



PRIVACY & CONFIDENTIALITY POLICY

Related Documents

Document	Name
Policy	
Our Voice Our Choice Pty Ltd Privacy and Compliance Policy	Privacy Policy
Our Voice Our Choice Pty Ltd Code of Conduct	Code of Conduct
Documents	
Australian Privacy Act 1988 (Cth)	https://www.legislation.gov.au/Details/C2020C00168
Health Records and Information Privacy Act 2002	https://www.legislation.nsw.gov.au/#/view/act/2002/71
Procedures / Manuals	
Forms	

Document history

Version/s	Approval	Version Date	Review Date	Comments
1.0	Kyle Prasser – Chief Operating Officer	June 2020	June 2021	Original March 2021
			June 2022	Reviewed 06/05/2022

1. Purpose

At Our Voice Our Choice (**OVOC**), we recognise the importance of your privacy and understand your concerns about the security of the personal information you provide to us.

This policy ensures we protect and handle personal information in accordance with the National Disability Insurance Scheme (**NDIS**) and relevant privacy legislation.

We are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework, and comply with

- the Australian Privacy Principles (**APPs**) as contained in the Australian *Privacy Act 1988* (Cth); and
- the NSW Health Privacy Principles (**HPPs**) as contained in the *Health Records and Information Privacy Act 2002* (**HRIP Act**).

The APPs detail how personal information may be collected, used, disclosed, stored and destroyed, and how an individual may gain access to or make complaints about the personal information held about them. The HPPs outline the legal obligations which OVOC must abide by when it collects, holds, uses and discloses a person's health information.

We acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality.

Personal information is information or an opinion about an identified individual, or about an individual who is reasonably identifiable.

Sensitive information, a sub-set of personal information, is information or an opinion about an individual's racial or ethnic origin, political opinions, political association membership, religious beliefs or affiliations, philosophical beliefs, professional or trade association membership, trade union membership, sexual orientation or practices or criminal record, and includes health information and genetic information.

Health information, regarded as one of the most sensitive types of personal information, is information or an opinion about an individual that involves:

- assessing, maintaining or improving a person's physical, mental or psychological health or disability, including an individual's express wishes about the future provision of health services to him or her;
- where a person's health cannot be maintained or improved – managing the person's physical or psychological health, diagnosing or treating a person's illness, disability or injury;

- recording a person's physical or psychological health for the purposes of assessing, maintaining, improving or managing the person's health or dispensing a prescription drug or medicinal preparation by a pharmacist;
- a health service provided, or to be provided, to an individual;
- other personal information collected to provide, or in providing, a health service;
- other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances;
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual; or
- a healthcare identifier.

This policy details how OVOC manages personal information about you.

2. Applicability

This policy applies to:

- all personal information, sensitive information and health information including the personal information of participants in our NDIS services; and
- the conduct of all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

3. Privacy and Confidentiality commitment

- We are fully committed to complying with the privacy requirements of the Privacy Act, the Australian Privacy Principles and for Privacy Amendment (Notifiable Data Breaches) as required by organisations providing disability services
- We are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework
- We provide all individuals with access to information about the privacy of their personal information
- Individuals have the right to request access to their personal records by requesting this with their contact person
- Where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality
- Personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued).

4. Guidelines

4.1 What personal information we collect and hold

The kinds of personal information we collect from you or about you depends on the services you have engaged with us to provide, and the services you are interested in.

The kinds of personal information that we commonly collect and hold from you or about you include: your name, address, phone number, email address, date of birth, bank account details, drivers licence, and recorded opinions or notes in relation to or about you.

The kinds of sensitive information that we commonly collect and hold from you or about you include: your NDIS number, your health information, ethnicity, religious beliefs or affiliations, sexuality and criminal record.

The kinds of health information that we commonly collect and hold from you or about you include: your Diagnoses (including physical and mental health assessments), Medication Prescriptions and your Treatment and Support Plans, including Allied Health.

Where appropriate, we may seek your consent to capture your images or video footage of you. Images or video footage will be not be used without your consent.

4.2 Cookies and our website

When you browse our website or contact us electronically, we record: geographical tagging and statistical data from your activity including your computer system internet address, your top level domain name (for example .com, .gov, .au, .uk etc), the date and time of your visit to the site, the pages you accessed and documents downloaded, the previous sites you have visited and the type of browser you are using. Note that none of the statistical information we collect allows us to identify a visitor to our website. The information we collect from your visit to our website is used by us to help administer and improve the website.

We use cookies to collect non personal information, and anonymous information about visits to our website and to track how you reached our website. Cookies are small text files placed on your hard drive by website hosts. Cookies recognise a repeat visitor to its site and enable sites to store information on the user's computer so that the information can be referenced later. You will be given the option to disable cookies when you visit our website, but this may prevent proper functionality of the website. In particular, you may not be able to store your preferences, and some of our pages might not display properly. If you'd like to delete cookies or instruct your web browser to delete or refuse cookies, please visit the help pages of your web browser.

Note that our website does not have facilities for the secure transmission of emails. If you are concerned about the security of any personal information you submit by email, please contact us using an alternative method (eg. telephone, fax, secure post or encrypted message).

Our website may also contain links to other websites of interest. However, once you have used those links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites, and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website/s in question.

4.3 How we collect and hold personal information

We aim to collect personal information only directly from you, unless it is unreasonable or impracticable for us to do so. For example, we collect personal information from you or about you from correspondence that you submit to us, forms that we ask you to complete and provide to us, meetings and interviews with us, telephone calls with us and submissions you make on our website.

Where any personal information that we collect relates to sensitive information or health information, we will obtain your consent to collect this information.

In some instances, we may receive personal information about you from third parties, such as associated businesses or government agencies. We may also receive personal information about you from your family members, authorised third parties and publicly available sources.

You can be anonymous or use a pseudonym when dealing with us, unless:

- the use of your true identity is a legal requirement; or
- it is impracticable for us to deal with you on such basis.

4.4 Why we collect, hold, use and disclose personal information

We collect, hold, use and disclose personal information from you or about you where it is reasonably necessary for us:

- to carry out and provide our services to participants, which enables a safe and healthy environment with individual requirements;
- to meet our duty of care obligations;
- to initiate appropriate referrals; and
- to conduct business activities to support those services.

We also collect, hold, use and disclose your personal information for related purposes that you would reasonably expect.

We may also disclose your personal information to third parties (including government departments and agencies, enforcement bodies and professional registration and accreditation bodies etc) where required or permitted by law. Where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language and nationality. Where OVOC is required to engage a third party for an external NDIS audit, you can participate if you wish.

If we do not collect, hold, use or disclose your personal information, or if you do not consent to the provision of such information, then we may not be able to provide the services that you or your organisation have engaged us to provide.

4.5 How we hold and store personal information

Your personal information is held and stored on paper, by electronic means or both. We have physical, electronic and procedural safeguards in place for personal information and take reasonable steps to ensure that your personal information is protected from misuse, interference and loss, and from unauthorised access, modification and disclosure. We have implemented a hierarchy based system to ensure that the personal information that we collect and hold about you is only accessible on a needs to know basis.

Data held and stored on paper is stored in lockable filing cabinets in locked rooms with secure keys. Our premises has secured entry and monitored alarms. Data held and stored electronically, including “in the Cloud”, is protected by internal and external firewalls, limited access via file and network passwords, and files can be designated read-only or no access. We also require our IT contractors and other third parties to implement privacy safeguards.

4.6 Destruction and De-identification

We will retain your personal information whilst it is required for any of our business functions, or for any other lawful purpose.

We will take reasonable steps and we will use secure methods to destroy or to permanently de-identify your personal information when it is no longer required for any purpose for which the personal information may be used under this Policy and otherwise in accordance with the Privacy Act.

As an example, our destruction and de-identification methods may include:

- Paper records being placed in security bins and/or shredded.
- Electronic records being deleted from all locations, to the best of our ability, or encrypted and/or placed beyond use.

4.7 Overseas disclosure

OVOC does not disclose your personal information overseas. If the need does arise to disclose your personal information overseas, we will seek your consent prior to the disclosure.

4.8 Requests for access and correction

We will take reasonable steps to ensure that the personal information we use or disclose is accurate, complete and up to date, having regard to the purpose of the use or disclosure.

We rely on the personal information we hold about you to efficiently provide our services. For this reason, it is very important that the personal information we collect from you is accurate, complete and up-to-date. To assist us to keep our records up-to-date, please notify us at admin@ovoc.com.au of any changes to your personal information.

We have procedures in place for dealing with and responding to requests for access to, and correction of, the personal information held about you.

In most cases, we expect that we will be able to comply with your request. However, if we do not agree to provide you access or to correct the information as requested, we will give you written reasons why. For further information, please contact us at admin@ovoc.com.au.

4.9 What is a data breach?

A data breach is type of security incident where personal or sensitive information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people affected by the data breach are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner.

In Australia, if we suspect that a data breach has occurred, we will undertake an assessment into the circumstances of the suspected breach within 30 days after becoming aware of the occurrence of the suspected breach. Where it is ascertained that a breach has actually occurred and where required by law, we will notify the Privacy Commissioner and affected individuals in accordance with our legal requirements.

5. Contact

Our Privacy Officer can be contacted to discuss or attempt to resolve any complaints relating to the collection, storage, use and disclosure of your personal information.

For further information, please contact our Privacy Officer as follows:

Privacy Officer

Our Voice Our Choice

PO Box 2110

East Maitland

T: 02 4058 3358

E: admin@ovoc.com.au