Privacy Policy

24 November 2025

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 Benevolent staff in the context of an "employee record").

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 (**Benevolent, we, us, our**).

All Board Directors, Committee members, staff, contractors and volunteers of Benevolent and any entity that is controlled by Benevolent 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 Benevolent staff. Personal information about Benevolent staff is an "employee record" and will be used in conjunction with the management of staff and for other purposes as required or permitted by law.

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:
   a. the *Australian Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (**APPs**);
   b. any contractual obligations relevant to a contracted service provider for a Commonwealth contract or as a NDIS registered provider;
   c. human rights laws as they relate to and are relevant to us;
   d. contractual or legislative obligations under relevant state-based privacy laws, where we are a contracted service provider for a State contract; and

e. other laws that exist to protect specific types of personal information arising from our service delivery, for example, personal information of children, older people, carers and those who receive our 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. All staff and volunteers must comply with our Privacy Guide *(internal link accessible through the Hub by Benevolent staff only)*. Our Privacy Guide is an internal document which guides our approach to privacy compliance. Additionally, all staff are required to complete mandatory training at least once per year.

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 website.

7. We recognise the value of Artificial Intelligence (AI) in enhancing our services and improving operational effectiveness. We are committed to the responsible use of AI through clear policy direction, practical guidelines, and ongoing efforts to build organisational capability in how we manage and interact with AI technologies. Before adopting any AI systems, we conduct appropriate due diligence and risk assessments to ensure alignment with our privacy, ethical, and security obligations. Importantly, we prioritise privacy by prohibiting the use, storage, or disclosure of personal information through AI in any public environment. We also only use AI systems in ways that are consistent with our contractual and legal obligations. Our use of AI remains compliant with applicable laws, regulations, and agreements with other parties. Through these measures, we aim to harness the benefits of AI responsibly, while safeguarding the privacy, safety, and trust of the individuals and communities we serve.

8. We do not sell or rent personal information.

9. 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.

10. If you have any queries, concerns or feedback about this policy, you may contact us at:

    Chief Privacy Officer
    The Benevolent Society
    PO Box 257
    Broadway NSW 2007
    t 1800 236 762
    privacy@benevolent.org.au

11. Any employee, volunteer, contractor or other agent of Benevolent who is found to have breached this policy may be subject to disciplinary action, which may include dismissal for serious misconduct or termination for breach of contract.

12. This policy will be made available via the Benevolent intranet policy page and on the Benevolent website. Internal directions, instructions and educational guides are available on the Legal and Corporate Governance Hub (*internal link accessible by Benevolent staff only*).

13. Any queries or uncertainties arising from this policy, including its practical application or any perceived inconsistencies with this or other policies, should be referred to the Group General Counsel, who is authorised to provide guidance and resolve such matters.

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 Safeguarding Committee.

This policy has been approved by:
The Board of The Benevolent Society

Appendix A

1. What is personal information?

In general, personal information refers to any information or opinion that identifies you, or from which your identity can reasonably be determined. If the information does not relate to an identifiable individual, such as where it has been properly de-identified, it may no longer be considered personal information.

In limited circumstances, you may interact with us anonymously or use a pseudonym. Where this is possible and lawful, we will let you know. If necessary, we may assign a reference or ID number to support ongoing communication while protecting your identity.

2. How do we handle your personal information?

We collect and manage personal information to support your engagement with us – whether you're accessing services, applying for a role, volunteering, making a donation, or in another role. This includes handling information to deliver services, build and manage relationships, and meet legal, regulatory and funding obligations.

This section provides a general overview of how we manage personal information across the various groups of people we engage with. It should be read in conjunction with the relevant privacy collection notice that applies to your specific interaction or relationship with us.

Our approach to managing your personal information

(a) We usually collect your personal information directly from you. This may include sensitive information such as health records.
(b) Where direct collection isn't possible, we may collect your personal information from third parties, such as an authorised representative, health professional, government agency, or referring organisation. When we do, we take reasonable steps to let you (or your authorised representative) know how and why your information was collected.
(c) We only use and disclose your personal information in accordance with this policy, relevant collection notice/s and applicable laws which relate to our service delivery and funding arrangements and/or court or tribunal orders. Otherwise, we will seek your consent.
(d) We do not routinely disclose your personal information to overseas recipients however there may be certain interactions where your personal information is disclosed outside Australia such as:
    i. to facilitate the provision of a service you have requested or agreed to e.g. post-adoption services;
    ii. when you engage with us through social platforms which store personal information overseas; or
    iii. when you have explicitly requested us to communicate to you through a platform which stores personal information overseas.

In these situations, we cannot ensure that overseas organisations handle your information according to the Australian Privacy Principles. By providing your consent (which we will seek where the disclosure relates to service delivery, or which will be deemed given if you initiate the interaction on a platform that stores personal information overseas) to the disclosure, you acknowledge and accept that we won't be accountable under Australian Privacy Principle 8.1 for how that information is handled by the overseas recipient.

(e) Our support centre may record telephone conversations for quality, compliance and training purposes. You can request not to be recorded by informing our staff.

How we manage personal information by stakeholder group

Who you are	What personal information we collect and hold	How we collect it	Who we collect from	Why we collect it (purpose)	Who we share it with	What happens if you don't provide it?	Do we send you direct marketing?
Clients (prospective or current)	Name, contact details, date of birth, employment information, health and service history and other details required to provide you with specific services	Forms, interviews, referrals, correspondence, service visits	From you and/or authorised representatives (e.g., powers of attorney, guardian, carer or next of kin) and/or third parties (e.g., government, non-government agencies, health service providers)	To assess eligibility, deliver services, ensure safety and meet legal/funding requirements	Staff, volunteers, contractors, authorised representatives, other third parties (health providers, government, non-government agencies), funding bodies, external supervisors, accreditation agencies, regulators, authorities	We may not be able to provide or tailor services, respond to your concerns or meet legal obligations	Depends – refer to the client privacy collection notice and your specific circumstances. Please refer to your Benevolent contact, if you would like further information.
Job Applicant	Name, contact details, qualifications, work history, salary and superannuation information, probity and screening	Information collected through application, interviews, screening, reference checks onboarding forms	From you and/or third parties e.g. government agencies for probity and screening checks and referees for reference checks	To assess suitability and manage the recruitment process	Staff, volunteers, contractors and other third parties such as insurers, brokers, government agencies,	We may not be able to consider or progress your application	No

Who you are	What personal information we collect and hold	How we collect it	Who we collect from	Why we collect it (purpose)	Who we share it with	What happens if you don't provide it?	Do we send you direct marketing?
	checks, health checks (as needed)				regulators, authorities		
Volunteers	Name, contact details, qualifications, work history, probity and screening checks, health checks (as needed) IT usage (if work email assigned)	Information collected through application, interviews, screening, reference checks, onboarding forms	From you and/or third parties e.g. government agencies for probity and screening checks and referees for reference checks	To assess suitability and manage your engagement, ensure compliance and safety	Staff, volunteers, contractors and other third parties such as insurers, brokers, government agencies, regulators, authorities, funding bodies	You may not be able to volunteer with us	No
Contractors	Name, business name, contact details, qualifications, insurance, compliance checks, IT usage (if work email addressed)	Due diligence enquiries and forms, contracts	From you and/or third parties e.g. government agencies for probity and screening checks and referees for reference checks	To assess suitability for engagement and manage contracts and meet legal requirements	Staff, volunteers, contractors and other third parties such as insurers, brokers, government agencies, regulators, authorities, funding bodies	We may not be able to engage you	No
Donors/Supporters	Name, contact details, donation records, communication preferences	Donation forms, events, online platforms	From you	To process donations, issue receipts, provide updates	Staff, volunteers, contractors, regulators, authorities	We may not be able to acknowledge your donation or issue receipts or in rare circumstances, accept your donation.	Yes, unless you opt out. We respect your preferences.
Visitors	Name, contact details, time of visit, purpose, surveillance	Sign-in sheets, sign-in systems, surveillance system	From you or a person you authorise to sign you on your behalf	To manage safety, security and compliance with	Staff, volunteers, contractors, regulators, authorities	You may be refused entry	No

Who you are	What personal information we collect and hold	How we collect it	Who we collect from	Why we collect it (purpose)	Who we share it with	What happens if you don't provide it?	Do we send you direct marketing?
	footage, health information (as needed)			workplace or public health requirements			

3. 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.

4. 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. We have a clear policy to retain personal information only for as long as necessary to fulfil the purpose for which it was collected.

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).

5. 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.

6. 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 from you 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). Sometimes it may take longer because of the age and/or volume of records, in which case we'll inform you beforehand. 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.

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

If you have questions, concerns, or a complaint about your privacy or a possible breach, please contact us at privacy@benevolent.org.au. We'll respond within a reasonable time to discuss your concerns and explain your options. Our goal is to resolve complaints promptly and appropriately.

If we don't respond within 28 days, or if you're not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC). Depending on your situation, you might also be able to complain to another regulator or government agency. We will assist you in identifying the right authority if needed.