



### PURPOSE

To describe OC Connections' approach to handling personal and sensitive information, in order to maintain individual privacy and confidentiality. This will uphold the rights of OC Connection's participants and staff; and ensure compliance with Australian law and best practice.

### SCOPE

This policy applies to all OC Connections Board members, Staff, Students, Volunteers and Contractors for the benefit of all, including participants.

### POLICY STATEMENT

OC Connections is committed to protecting and upholding people's right to privacy, dignity and confidentiality.

In line with the Australian Privacy Act 1988 (the Privacy Act), Australian Privacy Principles (APP) and NDIS Practice Standards, OC Connections will:

- manage personal information in an open and transparent way
- make available our policies on management of personal information, free of charge and in each individual's preferred method of communication
- provide individuals with the option of being anonymous or using a pseudonym, where it is lawful and practical
- only request and collect personal information that is directly relevant to its' primary purpose
- gain individual consent before collecting sensitive information
- not use or disclose personal information except for:
  - the purpose for which it was collected
  - a related purpose which would be reasonably expected
  - a purpose required or permitted by law
  - where the individual has consented
- take all reasonable steps to protect and safeguard personal information collected
- provide individuals with access to their personal information, except where required or entitled by law to refuse access
- tell individuals if their privacy has or may have been breached and explain what is being done to deal with the breach
- ensure that personal information is accurate, complete, and up to date. If information is found to be incorrect or incomplete it will be corrected as soon as possible



- take steps to destroy personal information if it is no longer needed for any purpose as per the *Document Retention and Disposal Policy*

## REASONS FOR COLLECTING PERSONAL INFORMATION

We collect, hold, use and disclose personal information for the following purposes:

- providing and improving our services and functions to participants
- contacting and communicating with workers, participants, their families and carers
- worker recruitment and retention
- conducting our business
- promoting our organisation
- complying with our legal obligations

## COLLECTING PERSONAL INFORMATION

We will only collect personal information, including sensitive information, if it is necessary for us to do so. We usually collect personal information directly from the person who the information is about. This can be in person, via post, or by interacting with us through OC Connections' website (for example, by submitting a message or comment, participating in an online survey, or subscribing to our newsletters or mailing lists).

There may be occasions where we collect personal information from log files and cookies via our website, or via a third party. Where we do so, we will ensure that this information is collected in accordance with our obligations under the Privacy Act.

When we collect personal information, we will take reasonable steps to inform the individual concerned of:

- who we are and our full contact details
- the purpose of collecting the personal information
- who we may disclose or transfer that personal information to
- any law which requires us to collect the personal information
- the main consequences if the personal information requested by us is not provided

## TYPES OF PERSONAL INFORMATION

The types of personal information we normally collect and hold include, but are not limited to:

- name, date of birth, telephone number, email and mailing address
- information necessary to provide safe and quality supports, for example health matters, personal preferences



- other personal information that individuals choose to share with u
- messages or comments emailed to us such as general and specific support related inquiries
- subscriptions to our blog, newsletter and mailing list
- information held in PLC files
- information collected when participating in an online survey
- information provided when completing a website enquiry form

## CONSENT

OC Connections will gain an individual's written consent to collect, hold and disclose sensitive information. We will make sure that:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

If an individual does not have capacity to give consent, even with additional support or resources, a nominee or guardian can provide written consent. Individuals will still be involved, as much as possible, in any decision-making process.

Individuals have the right to withdraw their consent at any time. Once consent has been withdrawn, OC Connections will not use past consent for future use or disclosure of personal information. Individuals will be informed of potential consequences of withdrawing consent, such as no longer being able to access a service.

## USING AND DISCLOSING PERSONAL INFORMATION

We may need to disclose personal information to government agencies, other organisations, or individuals. Where possible we will gain individual consent and deidentify personal information before disclosing it.

In certain circumstances, we may need to disclose personal information without consent, for example:

- where disclosure is required or authorised by law e.g. legal proceedings.
- where it is necessary to prevent or lessen serious threat to the life or health of the person we support, worker or another person.



If we are provided with information that we did not request, we will only store and use it if it is necessary to do so. We will not release this information to any third party without the written consent of the individual or their nominee/guardian.

All use and disclosure of personal information complies with the Privacy Act, APP's and our policy.

## ACCESSING OR CHANGING YOUR PERSONAL INFORMATION

### Access

Individuals have a right to request access to the personal information held about them. An administrative fee may be payable for the provision of personal information. In certain circumstances we might refuse access to personal information for reasons detailed in the Privacy Act.

### Correction

Individuals can request a change/correction to personal information we hold about them, if they believe it is inaccurate, out of date, incomplete, irrelevant or misleading.

We will respond to requests within 14 days of the request date. In situations where the request is complicated or requires access to a large volume of information, we will take all reasonable steps to provide access to the information requested within 30 days.

We will endeavour to promptly correct any information that is found to be inaccurate, incomplete or out of date.

## INFORMED CONSENT

In situations where a participant is unable to provide informed consent regarding the collection, storage, accessibility and disposal of their personal information, a family/carer/nominee or advocate must be contacted to assist the person through this process. Refer to the Advocacy Policy for more information.

## SURVEILLANCE ACTIVITIES

OC Connections may operate surveillance cameras to monitor people movement in, out or around our sites. Surveillance cameras are restricted to common areas and are not installed in participant areas without consent from participants and/or their family/carers/nominees or advocate.

The surveillance recordings, including personal information held on those recordings may be provided to law enforcement bodies or other third parties where required by applicable law or where considered it is reasonably necessary for the purposes set out in this policy.



### COMPLAINTS

If you believe that we have breached the Privacy Act and you wish to make a complaint, please contact us. In the event a complaint is received regarding a breach of privacy, the complaint will be reported to the Manager Quality and Risk and investigated and responded to by the relevant department representative within 5 business days of receipt.

If you are not satisfied with the resolution of your complaint by us, you can complain about a privacy matter to the Australian Information Commissioner (<https://www.oaic.gov.au/>).

### CONTACT DETAILS

<b>Name</b>	Manager Quality and Risk
<b>Address</b>	OC Connections Limited (ABN: 91480733899) 773 Warrigal Road, Oakleigh, Victoria 3166 (PO Box 127 Oakleigh VIC 3166)
<b>Email</b>	privacy@oconnections.org
<b>Phone</b>	(03) 9569 0603
<b>Postal address</b>	PO Box 127, Oakleigh 3166

### RESPONSIBILITIES

#### Board of Directors

OC Connections Board is responsible for, and committed to complying with all applicable laws, and requires that all workers and Board members act within the law at all times in the course of their duties for the organisation.

#### Chief Executive Officer

The CEO is responsible for monitoring legal compliance as delegated by the Board. The CEO is responsible for

- reporting any breach of procedure related to legal requirements
- overseeing any investigation
- determining whether specific auditing of compliance in a particular area is required
- reporting (as required) to the Board on the compliance status

#### Executive

The Executive are responsible for:

- the implementation of OC Connection's Compliance policy where relevant to their role



- fostering a compliance culture where breaches are effectively identified and reported
- ensuring all workers are aware of this policy and how it relates operationally.
- intervening promptly and appropriately when they become aware of a breach of this policy
- fostering a culture of continuous improvement

### Staff, Students, Volunteer and Contractors

Staff, students, volunteers and contractors must comply with all compliance policies and procedures. They also have daily responsibility for implementing compliance controls and identifying non-compliance.

### DEFINITIONS

<b>Disclosure</b>	to make personable information available to someone outside the organisation and release the subsequent handling of the personal information from its control.
<b>Log Files &amp; Cookies</b>	Log file lists actions that have occurred. Eg web servers maintain log files listing every request made to the server which can identify where visitors are coming from and how often they return. Cookies are industry standard for most major websites. They may be used to recognized a computer which has previously visit the website, and to customize OC Connections website according to previous preferences and site behaviour.
<b>Personal Information</b>	any information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether it is true or not, and recorded in a material form or not. Personal information that has been de-identified is no longer personal information. Examples include, but are not limited to, an individual's: <ul style="list-style-type: none"> <li>• name</li> <li>• signature</li> <li>• address</li> <li>• telephone number</li> <li>• date of birth</li> <li>• bank account and taxation details</li> <li>• identity documents e.g. passport or driving license</li> <li>• personal opinions.</li> </ul> Information held in worker people, learning and culture (PLC) files is also personal information.
<b>Pseudonym</b>	a name, term or descriptor that is different to an individual's actual name.
<b>Sensitive Information</b>	a subgroup of personal information. Examples include, but are not limited to, information about an individual's: <ul style="list-style-type: none"> <li>• racial or ethnic origin</li> <li>• political opinions</li> <li>• religious or philosophical views</li> <li>• sexual orientation or practices</li> <li>• criminal record</li> <li>• health information.</li> </ul>



### RELATED LEGISLATION AND REFERENCE DOCUMENTS

- Document Retention and Disposal Policy
- Data Breach Response Plan
- Decision Making and Choice Policy
- Advocacy Policy
- Compliments and Complaints Procedure
- Participant Safeguarding Policy
- The Privacy Act 1988 (Cth)
- Compliance Management Framework
- Continuous Improvement Policy
- Continuous Improvement Register
- Risk Management Policy & Framework
- National Disability Insurance Scheme Act 2013
- National Disability Insurance Scheme (Quality Indicators) Guidelines 2018
- NDIS Code of Conduct Rules 2018
- NDIS (Provider Registration and Practice Standards) Rules 2018
- NDIS Quality Practice Standards Nov 2021
- Disability Services Act 1986
- Fair Work Workplace Privacy Best Practice Guide