Privacy and Confidentiality Policy	Pages	1 of 4
	Date created	2005
	New, revised or updated	Revised: 19 March 2019
	Approved by Board	
	Next Review Date	March 2021

Policy Statement

All About Living Inc. (AAL) collects and holds participant's personal, financial, medical and health information and carer's personal information, to facilitate participant access to, and continuity of services which enable them to make informed choices about their service requirements.

The types of information collected includes any material collected and stored in any form, e.g. mobile devices, computers, laptops, tablets, graphics, written material or other information in tangible or intangible form, relating to the activities of of AAL or its participants with the exception of information placed in the public domain by the authority of the Board.

This policy supplements policies and procedures relating to participants' funding arrangements.

Purpose

To:

- protect the integrity and confidentiality of all participant data collected by AAL employees whilst facilitating access to, and provision of services
- ensure all documents which contain participants and/or carers' names and contact details (including address, telephone numbers and email addresses) are kept confidential and secured
- ensure that all data and documents collected, retained and stored is compliant with legislative requirements, referenced below, and that appropriate systems and processes are in place to protect the privacy and confidentiality of participant information during intake, service delivery and termination of AAL services
- ensure all Board Members, permanent, casual and temporary employees, volunteers and sub-contractors are aware of their responsibilities to ensure that any participant or carer information collected, provided or stored is secured
- educate employees of the requirement to report any breach of security to their manager and the CEO immediately once aware of, noting that a failure to do so may result in disciplinary action being taken that could result in dismissal.

Application

This policy applies to all Board Members, permanent, casual and temporary employees, volunteers and sub-contractors.

Process

AAL will maintain ongoing security, integrity and privacy of confidential information through periodic review and updating security measures. AAL will take all reasonable steps to ensure the protection of information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

When information is no longer required or relevant it will be disposed of in a secure manner. This will include archiving to comply with the relevant Acts and legislative requirements. Following expiration of statutory archived documents such records will be destroyed in accordance with prescribed guidelines.

When a breach of privacy or confidentiality occurs, the Notifiable Data Breach Procedure (Annexure A) will be followed, including :

- posting a notification that an eligible data breach has occurred on our website
- Informing the Office of the Australian Information Commissioner.

Compliance Requirements

AAL collects and stores information which is compliant with the provisions of:

1. ***The Privacy Act 2011: Privacy Amendment - Notifiable Data Breaches (NBD) Act 2017*** requires AAL to notify the relevant parties if there is an eligible data breach. Examples of eligible data breaches include, but are not limited to:

    - unauthorised access to, or disclosure of participant information; or information is lost and unauthorised access or disclosure is likely to occur
    - there is a reasonable chance that this could cause the participant serious harm (which can include physical, physiological, emotional, economic or reputational harm)
    - loss, through accidental or inadvertent loss of personal information in circumstances likely to result in unauthorised access of disclosure, e.g. :
        - o loss or theft of physical devices, laptops or storage devices, paper records containing personal information
        - o inadequate identity verification procedures
    - being unable to prevent the likely risk of serious harm with remedial action
    - unauthorised access of personal information made accessible to others outside the organisation.

Examples of NDBs warranting notification will arise when there has been unauthorised access to or unauthorised disclosure of personal information; access or disclosure would likely result in serious harm, to affected individuals e.g. malicious, system fault, or human error such as an email sent to wrong person.

Not all data breaches are eligible data breaches e.g. rapid resolution unlikely to result in serious harm and there is no requirement to notify individuals or the Commissioner.

An overview of a typical data breach response, including the requirements of the NDB scheme is contained in *Annexure A: Data breach response summary diagram* which forms part of this policy.

2. ***Privacy Act 2011*** **and the Australian Privacy Principles (APPs) outlined in the Act**.
   These are:

APP 1	Open and transparent management of personal information
APP 2	Anonymity and pseudonymity - collection of personal information
APP 3	Collection of solicited personal information
APP 4	Dealing with unsolicited personal information
APP 5	Notification of the collection of and dealing with personal information
APP 6	Use or disclosure of personal information
APP 7	Direct marketing
APP 8	Cross-border disclosure of personal information
APP 9	Adoption, use or disclosure of government related identifiers - of personal information
APP 10	Quality of personal information
APP 11	Security of personal information - access to, and correction of, personal information
APP 12	Access to personal information
APP 13	Correction of personal information

Related Documents and Links

Privacy and Confidentiality Guideline: S:\HUMAN RESOURCES\HR POLICIES.FORMS.LETTERS\POLICIES UNDER REVIEW 2015 & 2016\POLICIES IN PROGRESS\Privacy Confidentiality Policy replacing rescinded guideline 05012019.docx

Legislation

Privacy Act 2011: Privacy Amendment (Notifiable Data Breaches) Act 2017: https://www.oaic.gov.au
Privacy Act 2011and the Australian Privacy Principles (APPs) outlined in the Act: https://www.rti.qld.gov.au/information-privacy.act

Data Breach Response Summary

The following diagram provides an overview of a typical data breach response, including the requirements of the NDB scheme.