external professional individuals or organisations in circumstances where one of our employees is subject to external professional supervision or peer review.

We will only disclose your personal information as set out in this privacy policy and any specific privacy collection notice relevant to your service or engagement with us or to third parties as authorised or required by law or a court/tribunal order. In all other circumstances, we will disclose your personal information only with your prior consent.

8. Do we disclose your personal information to anyone outside Australia?

We do not disclose your personal information overseas unless it's part of a service we provide (such as our post adoption services). Further details can be found in the specific privacy collection notice relevant to your service. We may also disclose your personal information overseas with your consent.

We do use social media platforms such as Facebook and LinkedIn to facilitate our business activities and functions and post about services, employment opportunities and other information about our events and activities. If you choose to interact with us through these services, it is your responsibility to review and accept the privacy policy of that service prior to interacting with us.

9. How do we protect and store your personal information?

We take reasonable steps to ensure your personal information is protected from misuse, interference, loss and unauthorised access, modification or disclosure. We may hold your information in either electronic or hard copy form. Personal information is stored in secured premises or in electronic databases that require passwords and logins. It is our standard practice to destroy or de-identify your personal information once it is no longer needed. If we are required to give your personal information to a person that provides services to us, we will take reasonable steps to prevent unauthorised use or disclosure of your personal information.

10. What are our retention or destruction practices and obligations?

Subject to our retention requirements for health information outlined below, we will only keep personal information for as long as it is needed for any purpose for which it was collected, or otherwise if it is part of a Commonwealth record or is required to be retained under Australian law or by a court or tribunal. All personal information which is no longer needed or required by law to be retained will be properly de-identified or destroyed.

In accordance with the State-based health information protection laws, we are required to retain health information for 7 years after the last occasion on which we provided a health service to an individual, except where the information was collected while the individual was under 18 (in which case, we will keep the records until the individual has reached 25 years of age).

11. What are our websites and online presence privacy practices?

When you access our websites, we may send a 'cookie' (which is a small summary file containing a unique ID number) to your computer. This enables us to recognise your computer and keep track of services you view so that, if you consent, we can send you news about those services. We also use cookies to measure traffic patterns, to determine which areas of our websites have been visited and to measure transaction patterns in the aggregate. We use this to research our users' habits so that we can improve our services. Our cookies do not collect personal information. If you do not wish to receive cookies, you can set your browser so that your computer does not accept them.

We may log IP addresses (that is, the electronic addresses of computers connected to the internet) to analyse trends, administer the websites, track users' movements, and gather broad demographic information.

We will not acquire, use, offer or supply any address-harvesting software or harvested address list (or the right to use them).

Despite all precautions we take to protect your personal information, as our websites are linked to the internet, and the internet is inherently unsecure, we cannot provide any assurance regarding the security of any transmission of

information you communicate to us online. We also cannot guarantee that the information you supply will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which you transmit to us online is transmitted at your own risk.

Our websites may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices.

12. How can you access and correct your personal information?

You may request access to your personal information held by us at any time. The request must be in writing and addressed to our Privacy Officer (or, if you are a job applicant, to HR). You may also authorise another person to access your information on your behalf if, for whatever reason, you are unable to access it yourself. This authority must be in writing and a copy must be provided to us. The authority must name the person whom you authorise to access your information.

Once we have received your request and established appropriate personal identification, we will make available your information to you to inspect within a reasonable period of time (usually 14 days). We endeavour to provide access to personal information in the manner requested by you so long as it is reasonable and practicable to do so (considerations include volume and nature of the information and/or any special requirements).

Unfortunately, there may be circumstances where we cannot grant you access to your personal information. For example, we may refuse access where we reasonably believe that granting access would pose a serious threat to the life, health or safety of an individual or to public health and safety, or have an unreasonable impact on the privacy of another individual or if it would result in a breach of confidentiality. If that happens, we will give you written reasons for any refusal.

If we refuse you access to your personal information on the ground that it would present a serious threat to you or an individual's life or health, then we may provide access through an intermediary (such as a treating medical practitioner) on your request, which may include allowing the intermediary to consider whether access should be provided.

If you believe that the personal information we hold about you is incorrect, incomplete, out-dated or not relevant, then you may request us to amend it. We will consider if the information requires amendment. If we agree to correct the information then, where reasonably practicable, we will notify you of the changes that we have made. If we do not agree that there are grounds for amendment then we will notify you of the reasons for our refusal (to the extent that it is reasonable to do so) and of any available avenues for you to complain about the refusal, where possible. We will also add a note to the personal information stating that you disagree with our refusal to amend.

13. What is the process for complaining about a breach of privacy?

If you have any questions, concerns or a complaint regarding the treatment of your privacy or a possible breach of your privacy, please contact our Privacy Officer. We will contact you within a reasonable time after receipt of your complaint to discuss your concerns and outline options regarding how they may be resolved. We will aim to resolve your complaint in a timely and appropriate manner.

If we fail to respond to a complaint within 28 days of receiving it in writing or if you are dissatisfied with the response that you receive from us, you may make a complaint to the applicable regulator, such as the federal Privacy Commissioner (the OAIC) or the relevant State or Territory privacy commissioner or equivalent regulator.