PRIVACY POLICY AND PROCEDURE

Compliance with this Policy Directive is **Mandatory**

Document Type	Corporate Policy Document
Purpose of the Policy	This policy exists to provide a clear outline of how and when personal information including sensitive information is collected, disclosed, used, stored and otherwise managed by The Company. The Company is subject to Privacy legislation applying to the organisation and/or its client group. The organisation will follow the guidelines of the *Australian Privacy Principles* in its information management practices.
Definitions	**What is personal information?** Personal information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable. Information does not have to include your name to be personal information. For example, in some cases, your date of birth and post code may be enough to identify you. To be precise, the Privacy Act definition of personal information is: *"... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."* ***Sensitive information*** means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinion; (iii) membership of a political association; or; (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information.

	Health information means: (a) information or an opinion about: (i) the health or a disability (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to him or her; or (iii) a health service provided, or to be provided, to an individual; that is also personal information; or (b) other personal information collected to provide, or in providing, a health service; or (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. **What privacy is not** The protection of your personal information privacy is different to other related concepts such as: • confidentiality • secrecy • freedom of information
Key Principles	The Australian Privacy Principles: • **APP 1 — Open and transparent management of personal information** Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. • **APP 2 — Anonymity and pseudonymity** Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply. • **APP 3 — Collection of solicited personal information** Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information. • **APP 4 — Dealing with unsolicited personal information** Outlines how APP entities must deal with unsolicited personal information. • **APP 5 — Notification of the collection of personal information** Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters. • **APP 6 — Use or disclosure of personal information**

	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds. • **APP 7 — Direct marketing** An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. • **APP 8 — Cross-border disclosure of personal information** Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas. • **APP 9 — Adoption, use or disclosure of government related identifiers** Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual. • **APP 10 — Quality of personal information** An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure. • **APP 11 — Security of personal information** An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances. • **APP 12 — Access to personal information** Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies. • **APP 13 — Correction of personal information** Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.
Policy	The Company is committed to conducting our business in accordance with the Australian Privacy Principles in order to ensure that the confidentiality of personal information is protected and maintained. We will ensure that all staff, Board/Management Committee members and volunteers understand what is required in meeting these obligations. We will make readily available to all clients information about our policies and practices relating to what sort of personal information is held, for what purposes it is held, how it is collected, used, disclosed and stored, how to access and correct their own personal information and how they may complain if they feel there has

been a breach of their privacy rights.

The purpose of information collected

We will only collect personal information for purposes which are directly related to our functions or activities, and only when it is necessary for or directly related to such purposes. This information will only be retained as long as necessary for the fulfilment of those purposes.

We need to collect personal information about clients (including health information) in order to provide them with the relevant care and treatment.

If a client refuses to provide The Company with relevant personal information we may not be able to provide them with the support or services they require.

Type of information collected

The Company collects personal and sensitive information including but not limited to:

- Name, address, telephone number;
- Date of birth and country of birth;
- Occupation;
- Indigenous status;
- Medicare number and Department of Veterans Affairs details;
- Religion;
- Health fund and payment details;
- medical history; and
- Details of individual diagnosis, care and treatment

How information is collected and stored

The Company will collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.

The Company may collect personal information from individuals or organisations in a number of ways. These include, but are not limited to applications for a business account, contractual arrangements, surveys or questionnaires, receipt of employment applications, receipt of referrals, registration for program services, or direct communications with The Company by telephone, fax, writing, email, or any other electronic means.

In general The Company shall collect personal information about individuals directly from those individuals or their authorised representative. At each point of contact by our staff The Company clients will be told what information is being collected, how their privacy will be protected and their rights in relation to this information

Personal and/or sensitive information may sometimes be collected from a third

party or from a publicly available source, but only if:

- the individual has consented to such collection or would reasonably expect us to collect their personal information in this way, or
- if it is necessary for a specific purpose such as the development of appropriate care planning or recruitment processes.

To ensure privacy for clients, subcontractors, stakeholder organisations or staff when discussing sensitive or personal matters, The Company shall ensure:

- Details are captured in a private space
- Communications that require confidentiality are conducted in a private setting – single office space or private homes
- Clients are notified of home visits
- All directors sign deeds of confidentiality
- All staff sign confidentiality documents
- Mutual disclosure and/or non-disclosure documents are prepared and signed by organisations participating in contracting negotiations
- All contracts. subcontracts and agreements contain clauses outlining the principles of this policy
- Face to face interviews are held in private office spaces

Personal Information Security

The Company is committed to keeping your personal information secure, and we will take reasonable precautions to protect your personal information from unauthorised access, loss, release, misuse or alteration.

Personal information may be stored in hard copy documents, but is generally stored electronically on the The Company software or systems.

The Company maintains physical security over its paper and electronic data stores, such as locks and security systems. The Company also uses computer and network security technologies such as firewalls, antivirus software, external email filtering and passwords to control and restrict access to authorised staff for approved purposes and to secure personal information from unauthorised access, interference, disclosure, misuse and loss.

All personal information no longer needed and/or after legal requirements for retaining documents have expired will be destroyed or permanently de-identified.

How information may be disclosed or used:

The Company will not give personal information about an individual to other Government agencies, private sector organisations or anyone else unless one of the following applies:

- the individual has consented
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies

- it is otherwise required or authorised by law
- it will prevent or lessen a serious and imminent threat to somebody's life or health, or
- it is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.

Disclosure of information to overseas recipients

The Company will not use or disclose any personal information to an overseas entity without express consent in writing from the concerned individual. In these circumstances The Company will use every endeavour to ensure that the foreign entity has appropriate measures in place to protect any personal information so disclosed.

Participation 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, and
- given copies of any subsequent publications.

The Company shall comply with the National Statement on Ethical Conduct in Human Research and will, where appropriate apply to the Human Research Ethics Committee for approval prior to participating in any research project.

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. Organisational participants in research projects will generally be identified in The Company research, unless the nature of a particular project requires anonymity or an organisation specifically requests it.

How an individual may access personal information and/or seek correction of such information:

The Company' aim is to ensure that all personal information collected is accurate, complete and up-to-date. Individuals can request access and/or request corrections to the personal information held by the The Company by contacting the Operations Manager.

Procedure for gaining access:

- All requests for access to personal information must be made in writing to the Operations Manager.
- The Company will acknowledge a request for access to personal information within 14 days.
- It is reasonable to expect that extraction of the personal information required may then take up to fifteen working days due to the need to access both paper based and computerised information systems. A

nominal fee may be charged to meet the costs of extracting the information. This is at the discretion of the Managing Director.
- If this timeframe is impracticable The Company will notify the individual making the request of a more appropriate timeframe.
- Individuals requesting access to personal information will be asked to verify their identity.

There may be instances where access is denied to certain record or aspects of records in accordance with the Privacy Act. These circumstances include:

- access would create a serious threat to safety;
- providing access will have an unreasonable impact upon the privacy of other individuals;
- denying access is required or authorised by law;
- the request is frivolous or vexatious;
- legal proceedings are underway or anticipated, and the information would not be accessible through the process of discovery in the proceedings;
- negotiations may be prejudiced by such access;
- providing access is likely to prejudice law enforcement;
- providing access is likely to prejudice action being taken or to be taken with respect to suspected
- unlawful activity or serious misconduct relating to the Group's functions or activities; or
- access would reveal a commercially sensitive decision making process.

If The Company denies access to personal information, it will provide reasons in writing to the individual making the request.

How an individual may complain about a breach of the Australian Privacy Principles:

Complaints can be made directly to The Company by telephone, email or in writing using the details provided here:

Telephone: 1300 364 876
Email: feedback@careassess.com
South: Level 2, 6 Bayfield Street, Rosny TAS 7018
North: 101 Stanley St, Summerhill TAS 7250
North West: 63 Best St, Devonport TAS 7310

If you believe The Company has not adequately dealt with your complaint, you may complain to the Privacy Commissioner whose contact details are as follows:

Officer of the Australian Information Commissioner (OAIC)
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
GPO Box 5218 Sydney NSW 2001

How The Company will deal with such a complaint:

Any complaint by an individual over an alleged breach of privacy will be dealt with under the Complaints Management Procedure and Policy.

Scope	This policy conforms to the *Privacy Act 1988* and *the Privacy Amendment (Enhancing Privacy Protection) Act 2012* 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 individuals, and to interviews or discussions of a sensitive personal nature. This policy is made available to all directors, management, staff, volunteers, subcontractors and the general public by request and via publication on the website.
References	1- Protecting Information Rights – Advancing Information Policy : Office of the Australian Information Officer 2- The Privacy Act 1998
Related Policies/ Procedures/ Documents	• Client Records Policy and Procedure • Confidentiality Policy • Access to Confidential Information • Complaints and Feedback Policy • Complaints and Feedback Procedure
Standards	Home Care Standards EO 1.1: Corporate Governance EO 1.2: Regulatory Compliance EO 1.2: Information Management Systems