Purpose

SupportAbility Software Pty Ltd ABN 72 113 901 830 (**SupportAbility**) values the privacy of all its people, customers, suppliers and other parties it does business with, and recognises that the personal information we collect and hold is often sensitive.

This Policy explains how we collect, use, hold and disclose personal information, as well as ensuring the quality, integrity and security of personal information in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) (**Privacy Act**).

Our business is to understand and meet our clients' needs for delivering services under the National Disability Insurance Scheme (**NDIS**). To do this effectively, we need to collect certain personal, sensitive health information and the SupportAbility Privacy Policy describes our current policies and practices in relation to the collection, handling, use and disclosure of personal information.

We may modify, amend or replace this privacy policy from time to time. A new version of the policy will be posted to our website www.supportability.com.au when this happens. Therefore, we recommend that you regularly review our privacy policy.

Scope

The requirements and expectations outlined in this policy apply equally to all personnel defined as:

- All full time, part time, temporary or casual SupportAbility employees;
- All contractors engaged by SupportAbility and
- All suppliers that provide services to SupportAbility.

Definitions

Term	Definition
Personal Information	Personal Information includes any information or opinion about an identified individual or individual who can be reasonably identified from that information. The information or opinion will still be personal information whether it is true or not and regardless of whether we have kept a record of it. Examples of this information include records containing a person's name, address, telephone number and gender. SupportAbility collects information from our employees, clients and by default, their clients' customers.
Sensitive	Sensitive information is a form of personal information. Some types of personal information are categorised as sensitive, recognising that this type of information is higher risk and needs to be handed with a higher level of protection. Examples of sensitive information may include information or an opinion about an individual's: ● racial or ethnic origin; ● religious and philosophical beliefs or affiliations; ● sexual orientation or practices; ● etc…

Health Information	Health information is a specific type of sensitive information, and includes information or an opinion about the physical or mental health of a person, or the disability of an individual. Examples may include: ● information about an individual's physical or mental health; ● notes of an individual's symptoms, diagnosis and treatment; ● specialist reports and test results; ● an individual's wishes about future health services; and ● appointment and billing details.

Who is responsible for privacy?

It is the responsibility of all SupportAbility employees, suppliers and contractors to protect the privacy of our clients by managing all personal information in accordance with this policy and the APPs.

Policy Detail

Privacy Standards

Information Collected

As a provider of client management system software that empowers disability service providers who deliver under the NDIS to manage their customer data and business operations, SupportAbility is designed to store a range of personal information (including sensitive and health information) entered by providers about their organisation, their customers, their employees and business operations.

Our ability to provide NDIS service provider clients with comprehensive professional services and advice is dependent on us storing certain personal and sensitive health information entered by our clients. The type of personal information SupportAbility stores about providers, their employees and their customers includes:

- Personal details such as name, address, date of birth, and contact details including telephone numbers and address
- Information about individuals' disabilities, the nature of their condition and the manner in which the disability or condition occurred
- Functional and psychological status in relation to the compensable injury and any other medical factors that may be disclosed that may impact on functional or psychological capacity

How Information is Collected

SupportAbility provides a Software as a Service (**SaaS**) application which their clients use to upload and manage personal information (including sensitive information such as health information) pertaining to their customers, employees and business operations. SupportAbility does not expressly use this information for any operational purposes. However, the information is collected in a manner that is:

- Lawful - SupportAbility only collects personal information provided by their clients through their SaaS application. This information is not used by SupportAbility but rather by their customers in delivering NDIS services.
- Relevant – SupportAbility does not have any responsibility in ensuring the information uploaded into their SaaS application is relevant, accurate, complete and up to date. The responsibility to maintain the data's integrity lies with the client.
- Direct – SupportAbility collects personal and health information directly from their clients.
- Open – SupportAbility takes reasonable steps to inform clients why we are collecting information, what we will do with it and who will see it.

We may also collect personal information about an individual from a range of sources using a variety of means including:

- forms (either physical or online), mail correspondence, emails and other electronic communications;
- feedback provided by our clients to us in relation to the services provided;
- inquiries or discussions about us and/or the services we provide;
- publicly available sources of information;
- interactions with social media channels that we may offer or monitor;
- from job applicants and staff members;
- direct contact in the course of providing services (including the administration of accounts established with us);
- in the course of conducting market research, including customer surveys; and
- from current and prospective suppliers of goods and/or services to us.

Cookies and Other Tracking Technologies

SupportAbility uses various technologies to deliver its services, which may include sending cookies to your computer or mobile device. Cookies are small data files stored on your hard drive or in device memory that helps us to improve our customer service and your experience, see which areas of our website are popular, and to count visits on our website. We may use cookies to:

- Manage security in the SupportAbility web and mobile applications;
- Gather service usage data for the purposes of anonymous and aggregate analytics; and
- Carry out any other purpose for which the information was collected.

Web and Mobile Applications Users:

Most web browsers are set to accept cookies by default. Whilst you can set your browser to remove or reject browser cookies; doing so causes the SupportAbility web and mobile applications to no longer work in the selected web browser.

SupportAbility Website Visitors:

If you visit our website, we will collect information such as your IP address, internet service provider, the web page directing you to our website and your activity on our website.

Although this information is usually anonymous and we do not use it to identify individuals, this information might contain details that identify you because of the nature of internet protocols.

Most web browsers are set to accept cookies by default. If you prefer, you can set your browser to remove or reject browser cookies; however, this may affect your browsing experience. We use “cookies” on some (but not all) web pages to deliver personalised content or to tailor our information offerings or responses according to the way you use our website, and/or your current context on our website.

Privacy Policy

Purpose of Collecting and Holding Personal Information

SupportAbility collects information to:

- Ensure accuracy, efficiency and useful direction of client management services;
- Meet our obligations to employees (including payroll, taxation and superannuation); and
- To help run our business.

Storage of Personal Information

SupportAbility is responsible for the collection of personal information on its clients, users and prospective employees and it uses such information during its normal business operations. SupportAbility holds personal information within its cloud environment and takes steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

SupportAbility has contractual arrangements with Amazon Web Services (AWS) under which AWS provides our 'cloud infrastructure' and related services. Under this arrangement, AWS acts as a data processor in that it stores client data, including personal information, on our behalf.

Use & Disclosure

SupportAbility will only use or disclose personal information for the purpose for which it was collected (known as the "primary purpose"), another purpose related to the primary purpose where the individual would reasonably expect it to be used or disclosed for such a related purpose (known as the "secondary purpose"), with the individual's consent or as otherwise allowed under the Privacy Act. In regards to sensitive information (which includes health information), SupportAbility will only ever use or disclosure sensitive information with consent, for the primary purpose for which it was collected, or for another purpose *directly related* to the primary purpose where the individual would reasonably expect it to be used or disclosed for such a *directly related* purpose.

SupportAbility may be required to disclose personal information by law, by court order or to investigate suspected fraud or other unlawful activity. SupportAbility may also disclose personal information to third parties in certain circumstances including:

- if the individual agrees to the disclosure;
- when SupportAbility uses it for the primary purpose for which it was collected (including to provide clients with services);
- if the individual would reasonably expect us to disclose the personal information for a secondary purpose related to the primary purpose;
- where disclosure is required or permitted by law;
- to related entities, in accordance with the Privacy Act;
- if disclosure will prevent or lessen a serious or imminent threat to someone's life or health; or
- where it is reasonably necessary for an enforcement related activity.

SupportAbility takes steps to ensure personal information is not disclosed to any overseas recipients.

Consent

By subscribing to SupportAbility and using the SaaS application (in web or mobile form), you consent to the collection of information uploaded to the SupportAbility SaaS application. As mentioned above, this information is not used by SupportAbility, but rather by their customers in delivering NDIS services.

Retention of Personal Information

We apply a general rule of keeping personal information only for as long as required to fulfil the purposes for which it was collected. When the personal information that we collect is no longer required, we will destroy or de-identify the personal information as soon as reasonably practicable. In general, we retain your personal information for a period of time corresponding to a statute of limitation, for example to maintain an accurate record of your dealings with us. More information on data retention can be seen in our Data Retention Policy which can be provided upon request.

However, in some circumstances we may retain personal information for instance where we are required to do so in accordance with legal, tax and accounting requirements, or if required to do so by a legal process, legal authority, or other governmental entity having authority to make the request, for so long as required.

Access to and Correction of Personal Information

Individuals are welcome to request that we provide access to the personal information we hold about them by contacting us using the details listed under the "Feedback and Complaints" section of this Policy below. Generally, we will provide access to the information unless applicable laws allow us to refuse, or prevent us from giving, access to the personal information we hold. We will not unreasonably refuse requests to access personal information.

Where we agree to provide access to personal information, we may make this conditional on us recovering our reasonable costs of doing so. No fee will be incurred for requesting access, but if a request for access is accepted, the individual will be notified of the fee payable (if any) for providing access if the individual proceeds with the request.

Individuals may also lodge a request to correct personal information we hold if they believe it is inaccurate, incomplete, irrelevant, misleading or out of date. There is no fee for doing this. To do so, please contact us at the contact details listed under the "Feedback and Complaints" section of this Policy below.

In regards to personal information that is uploaded to the SupportAbility service by our clients, please note that clients have control over this information and, as such, any access or correction requests should be directed to the client responsible for uploading the personal information to the SupportAbility service, and not to SupportAbility.

Direct Marketing

We may use personal information, from time to time, to send marketing materials to current or prospective customers. We will only do so with consent or where allowed by applicable laws. Our communications may be sent in various forms such as by post or by electronic means (including email and SMS). If you wish to cease receiving marketing information, please contact us directly asking to be removed from our mailing lists, or use the "unsubscribe" or "update your preferences" facilities included in all our marketing communications.

Please note that we will never use sensitive information for direct marketing purposes.

Employment and Recruitment

Please note that this Privacy Policy applies to the handling of personal information about prospective job applicants, but does not apply to our handling of information about employees. Our handling of employee records is exempt from the APPs under the Privacy Act if the act or practice is directly related to:

- either a current or former employment relationship between us and the individual; and
- an employee record held by us relating to the individual.

For information about our practices relating to employee records, please contact us by using the contact details listed at the end of this Policy below.

Notifiable Data Breaches

The Privacy Act 1998 (Cth) includes a Notifiable Data Breaches (**NDB**) scheme which requires SupportAbility to notify you and the Office of the Australian Information Commissioner (**OAIC**) of certain data breaches and recommend steps you can take to limit the impacts of a breach (eg. enabling Multi-Factor Authentication and/or Password Strength Management).

The NDB scheme requires us to notify about "eligible data breaches", which occur when there is a data breach that is likely to result in serious harm to affected individuals and we are unable to prevent the likely risk of serious harm with remedial action.

If we suspect a privacy breach has occurred, our priority is to contain and assess the suspected breach. In doing so, we will:

- take any necessary immediate action to contain the breach and reduce the risk of harm;
- determine the cause and extent of the breach;
- consider the types of information involved, including whether the personal information is sensitive in nature;
- analyse the nature of the harm that may be caused to affected individuals;
- consider the person or body that has obtained or may obtain personal information as a result of the breach (if known); and
- determine whether the personal information is protected by a security measure.

If we believe an eligible data breach has occurred we will, as soon as practicable, notify the OAIC and all affected individuals or, if it is not possible to notify affected individuals, provide public notice of the breach (in a manner that protects the identity of affected individuals), such as a notice on our website.

If you believe that any personal information we hold about you has been impacted by a data breach, please contact SupportAbility's CEO:
William Jamieson
william@supportability.com.au

Feedback and Complaints

We welcome any questions, feedback and complaints about our systems and processes for handling personal information. You have the right to complain if you believe we have breached this policy or your rights under the APPs.

To lodge a complaint, please write to our CEO at the following address:

william@supportability.com.au

or

William Jamieson c/o SupportAbility

Collins Street Tower
Level 3, 480 Collins Street
Melbourne VIC 3000

We will promptly acknowledge receipt of your complaint and we will endeavour to deal with your complaint and to provide you with a response within a reasonable time period following receipt of your complaint (generally within 30 days of receipt). Where a complaint requires a more detailed investigation, it may take longer to resolve. If this is the case, then we will provide you with progress reports.

We reserve the right to verify the identity of the person making the complaint and to seek (where appropriate) further information from the complainant in connection with the complaint.

Where required by law, we will provide our determination on your complaint to you in writing. Please note that we may refuse to investigate or to otherwise deal with a complaint if we consider the complaint to be vexatious or frivolous.

If you are not satisfied with our response, you can contact the Office of the Australian Information Commissioner.

Office of the Australian Information Commissioner

Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Website: www.oaic.gov.au

Reference Documentation

This policy will be read in conjunction with:

- SupportAbility's suite of information security policies and procedures; and
- Information Security Standard ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Compliance and Enforcement

Term	Risk	Description
must	High	Policy statement is mandatory unless a risk assessment is approved by the Top Management
should	Medium	Policy statement is strongly advised unless a risk assessment is performed, and risk accepted by the information asset owner and approved by a manager.
may	Low	Policy statement is advised unless a risk assessment is performed and accepted by the asset owner

Failure to comply with any element of this policy may result in disciplinary action, up to and including termination of employment in accordance with SupportAbility's disciplinary process.

Exemption from this policy must be sought from the Chief Executive Officer (CEO).

Policy Review

This policy shall be subject to annual review or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness. Reviews shall incorporate:

- Assessment of opportunities for improvement of SupportAbility's approach to information security; and
- Consideration of changes to the organisational environment, business circumstances, legal conditions, or the technical environment. Policies will be endorsed by the SupportAbility CEO.

Document Control

Version number	Effective date	Owner	Approved by (date)	Review date
1.0	12/05/2022	Chief Technology Officer	Chief Executive Officer	February 2023
1.1	18/07/2022	Chief Technology Officer	Chief Executive Officer	February 2023
1.2	25/07/2022	Chief Technology Officer	Chief Executive Officer	February 2023