## Statement of Purpose

Fairhaven Services is committed to protecting and upholding the right to privacy of all participants, workers, Board members, volunteers and representatives of agencies we deal with. Fairhaven is committed to protecting and upholding participants' rights to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

Fairhaven requires all workers, volunteers and Board members to be consistent and careful in the way they manage what is written and said about participants and how they decide who can see or hear this information.

As an NDIS registered provider, Fairhaven is subject to the provisions of both the *Privacy Act 1988 (Cth)* and the *National Disability Insurance Scheme Act 2013 (NDIS Act)*, which work together to protect personal information. Fairhaven follows the guidelines of the *Australian Privacy Principles* in its information management practices.

Fairhaven will ensure that:

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of participants and organisational personnel
- participants are provided with information about their rights regarding privacy
- participants and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all workers, volunteers and Board members understand what is required in meeting these obligations
- it adheres to all requirements imposed under the *Privacy Act 1988 (Cth),* as amended from time to time.

This policy conforms to the *Privacy Act 1988 (Cth)* and *the Australian Privacy Principles* which govern the collection, use and storage of personal information. This policy will apply to all records, whether hard copy or electronic, containing personal information about participants, and to interviews or discussions of a sensitive personal nature.

## Definitions

*Personal information* includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information
- employee record information
- photographs
- internet protocol (IP) addresses
- voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- location information from a mobile device (because it can reveal user activity patterns and habits).

*Sensitive information* is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

Generally, sensitive information has a higher level of privacy protection than other personal information.

**Procedures**

**Dealing with personal information**

In dealing with personal information, Fairhaven staff will:

- ensure privacy for participant, workers, volunteers or Board members when they are being interviewed or discussing matters of a personal or sensitive nature
- only collect and store personal information that is necessary for the functioning of the organisation and its activities
- use fair and lawful ways to collect personal information
- collect personal information only by consent from a participant
- ensure that people know what sort of personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it
- ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any participant or staff member to review information or correct wrong information about themselves
- take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure
- destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired
- notify participants and the Office of the Australian Information Commissioner (OAIC) when there has been a data breach (or suspected breach) of personal information, if it is likely to result in serious harm to participants whose privacy has been breached.

**Dealing with sensitive information**

Sensitive information will be collected, used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless agreed otherwise, or the use or disclosure of the sensitive information is allowed by law.

Fairhaven will take all reasonable steps to prevent and manage personal and sensitive information from being misused, and to keep private and sensitive information secure. This includes:

- *organisational measures* such as delegated responsibilities for managing access to personal

information, deactivating accounts when employees leave and ongoing staff training
- *technical security measures* including role-based access control to computer systems and data to ensure users only have the access they need to perform their role as well as multifactor authentication to access systems and data.

**Responsibilities for managing privacy**

All workers are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.

The CEO is responsible for content in Fairhaven publications, communications and website and must ensure the following:

- appropriate consent is obtained for the inclusion of any personal information about any individual including Fairhaven personnel
- information being provided by other agencies or external individuals conforms to privacy principles
- that the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.

The CEO is responsible for safeguarding personal information relating to Fairhaven workers, volunteers, contractors and Board members.

**Privacy Contact Officer**

The Privacy Contact Officer is the Human Resources and Culture Manager who is responsible for:

- ensuring that workers, volunteers and Board members are provided with information about their rights regarding privacy
- ensuring that all workers are familiar with the Privacy Policy and administrative procedures for handling personal information
- handling any queries or complaint about a privacy issue.

**Training and Development**

Fairhaven implements regular worker, volunteer and Board member training to ensure appropriate understanding of the technical measures employed to ensure privacy and security. Organisation-wide training is enforced to build all workers' ability to detect evolving threats or breaches of privacy.

**Privacy information for participants**

As part of the intake process participants are advised about the information that is being collected, how their privacy will be protected and their rights in relation to this information.

Unless required by law, consent is required for any personal data collection including geo-location tracking data and any data shared with an external party. For participants with a Behaviour Support Plan, Fairhaven will only collect personal and sensitive data as required by the specialist behaviour support provider and as prescribed in the *National Disability Insurance Scheme (Restrictive Practices and Behaviour Support) Rules 2018*.

Consent for the collection or use of any personal data must be voluntary, informed, specific, up to date/ current and easily withdrawn. Informed consent means the individual knows how the data is

being used and will specify any overseas parties the data may be shared with, whether the organisation will use the data for high-risk activities and how long the organisation will hold and store the data before correctly deactivating the storage.

**Managing automated decision-making**

Automated decision-making programs are computer systems that make decisions or provide recommendations without direct human intervention. In Supported Independent Living and Specialist Disability Accommodation Fairhaven uses the MedCare Medication Management System, which is integrated with Webstercare's MedSig e-signing platform. This system connects the entire medication care team including pharmacists, general practitioners, and support staff via a cloud-based, centralised medication profile system and supports effective and timely communication.

Personal information is encrypted in-transit and stored securely on Medsig's own data centre in Sydney. MedSig uses automated decision-making in the form of alerts and reminders to support, but not replace, human judgment. It automatically triggers alerts for tasks like returning to a participant if they were missed during a medication round and provides data-driven reporting to assist with patient care and organisational decision-making.

**Privacy for interviews and personal discussions**

To ensure privacy for participants or workers and volunteers when discussing sensitive or personal matters, the organisation will ensure privacy is provided through the use of private interview spaces or home visits and that telephone calls discussing individuals or their personal information are made in a private area.

**Participants in research projects**

People being invited to participate in a research project must be:

- given a choice about participating or not
- given the right to withdraw at any time
- informed about the purpose of the research project, the information to be collected, and how; information they provide will be used
- given copies of any subsequent publications.

The collection of personal information will be limited to that which is required for the conduct of the project. Individual participants will not be identified.

**Privacy of care**

The specific services, treatments and care that are provided by Fairhaven to individuals remain private and confidential. Fairhaven ensures that individuals have choice over when and how they receive physical care or treatment, and that this is carried out in private.

**Privacy Breach – Accidental or unauthorised disclosure of personal information**

Fairhaven will take seriously and deal promptly with any accidental or unauthorised disclosure of personal information of participants, workers, volunteers or board members and comply with the Notifiable Data Breaches (NDB) Scheme. The NDB Scheme strengthens protections for personal information and allows individuals to take steps to protect their information following a breach, or suspected breach.

A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure. For example:

- a client's personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

Under the NDB Scheme Fairhaven must notify individuals and the Office of the Australian Information Commissioner (OAIC) when there has been a data breach (or suspected breach) of personal information, if it is likely to result in serious harm to individuals whose privacy has been breached.

**Enquiries and Privacy Complaints**

Enquiries or complaints about the way Fairhaven collects, manages and stores personal or sensitive information about an individual should be directed to the People and Culture Manager at askhr@fairhaven.org.au or in writing to PO Box 6176, West Gosford, NSW, 2250. Fairhaven takes any privacy complaint seriously and aims to resolve the complaint in an efficient manner within 30 days.

If the complainant is dissatisfied with Fairhaven's response, a formal complaint can be lodged in writing with the Australian Information Commissioner as follows:

- on their online privacy complaint form or privacy complaint form (DOCX, 63 KB)
- in a letter to PO Box 5288 Sydney NSW 2001
- in a fax to +61 2 6123 5145.

| **Policy context** – this policy relates to: | |
|---|---|
| Standards | NDIS Practice Standards Core Module:<br>Outcome 1: Rights and Responsibility for Participants<br>1.3 Privacy and Dignity<br>Outcome 2: Provider Governance and operational management<br>2.4 Information Management<br>2.7 Human Resource Management |
| Legislation | National Disability Insurance Scheme Act 2013 (NDIS Act)<br>Privacy Act (Cwth) 1988<br>Australian Privacy Principles<br>National Disability Insurance Scheme (Supports for Participants) Rules 2013<br>National Disability Insurance Scheme (Code of Conduct) Rules 2018<br>National Disability Insurance Scheme (Restrictive Practices and Behaviour Support) Rules 2018. |
| Contractual obligations | Service Agreement<br>Tenancy Agreement<br>Employment Agreement |

| | |
|---|---|
| Organisation policies and documents | QA-POL-019 Service Access Policy Statement<br>QA-POL-013 Fairhaven Client Service Charter<br>SP-POL-102 Choice and Control Policy<br>QA-POL-017 Information, Technology and Security Policy and Procedure<br>COR-PP-003 Confidentiality Policy and Procedure<br>COR-DOC-005 Data Breach Policy and Response Plan |
| Forms | Information Exchange and Media Consent Form |