Objective

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

Fighting Chance needs to collect and maintain personal information in order to provide services to participants. The information we collect is used to provide services in a safe and personalised way, to meet duty of care obligations, to make appropriate referrals (where necessary), and to carry out business administration to support those services.

Scope

This policy applies to:

- all personal information and sensitive personal information including the personal information of employees and participants.
- all company confidential information - that is any information not publicly available.
- all Fighting Chance representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

Definitions

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

Personal information: Personal information includes (regardless of its accuracy): name, address, phone number, email address, date of birth, recorded opinions or notes about someone and any other information that could be used to identify someone.

Sensitive personal information: Sensitive personal information can include personal information that is normally private such as:

- health information

- racial or ethnic origin
- sexual orientation or practices
- religious or philosophical beliefs
- criminal record
- biometric information (such as fingerprints)
- political opinions or associations
- trade union membership or associations

Media material: materials including photos, video, written and verbal statements, blog entries, anecdotal stories, experiences and other similar material that may be used as content for marketing and promotional materials via a range of platforms and media including but not limited to newspapers and magazines, reports and presentations, brochures, radio segments, intranet and internet sites, and social media such as (but not limited to) Facebook, Instagram and LinkedIn.

Workplace: any place where a worker goes or is likely to be while work is carried out for the business or undertaking.

Statement

- Fighting Chance is committed to complying with the privacy requirements of the Privacy Act, the Australian Privacy Principles (APPs) and 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 and relevant state or territory requirements.
- We provide all individuals with access to information about the privacy of their personal information.
- Each individual has the right to opt out of consenting to and providing their personal details if they wish. However, this may impact how Fighting Chance delivers services to the participant - for example, if a participant refuses to share support plans or clinical information, it may affect the safety and quality of the support we can provide
- Individuals have the right to request access to their personal records.
- Individuals have the right to request amendments to personal information if it is incorrect.
- 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).
- Images, video or other collected content involving participants will not be used without their consent.
- Participants are able to opt out of NDIS audits.
- Fighting Chance does not disclose personal information to overseas entities unless directed by the participant - for example, if the participant's family resides overseas and requests an update on their service attendance at Fighting Chance.

Activities that involve personal information handling

- meet duty of care obligations,
- to make appropriate referrals (where necessary), and
- to carry out business administration to support those services.

Collecting your personal information

The means by which we collect your personal information will depend on the nature of the service that we are providing to you. We may collect your personal information:

a. Directly from you;
b. When you access and interact with our websites;
c. From other sources, including from referrers.

We will always collect your personal information directly from you unless it is impracticable to do so. This would usually be done through application forms, over the telephone, in person or over the internet.

Your personal identifiable information will not be collected if you are only browsing our websites.

At the time of collecting your personal information, we will remind you of the following:

1. Our details, including our contact details;
2. That we are collecting your information and the reasons why we are collecting your information;
3. If the collection is required or authorised by law, the details of the law;
4. What happens if we cannot collect your personal information;
5. Any third parties to whom we may disclose the personal information;

6. How you can access and correct your personal information; and
7. How you can complain about any breach of the APPs and how we will handle any such complaints

The purposes of collecting your personal information

We may use and disclose your personal information for the purposes for which it was collected or for a related purpose such as:

1. To consider your request for a product or service;
2. To enable us to provide a product or a service to you;
3. To facilitate the provision of a product or service to you;
4. To carry out or respond to your requests;
5. To our third party service providers to assist us in providing and improving our services to you and better understand your needs or to develop, improve and market our services to you;
6. For regulatory reporting and compliance with our legal obligations;
7. To various regulatory bodies and law enforcement officials and agencies to protect against fraud and for related security purposes;
8. To perform administrative and operational tasks (including risk management, systems development and testing and sta training);
9. To include in a database compiled by us for use in fundraising, donations, sponsorship, events, direct marketing of promotions, products and services we think may be of interest to you;
10. To seek your feedback in relation to customer satisfaction and our relationship with you;
11. To monitor or improve the quality and standard of service that we provide to you;
12. To consider any concerns or complaints you may raise against us;
13. To notify you of others that may be of interest to you; and
14. To better understand your preferences.
15. To doctors and health care professionals, who assist us to deliver our services;
16. To referees and former employers of job candidates and volunteers, and candidates for employee and volunteer positions at Fighting Chance;
17. To professional advisors, including our accountants, auditors and lawyers.
18. To emergency services in a medical emergency.

Sharing your personal information with others

We may share your personal information with other entities within the Fighting Chance group where there is no conflict of interest i.e. Support Coordination.

We deal with third party service providers (who may be based overseas) who may assist us with a variety of functions including with research, mail and delivery, security, insurance, professional advisory (including legal, accounting and auditing advice), banking, payment processing, credit reporting, offsite storage or technology services. Where we engage third party service providers to perform services for us, those third parties may be required to handle your personal information. Under these circumstances, those third parties must safeguard this information and must only use it for the purposes for which it was supplied and we will make all reasonable enquiries to try to ensure that this is the case.

Wherever possible, we will limit the information provided to independent third parties to that information required for those third parties to properly perform their functions. Further, our contracts with these third parties will always require the third parties to comply with the APPs (or equivalent standards).

If you choose not to give consent to share information, Fighting Chance will still provide a participant's medical information to emergency services in a medical emergency.

Holding your personal information

We store personal information in the following locations:

- Our care management system, SupportAbility
- Google Drive (in locked, secure folders for scanned documents such as medication charts)
- Printed copies of support plans (e.g. epilepsy management plans) for support workers to read before their shift

Access to personal information is restricted to relevant staff who need it to perform their role and support participants safely.

Security of information

- We take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.

- Personal information is accessible to the participant and is available for use by relevant workers based on the service they work in, their role in the service, and on a need to know basis.
- Security for personal information includes data encryption, password protection and Multi Factor Authentication (MFA) for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel permitted access.
- We restrict the use of personal information with AI conversational and AI generative platforms (e.g. ChatGPT, Gemini, etc) unless using approved corporate subscriptions.
- While care is taken to protect your personal information on our Websites, unfortunately no data transmission over the Internet is guaranteed as 100% secure. All unencrypted information exchanged via the Internet may be accessed and used by people other than those for whom it is intended, for example if any personal information is sent by email it is sent at the risk of the sender. Once we receive your personal information, we are required to protect it in accordance with the Privacy Act 1988.
- Personal information no longer required is securely destroyed or de-identified.

Data Breaches

- We will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only to relevant workers.
- If we know or suspect your personal information has been accessed by unauthorised parties, and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach
- A breach of privacy and confidentiality may require an investigation (including a review of IT system and email account access logs)
- An intentional breach of privacy and confidentiality will result in disciplinary action up to and including termination of employment.

Making a complaint about the Fighting Chance privacy procedures

We are committed to maintaining and protecting your privacy. If you are concerned with the way your personal information has been handled, you are entitled to make a complaint. If you would like to lodge a complaint, please contact us via email hello@fightingchance.org.au (with Privacy as the subject) or call (02) 9905 0415 and ask to speak with a member of the Quality & Continuous Improvement Team.

If your personal information has not been handled in an appropriate way, we will do our best to remedy your concerns as quickly as possible.

If your complaint is not satisfactorily resolved, you may approach an external dispute resolution service or apply to the Office of the Australian Information Commissioner ("OAIC") , enquiries Line (1300 363 992), to have the complaint heard and determined.

Related Framework Documents

- PRO-OPS-003 Privacy, Dignity and Confidentiality Procedure
- PRO-SER-001 Decision Making and Consent Procedure
- FM-OPS-006 Privacy and Consent Form
- FM-ACC-001 Base Privacy Consent Form

Monitor & Review

This policy will be reviewed annually in accordance with Fighting Chance's quality assurance and continuous improvement process. The Quality and Continuous Improvement Advisor will report on the outcome of the review and make recommendations for amendment, alteration or substitution if considered necessary.

Document Version Control

Date	Summary of Amendments	Author
October 2021		CEO/ Compliance
November 2024	Review of policy	Q&CI