Privacy and Confidentiality

Policy and Procedure

adeniumliving.com.au

SPECIALIST
DISABILITY
ACCOMMODATION

Adenium Living

Adenium Living **Privacy and Confidentiality Policy and Procedure**

Introduction

Adenium Living will actively protect the privacy of everyone involved with its functions and services by ensuring that information collected is shared with others only when:

- the Australian Privacy Principles are met, and
- it is in the interest of the person, and
- only when the appropriate consents are given, and
- only on a 'need to know' basis.

Purpose

The purpose of this Policy is to comply with:

1. The Australian Privacy Principles, as set out in the Privacy Act 1988, and amended by:
   - The Privacy Amendment (Private Sector) Act 2000 and
   - The Privacy Amendment (Enhancing Privacy Protection) Act 2012.
2. The SA Government Information Sharing Guidelines (ISG) Policy.
3. The NDIS Code of Conduct; Guidance for Service Providers.

Scope

This Policy applies to all employees and officers of Adenium Living and officers of the Adenium Living and includes staff and participant information. All staff are responsible for complying with this policy and procedure and their privacy, confidentiality, and information management responsibilities. Staff must keep personal information about participants, other staff, and other stakeholders confidential, in accordance with the confidentiality provisions in their employment or engagement contract.

Definitions

Access	This involves Adenium Living giving an individual/advocate information about the participant. This may include inspecting personal information held by Adenium Living or providing a copy of the information.
Collection	Adenium Living collects personal information if it gathers, acquires or obtains personal information from any source or by any means. This includes information not requested, or information obtained by accident.
Disclosure	In general terms, information is disclosed when Adenium Living releases information to others. Disclosure does not include giving information to a participant/advocate about the participant - that is, access.

Personal Information	Is information or opinion (including any forming part of a database) relating to a participant, which may be provided to Adenium Living, as part of its support activities, either in material form or not, and whether true or not. Such information may personally identify a participant or make a person's identity apparent.
Purpose	Is the reason for which Adenium Living collects personal information.
Record	A document, data base (however kept), photograph or other pictorial representation of a person.
Sensitive Information	Refers to information or an opinion about a participant's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual practices, criminal record or health information, including any disability.
Use	Refers to the handling and managing of information within Adenium Living, including use of the information in a publication.

Policy

Policy Principles

1. Before any private information held by Adenium Living is released to a third party by Adenium Living, the written and informed consent of the person must be obtained. Where a participant is unable to sign, their verbal consent (or other method of consent) will be recorded.
2. Participants may make a request to access to their own personal information.
3. If an individual believes that Adenium Living has breached their privacy under any aspect of this Policy, they firstly should lodge a complaint by referring to the Complaints Handling Procedure.
4. All employees, contractors and volunteers are required to sign a confidentiality clause which is included in their Contract, prior to commencement of working with Adenium Living.
5. All representatives making decisions on behalf of a participant who is 18 years of age (or older) will need to provide Adenium Living written evidence of their authority to decide one where the participant resides and who they reside with, and to sign service agreements and tenancy agreements on behalf of the participant.

Adenium Living recognises, respects, and protects everyone's right to privacy. All individuals (or their legal representatives) have the right to decide who has access to their personal information.

Adenium Living recognises the importance of protecting personal information, which it may need to collect from its employees, participants, volunteers and those associated with the service and will take all reasonable steps in order to comply with the Privacy Act and protect the privacy of the personal information that it holds.

Adenium Living's privacy and confidentiality practices support and are supported by its records and information process (See the Records and Information Management Policy and Procedure). Privacy and confidentiality processes interact with the information lifecycle in the following ways:

Create - Collection and Consent
Store - Secure Storage and Limited Access
Use - Access, Update, Disclose and Report
Archive - Secure Storage
Dispose - Secure Disposal

All staff are responsible for maintaining the privacy and confidentiality of participants, other staff and Adenium Living.

It is Adenium Living's Policy to follow the Australian Privacy Principles, as set out in the Privacy Act 1988 (Amended by the Privacy Amendment (Private Sector) Act 2000) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

In addition, it is Adenium Living's Policy to follow the SA Government's Information Sharing Guidelines for promoting safety and wellbeing (ISG) issued 2013; which outlines conditions under which information can be shared across agencies.

Responsibilities

The Quality and Compliance Leadership Team is responsible for ensuring Adenium Living complies with the requirements of the Privacy Act 1988.

This includes developing, implementing, and reviewing process that address:

- Why and how Adenium Living collects, uses and discloses personal information.
- What information Adenium Living collects about individual and its source.
- Who has access to the information.
- Information collection, storage access use, disclose and disposal risks.
- How individuals can consent to personal information about them.
- How Adenium Living safeguards and manages personal information about them, including how it manages privacy queries and complaints' and
- How information that needs to be updated, destroyed, or erased is managed.

Adenium Living has the ultimate responsibility for implementing this Policy plus ensuring awareness of all employees, contractors, and volunteers.

Adenium Living also has responsibility to ensure privacy through appropriate document management and control procedures. To meet the NDIS standards, participant information and records of decision making must be retained on file in an appropriate electronic document management system. Any hard or electrical copies will be protected by appropriate security measures to ensure participant information is protected and backed up.

Procedures

Induction and Ongoing Training

All staff must undergo induction which includes training in privacy, confidentiality, and information management. Staff knowledge and application of confidentiality, privacy and information management process is monitored on a day-to-day basis and through regular supervision/mentoring meetings. Additional formal and on-the-job training is provided to staff where required.

Adenium Living's Privacy information is found in the Participant Handbook. A full copy of this policy and procedure must be provided upon request.

Photos and Videos

Photos, videos, and other recordings are a form of personal information. Staff must respect people's choices about being photographed or videoed and ensure images of people are used appropriately, this includes being aware of cultural sensitivities and the need for some images to be treated with special care.

Information collection and consent

Participant information collection and consent

Adenium Living will only request personal information that is necessary to:

- Assess a potential participant's eligibility for a service.
- Provide a safe and responsive service,
- Monitor the services provided; and
- Fulfil government requirements for non-identifying and statistical information.

Personal participant information that Adenium Living collects includes, but is not limited to:

- Contact details for participants and their representatives or family members
- Details for emergency contacts and people authorised to act on behalf participants
- Participants' health status and medical records
- External agency information
- Feedback
- Incident Reports
- Consent forms.

Prior to collecting personal information from participants in their representatives, staff must explain:

- That Adenium Living only collects personal information that is necessary for safe and effective SDA provision.
- That personal information is only used for the purpose it is collected and its stored securely.
- What information is required.
- Why the information is being collected and how it will be stored and used.
- The occasions when the information may need to be shared and who or where the information may be disclosed to.
- The participant's right to decline providing information.
- The participant's rights in terms of providing, accessing, updating and using personal information, and giving and withdrawing their consent; and
- The consequences (if any) if all or part of the information required is not provided.

Participants and their families must be informed that a copy of this policy and procedure is available upon request.

Staff must provide privacy information to participants and their families in ways that suit their individual communication needs.

After providing the above information, staff must:

- Confirm the above information has been provided and explained well.
- Obtain consent from participants or their legal representatives to collect, store, access, use, disclose and dispose of their personal information.
- Participants and their representatives or families are responsible for:
- Providing accurate information when requested.
- Completing Consent Forms and returning them in a timely manner

NDIS Audits

Adenium Living complies with the requirements of the National Disability Insurance Scheme (Approved Quality Auditor Scheme) Guidelines 2018 whereby participants are automatically included in audits against the NDIS Practice Standards. Participants may be contacted at any time by a NDIS Approved Quality Auditor for an interview or for their participant files and plans to be reviewed.

Participants who do not wish to participate in these processes can notify any staff member who must inform their manager in writing. Their decision will be respected by Adenium Living and will be documented in their participant file. Upon commencement of any audit process,

Adenium Living notifies its Approved Quality Auditor of participants who have opted-out of the audit process.

Staff Information Collection and Consent

Personal staff information that Adenium Living collects includes, but is not limited to:

- Tax declaration forms.
- Superannuation details.
- Payroll details.
- Employment/engagement contracts.
- Personal details.
- Emergency contact details
- NDIS Worker Screening Checks, Police Checks and Working with Children Checks.
- First Aid and CPR certificates and other relevant training.
- Personal resumes.

Storage

Refer to the Records and Information Management Policy and Procedure for details on how Adenium Living securely stores and protects both staff and participant personal information.

Access

Staff personal information must only be accessed by the Management Team, who may only access the information if it is required in order to perform their duties.

Staff must only access participants' personal information if it is required in order to perform their duties.

Staff and participants have the right to:

- Request access to personal information Adenium Living holds about them, without a providing a reason for requesting access.
- Access this information.
- Make corrections if they believe the information is not accurate, complete, or up to date.

All staff access or correction requests must be directed to their direct line manager. Within 2 working days of receiving an access or correction request, the responding staff member will:

- Provide access or explain the reason for access being denied.
- Correct the personal information or provide reasons for not correcting it.
- Provide reasons for any anticipated delay in responding to the request.

An access of correction request may be denied in part or in the whole where:

- If the request is frivolous or vexatious.
- It would have an unreasonable impact on the privacy of other individuals.
- It would pose a serious threat to the life or health of any person; or
- It would prejudice any investigations being undertaken by Adenium Living or any investigations it may be the subject of.

Any staff access or correction requests that are denied must be approved by the Director and documented on the staff member's file.

Disclosure

Participant or staff personal information may only be disclosed:

- For emergency medical treatment
- With written (or verbal, where appropriate) consent from someone with lawful authority; or
- When required by law, or to fulfil legislative obligations such as mandatory reporting.

Reporting

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) Scheme is a national scheme that operates under the Privacy Act 1988 requires organisations to report certain data breaches to people impacted by the breach, as well as the Australian Information Commissioner.

A data breach occurs when personal information about others is lost or subject unauthorised access. A data breach may be caused by malicious action, human error or a failure in information management or security systems.

Examples of data breaches include:

- Loss or theft of devices (such as phones, laptops, and storage devices) or paper records that contain personal information.
- Unauthorised access to personal information by a staff member.
- Inadvertent disclosure of personal information due to 'human error', for example and email sent to the wrong person.
- Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

In addition to harm caused to people who are the subject of data breaches, an incident like this may also cause Adenium Living reputational and financial damage.

Further detail about the NDB Scheme is contained in the Office of the Australian Information Commissioner (OAIC) - Data breach preparation and response https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response

Identifying a Notifiable Data Breach

A Notifiable Data Breach, also called an 'eligible data breach', occurs when:

- There is unauthorised access to or disclosure of personal information, or information is lost in circumstances where unauthorised access or disclosure is likely to occur.
- The disclosure or loss is likely to result in serious harm to any of the people that the information relates to. In the context of a data breach, serious harm may include serious physical, psychological, emotional, financial, or reputational harm; and

- Adenium Living has been unable to prevent the likely risk of serious harm through remedial action.

All potential or actual data breaches must be reported to the Director, who will determine Adenium Living's response and whether the breach needs to be reported under the NDB Scheme.

If Adenium Living acts quickly to remediate a data breach and as a result it is not likely to result in serious harm, it is not considered a Notifiable Data Breach.

Responding to a Data Breach

If the Director suspects a data breach is notifiable under the NDB Scheme, they must make an assessment to determine if this is the case.

The Director must notify all impacted individuals of the breach as soon as practicable.

All data breach incidents (whether notifiable or not) must be responded to and recorded in Adenium Living's Incident Register, with relevant actions tracked in its Continuous Improvement Register where appropriate.

Where a breach is referred to the Director, the response will be based on the following steps:

Step 1: Contain the data breach.
Step 2: Assess the data breach and the associated risks.
Step 3: Notify individuals and the relevant authorities; and
Step 4: Prevent future breaches.

Notifiable Data Breaches Involving More Than One Entity

The NDB Scheme recognises that personal information is often held jointly by more than one entity. For example, one entity may have the physical possession of the information, while another has the legal control or ownership of it. Examples include:

- Where information is held by a cloud service provider.
- Subcontracting or brokering arrangements; and
- Joint ventures.

In these circumstances, an eligible data breach is considered the responsibility of both entities under the NDB Scheme. However, only one entity needs to take the steps required by the NDB Scheme and this should be the entity with the most direct relationship with the people affected by the data breach. Where obligations under the Scheme (such as assessment or notification) are not carried out, both entities will be in breach of the Scheme's requirements.

Archiving and Disposal

Refer to the Records and Information Management Policy and Procedure for details on how Adenium Living archives and dispose of staff and participant personal information.

Monitoring and Review

The Quality and Compliance Leadership Team reviews these processes regularly through annual privacy audits (See Adenium Living's Audit Schedule – External Audit and Internal Review).