Being | Mental Health & Wellbeing Consumer Advisory Group

Privacy Policy

Document Number	
Version	v1.4
Date of Publication	September 2018
Date of Review	[May] 2019

Background

Being respects your right to privacy and is committed to safeguarding the privacy of our members, customers, those who seek and engage in the provision or receipt of our services and those who visit our website.

This privacy policy outlines our Personal information handling practices 'Personal information' is information we hold which is identifiable as being about you. We recognise and value the trust that individuals place in us when providing us with Personal information and we are committed to safeguarding the privacy and security of the Personal information we collect.

Being has opted in to be bound by the provisions of the *Privacy Act* 1988, including the Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for how we handle and maintain Personal information. This includes how we collect, store, use, disclose, quality assure and secure Personal information, as well as your rights to access or correct your Personal information. The specific legal obligations that apply to us when collecting and handling your Personal information are outlines in the Privacy Act 1988 and in particular in the APPs found in that Act. We will update this privacy policy when our information handling practices change.

Please read this policy before submitting any Personal information (whether via our websites, by email, in person or over the phone). By using our services, you will be asked to provide Personal information and, by doing so, you are accepting and consenting to the practices described in this policy. Further notices highlighting certain uses we wish to make of your Personal information, together with the ability to opt in or out of selected uses will also be provided to you when we collect Personal information from you. If we are not able to collect your Personal information, we may not be able to provide you with our services or do business with you or the organisation with which you are connected.

If you link to or use other websites, services or software, please review the privacy policies posted at those websites. This policy does not apply to, and we are not responsible for, any third-party websites which may be accessible through links from this website. If you follow a

link to any of these third-party websites, they will have their own privacy policies and you will need to check these policies before you submit any Personal information to such third party websites.

This policy outlines:

- Being's obligations
- What constitutes Personal information
- How Being can collect, store, use or disclose Personal information in the course of providing services
- Steps in response to a notifiable data breach

Scope

This policy applies to all members, employees, lived experience representatives, volunteers, students on placement, contractors and Directors of Being. This policy also applies to all visitors to our website, people accessing services provided by Being, and suppliers.

Definitions

Privacy is the protection of an individual's personal and/or sensitive information.

Confidentiality is a guideline or procedure that limits access or places restrictions on personal and/or sensitive information.

Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

Personal information is information which directly or indirectly identifies a person such as, but not limited to a person's name, postal or email address, date and place of birth, image and financial details.

Sensitive Information is a subset of Personal information and includes but is not limited to information or an opinion about a person's racial or ethnic origin, political opinions, religious beliefs or affiliations, memberships of a professional or trade association or union, sexual preferences, criminal record or health information.

Australian Privacy Principles

1. Sensitive Information (APP 10) – Individuals and other stakeholders

Under the APPs, health information is considered "sensitive" information. As a representative organisation for people with lived/living experience of mental health services, Being holds sensitive information and is committed to ensuring the safety, confidentiality and protection of that information in accordance with the Act and this policy, as expanded on below.

2. Collection (APP 1)

Being only collects Personal information where that information is reasonably necessary for, or directly related to, one or more of our functions or activities or when Personal information is volunteered by you and given to us. Being tries to only collects information necessary to provide individuals and the community with our services.

You are not obliged to give us your Personal information. The main way we collect Personal information about you is when you give it to us. However, if you choose not to provide us with your Personal information we may not be able to provide you with our services or fulfil one or more other purposes for which your Personal information is requested.

Being will only collect sensitive information (such as health information) if you consent to doing so and it is reasonably necessary for, or directly related to, one or more of our functions or activities. We will not collect any Personal information if we do not need it. Applications for General Membership are limited to persons who have lived/living experience of mental health services

Being may collect Personal information directly from you, your representative or a third party. We primarily collect information directly from you or another individual, but in certain circumstances we may also obtain Personal information collected by other organisations. If your Personal information is collected by us from a third party, Being is under no obligation to inform you of the collection, but such information will be subject to this policy and will be accessible by you on request, subject to any limitations or exceptions in the Act.

Being collects Personal information in a variety of ways, including paper-based forms such as membership application, online (through our website as well as email), over the telephone and by fax. When you visit our website, we record, for statistical purposes or in order to improve the website or our service delivery, the following information:

- the date, length and time of your visit;
- web pages you have accessed;
- documents you have downloaded;
- your IP address;
- the features you use;
- the links you click on; and
- the type of operating system and internet browser you use.

From time to time we use cookies on our website. Cookies are very small files which a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies, but you can choose to reject cookies by changing your browser settings. However, this may prevent you from taking full advantage of our website.

The Kinds of Personal information that we hold

Being only collects Personal information that is necessary for, or directly related to its functions or activities. It may include:

- personal contact details
- organisational membership and consumer disclosures
- personnel/employee records including educational qualifications
- complaint and feedback information
- financial payment records
- contract, tender and submission documents
- litigation and compensation records
- grants information
- employee conflict of interest declarations
- mailing and subscription lists.

We may also collect and hold a range of sensitive information, including:

- health information – where you provide details of your medical history to us (such as in a submission to a review we are conducting) or the health information of staff (such as rehabilitation and compensation case files, next of kin or details of disabilities or injuries);
- racial or ethnic origin – of staff members for reporting purposes, or
- criminal records – as part of pre-employment screening.

When Being collects sensitive information, it is usually collected with the consent of the individual concerned. In limited circumstances we may collect sensitive information from a third party or if it is authorised under an Australian law. If sensitive information about an individual is collected from another source, reasonable steps will be taken in the circumstances to notify the individual of the circumstances of the collection.

3. Use and Disclosure (APP 2)

Being only uses or discloses Personal information for the purpose for which it was collected and where we are permitted to do so by law. We will not give your Personal information to anyone else unless you consent in ways which have been made explicit or if one of the following exceptions applies:

- you would reasonably expect us to use the information for that other purpose
- it is legally required or authorised, such as by an Australian law, or court or tribunal order
- we reasonably believe that it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety
- we have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being or may be engaged in and we reasonably believe that it is necessary in order for us to take appropriate action in relation to the matter
- it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim
- it is reasonably necessary for the purposes of a confidential dispute resolution process.

We use Personal information collected from you to provide you with information, updates, support and our services. We may also make you aware of new and additional products, services and opportunities available to you.

We may use your Personal information to improve our products and services and better understand your needs, to enforce this policy and to exercise our legal rights. Below are the principal legal grounds and purposes for which we use the information we collect about you:

- to provide access to our website and our services and personalise your experience
- to answer your enquiries and deliver customer support
- to communicate to you about our services
- to market, promote and drive engagement with us and our services that we think might be of interest to you
- to maintain and improve our website and our services
- to meet our legal and regulatory obligations and protect our legitimate business interests and legal rights
- to promote safety and security
- to undertake activities for which we have obtained your consent

We use a variety of measures to contact individuals, including, but not limited to telephone, email, SMS or mail.

Being is occasionally approached for consumer opinions by external parties. Being will in all cases contact you first on the third party's behalf and only pass appropriate referral information back to that third party if you consent.

Being represents views and opinions of persons with lived/living experience. When it does so it is done with the express consent from that person to be named as someone with a lived experience of mental illness. You have the right to have your view represented by Being anonymously.

The Being Constitution provides that all members of Being are able to access the database of Being's membership. This database contains only initials, suburb together with the date on which membership commenced, and the date of cessation. All other information will be kept confidential and not shared with any third party or organisation. Any requests for inspection of the membership database will be assessed on a case by case basis to ensure compliance with this policy.

Exceptions

The *Privacy Act 1988* has two important groups of exceptions: '**permitted general situations**' and '**permitted health situations**', where the collection, use or disclosure of Personal or sensitive information without consent will not be a breach of specified legislative obligations.

Examples of these permitted situations include:

- serious threats to life, health or safety of an individual, or to public health and safety
- suspected unlawful activity or serious misconduct
- locating missing persons
- disclosure to a responsible person where the patient of a health service cannot give consent
- collection required to provide a health service
- collection and use or disclosure for research
- disclosure under a court order, valid subpoena or other enforceable legal obligation, for example the reporting of concerns regarding children at risk under child protection laws.

Permitted situations are subject to it not being reasonably practical to get the permission of the person concerned and may require the disclosing organisation to also comply with guidelines issued by the Information Commissioner or other bodies.

Where Being is required to disclose Personal information to others under a court order, subpoena or other enforceable legal obligation, and the person concerned does not know about it, Being will take reasonable steps to let the person concerned know, unless Being is required not to do so.

4. Data Quality (APP 3)

Being will take all reasonable steps to ensure that the Personal information we collect, use or disclose is as accurate and as current as possible. This includes correcting your Personal information where it is appropriate to do so.

To ensure that the Personal information we collect is accurate, up-to-date and complete we:

- record information in a consistent format
- where necessary, confirm the accuracy of information we collect from a third party or a public source
- promptly add updated or new Personal information to existing records
- regularly audit our contact lists to check their accuracy.

We also review the quality of Personal information before we use or disclose it.

5. Data Security (APP 4)

Being will take all reasonable steps to ensure that all Personal information is kept safe and secure. Being takes reasonable steps to protect Personal information from misuse, loss, unauthorised or unnecessary access, alteration or disclosure.

Being stores all Personal information securely and restricts access to those employees who need access in order to perform their duties or to assist individuals. In general, Personal information is stored electronically in record keeping systems, on hard drives or in emails.

When Personal information is no longer required, we delete or destroy it in a secure manner, unless we are required to maintain it because of a law, or court or tribunal order.

6. Openness (APP 5)

Being's Privacy Policy is available to anyone who requests it and can be obtained from our website on www.being.org.au, or by calling 02 9332 0200.

Being has a Complaints policy for anyone who believes their information is not being handled properly or in accordance with this policy. A copy of Being's complaints procedure may also be obtained through the website at www.being.org.au or by calling on 02 9332 0200.

7. Access and Correction (APP 6)

Access to Personal information can only be done by staff in the performance of their duties or specifically at the request of the individual to whom the information relates subject to the below.

You also have a right to access Personal information we hold about you and have rights under the *Privacy Act* to request corrections to any Personal information that we hold about you if you think the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. We will ask you to verify your identity before we give you access to your information or correct it, and we will try to make the process as simple as possible. If we refuse to give you access to, or correct, your Personal information, we must notify you in writing setting out the reasons.
There is no charge associated with making a request and notification of the outcome will be provided, in most cases, within 30 days. For security reasons, and to protect other person's privacy, applicants may be asked to provide proof of their identity.

To access Personal information, a written request should be sent to Being by email at info@being.org.au.

We can decline access to, or correction of, Personal information under circumstances set out in the *Privacy Act*. Generally, where we refuse to give you access, we will give you written notice of the reasons for refusal and the mechanisms available to you to dispute that decision.

8. Identifiers (APP 7)

Being does not use identifiers or reference numbers assigned by other organisations or government departments or services.

Being assigns its own identifiers or references to Personal information records such as database numbers for newsletter mail outs.

9. Anonymity (APP 8)

You will generally be able to remain anonymous or use a pseudonym when interacting with Being. However, it may not always possible for this to occur—for example, when we are authorised or required under the law to deal with individuals who have identified themselves. We will inform you if you are unable to remain anonymous or use a pseudonym when dealing with us.

10. Trans-border Data Flows (APP 9)

Being will only send Personal information to a third party in a foreign country with prior consent from the person the information relates to or if the information has protection substantially similar to the Australian Privacy Principles outlined in the Act. We will also take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

Confidentiality

Confidentiality is the assurance that all written, verbal and electronic information is protected from access and use by any unauthorised person. With respect to confidentiality, Directors, members, employees, lived experience representatives, volunteers, students and contractors must note that disclosure or misuse of confidential information held by Being may constitute a criminal act, and could also be subject to civil action by an individual or group.

Employees, Board members, volunteers, contractors and students are required to sign a *Privacy and Confidentiality Agreement* on commencement of service, agreeing to maintain the confidentiality of individuals, employees, volunteers and business operation issues of the organisation. A copy of the agreement will be kept in the personnel file.

Eligible Data Breach

Being is committed to protecting privacy in accordance with the Guide to securing personal information issued by the OAIC.

While every effort is made to secure information transmitted to us over the internet, there is a possibility that this information could be accessed by a third party while in transit. Australian laws provide that an eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of Personal information, or a loss of Personal information, that we hold;
2. this is likely to result in serious harm to one or more individuals; and
3. we have not been able to prevent the likely risk of serious harm with remedial action.

Being is required to take all reasonable steps to ensure an assessment of an eligible data breach is completed within 30 days. If an eligible data breach is confirmed, as soon as practicable we must provide a statement to each of the individuals whose data was breached or who are at risk, including details of the breach and recommendations of the steps individuals should take. A copy of the statement must also be provided to the Office of the Australian Information Commissioner.

Some examples of data breach include:

- Lost or stolen laptops, portable storage devices, or physical files containing Personal information. Paper records inadequately recycled or left in garbage bins.

- Mistakenly providing Personal information to the wrong person, for example by sending details out to the wrong address.
- Employee's accessing Personal information outside the requirements or authorisation of their employment.
- Computer hard drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without erasing contents.
- Databases containing Personal information being hacked into or otherwise illegally accessed by individuals outside of Being.
- An individual deceiving an agency or organisation into improperly releasing the Personal information of another person.

In the event of a notifiable data breach, Being is guided by legislation and the Office of the Australian Information Commissioner's information on its website at: www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

Complaints

All reports of privacy breaches will be treated seriously and promptly with sensitivity and complete confidentiality.

If you wish to make a complaint you should provide sufficient detail so the issues and concerns can be investigated.

If you are not satisfied with the outcome of an investigation, a complaint can be submitted to the Office of the Australian Information Commissioner (OAIC). Further details about making a privacy complaint to the OAIC can be found at www.oaic.gov.au/privacy/making-a-privacy-complaint.

Breach of this Policy

Directors, members, employees, lived experience representatives, volunteers, students on placement and contractors should note that breaches of this policy may be a breach of the *Code of Conduct*.

Breaches of the *Code of Conduct* may lead to disciplinary action, loss of membership for members, disciplinary action or dismissal for employees, or cessation of work for volunteers, lived experience representatives, students on placement and contractors.

Changes to Privacy Policy

Please be aware that we may change this policy in the future, in our sole discretion and all modifications will be effective immediately upon our posting of the modifications on our website. Please check back from time to time to review our policy. Where required by applicable law, we will obtain your consent.

Being | Mental Health & Wellbeing Consumer Advisory Group

Related Documents

- Australian Privacy Principles www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
- Data breach notification — A guide to handling Personal information security breaches www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches
- Code of Conduct
- Commonwealth Privacy Act 1988 www.oaic.gov.au/privacy-law/privacy-act/
- Complaints Policy
- Information (Public Access) Act 2009 (previously the Freedom of Information Act 1989) www.legislation.nsw.gov.au/acts/2009-52.pdf
- Privacy and Confidentiality Agreement

Review

This policy will be reviewed annually or as required.

Contact Details

For any questions about Being's Privacy Policy contact the office by telephone on: 02 9332 0200 or e-mail info@being.org.au

Copies of the Privacy Policy can be downloaded from Being's website at: http://www.being.org.au

The Office of the Federal Privacy Commissioner's website contains detailed information on privacy obligations including a copy of the Privacy Act http://www.privacy.gov.au.