ARALUEN

IMAGINING BETTER

Privacy

Scope

This privacy policy explains how Araluen collects, uses, discloses and otherwise handles personal information. Failure to appropriately collect, store, use and disclose information can leave Araluen without key information to support participants efficiently and effectively and it also exposes staff and participants to risk. This policy assists employees to:

- understand their obligations in relation to privacy and information security
- become familiar with the relevant legislative and compliance frameworks, including how Araluen will be monitored in relation to privacy and information security
- develop a 'privacy conscious' culture through best practice information

Policy Statement

Araluen is committed to respecting people's human rights, including their right to privacy. Privacy is the term used to explain information that is personal in nature, that identifies who a person is and facts about their life that they may only want some people to know. Araluen collects information about people for a variety of reasons, including information about participants that allows employees to meet their needs and expectations. Araluen will never collect information about anyone in ways that they do not know about or that is unlawful.

Application

The kind of personal information that Araluen collects about individuals depends on the type of dealings they have with the organisation. For example, if a person is someone Araluen supports or is connected to a person Araluen supports (e.g. a family member, carer, advocate or nominated representative), Araluen may collect their:

- name, address, telephone and email contact details
- gender, date of birth and marital status, information about their disability and support needs
- health and medical information

- Medicare number and other identifiers used by Government Agencies or other organisations to identify individuals
- financial information and billing details including information about the services individuals are funded to receive, whether under the National Disability Insurance Scheme or otherwise
- records of interactions with individuals such as system notes and records of conversations individuals have had with Araluen's employees
- information about the services Araluen provides to individuals and the way in which Araluen will deliver those to individuals

Araluen may also collect information about:

- people who attend an Araluen event, including their name, organisation, contact details, payment details (if applicable) and any dietary and accessibility requirements.
- People who engage in Araluen consultation activities such as surveys and focus groups, including their name, organisation contact details and their responses
- People who send Araluen an enquiry, including their name, contact details and the details of their enquiry
- People who visit Araluen's website. Araluen uses 'cookies' and may use tools to track visits to the organisations website including how individuals arrive at the website and which pages they use. Araluen may also collect data to enable the organisation to personalise a webpage or pre-fill a form with their details.
- People who provide feedback or make a complaint. Araluen may collect people's name, contact details, the details of their feedback or complaint, information collected in any investigation of the matter and details of the resolution of a complaint.
- People who apply for a job or volunteer role at Araluen. Araluen may collect information about people included in their application, including their cover letter, resume, contact details and referee reports, their tax file number and other identifiers used by Government Agencies or other organisations to identify individuals, information from police checks, working with children checks (or similar), and information about a person's right to work in Australia.

Araluen employees must only collect information where it is reasonably necessary for Araluen's functions or activities and either:

- the individual has consented or

- Araluen is required or authorised by or under law (including applicable privacy legislation) to do so.

For example, in order to provide Araluen's services to a participant or to respond to a potential participants enquiries about services, Araluen may be required to collect and hold their information including health and medical information and information relating to their disability and support requirements.

Consent

Where Araluen collects personal information about individuals, Araluen employees must take reasonable steps to notify them of certain matters. Employees must do this at or before the time of collection, or as soon as practicable afterwards.

Why does Araluen collect personal information?

Araluen provides a wide range of support services for adults with disability. This range of essential, quality services includes: options for community living, community participation and support coordination.

The main purposes for which Araluen collects, holds, uses and discloses personal information are set out below.

Provision of support services:

- Providing individuals with information about Araluen's services and supports
- Answering people's enquiries
- Delivering Araluen's services and supports and to process payments
- Conducting quality assurance activities including conducting surveys, internal audits and analysis and resolving complaints
- Complying with laws and regulations and to report to funding and Government Agencies.

General administration

- Recruiting employees, contractors and volunteers

Other purposes

Araluen may also collect, hold, use and disclose personal information for other purposes which are explained at the time of collection, purposes which are required or authorised by or under law (including, without limitation, privacy legislation) or purposes for which an individual has provided their consent.

Information collected about individuals that does not identify individuals may be used for research, evaluation of services, quality assurance activities, and regulation. If individuals do not wish for their de-identified data to be used this way, they should contact Araluen.

When someone does not consent to providing Araluen with private information

The nature of the services Araluen provides means that, generally, it is not possible for the organisation to provide services to participants or otherwise deal with individuals in an anonymous way. However, in some circumstances Araluen allows individuals the option of not identifying themselves, or of using a pseudonym, when dealing with the organisation (for example, when viewing Araluen's website or making general phone queries).

Direct marketing

Araluen may use individuals' personal information to keep them informed and up to date about the organisations work, for example, changes to the National Disability Insurance Scheme or information about disability supports, either where Araluen has their express or implied consent, or where Araluen is otherwise permitted by law to do so. Araluen may send this information in a variety of ways, including by mail, email, SMS, telephone, or social media.

Where individuals have consented to receiving marketing communications from Araluen, that consent will remain current until they advise Araluen otherwise. However, individuals can opt out at any time, as explained below.

Araluen website cookies

Araluen uses 'cookies' to manage and improve users' experience on the organisations website. A cookie is a small text file that Araluen's site may place on their computer as a tool to remember their preferences. Individuals may refuse the use of cookies by selecting the appropriate settings on their browser.

Araluen uses tools that tell the organisation when a computer or device has visited or accessed Araluen's content. This allows Araluen to tailor advertising, both on Araluen's website and through advertising networks on other websites, based on their visits or behaviour through cookies on their device. Individuals can control how cookies are used and for what through the settings on their chosen browser.

Araluen also uses Google Analytics to track visits to the organisations website, using this information to track the effectiveness of the website. While this data is mostly anonymous, sometimes Araluen will connect it to individuals, for instance in personalising a webpage, or pre-filling a form with their details. For more information on Araluen's analytics tools, read Google's privacy policy.

Privacy Statement

Through Araluen's Privacy Statement (https://www.araluen.org/privacy-policy/) participants and relevant others are also informed about how their personal information will be used and disclosed, including how their personal information is protected from misuse, loss, unauthorised access, modification and disclosure.

What third parties does Araluen disclose personal information to?

Araluen may disclose personal information to third parties where appropriate for the purposes set out above, including disclosure to:

- Government and regulatory bodies, including the National Disability Insurance Agency, Medicare, the Department of Social Services, the Department of Health & Human Services, and the Australian Taxation Office;
- people acting on their behalf including their nominated representatives, legal guardians, executors, trustees and legal representatives;
- the police, or to the Disability Services Commissioner, or to comply with compulsory notices from courts of law, tribunals or Government Agencies;
- financial institutions for payment processing;
- referees whose details are provided to Araluen by job applicants; and
- Araluen's contracted service providers, including:
    - information technology service providers
    - conference, function and training organisers
    - freight and courier services
    - printers and distributors of direct marketing material including mail houses
    - external business advisers (such as recruitment advisors, auditors and lawyers).

In the case of these contracted service providers, Araluen may disclose personal information to the service provider and the service provider may in turn provide Araluen with personal information collected from individuals in the course of providing the relevant products or services.

Cross border disclosure of personal information

Araluen utilises technology infrastructure that makes use of cloud infrastructure or servers that are located interstate or located out of Australia. Other than this, Araluen does not typically transfer personal information interstate or overseas. By providing their personal information to Araluen or using Araluen's services and supports, individuals are taken to have consented to this transfer.

If Araluen transfers information overseas for other purposes, it will only do so with their consent or otherwise in accordance with Australian law. Araluen will require that the recipient of the information complies with privacy obligations to maintain the security of the information.

Data quality and security

Araluen holds personal information in a number of ways, including in hard copy documents, electronic databases, email contact lists, and in paper files held in drawers and cabinets. Paper files may also be archived in boxes and stored offsite in secure facilities.

Araluen employees must take reasonable steps to:

- make sure that the personal information that Araluen collects, uses and discloses is accurate, up to date and complete and (in the case of use and disclosure) relevant;
- protect the personal information that Araluen holds from misuse, interference and loss and from unauthorised access, modification or disclosure; and
- destroy or permanently de-identify personal information that is no longer needed for any purpose that is permitted, subject to other legal obligations and retention requirements applicable to Araluen.

Unfortunately, there are inherent risks in the management of personal information and Araluen cannot and does not guarantee that unauthorised access to individuals personal information will not occur.

Security

The steps Araluen takes to secure the personal information the organsiation holds include website protection measures (such as encryption, firewalls and anti-virus software), security restrictions on access to Araluen computer systems (such as login and password protection), controlled access to Araluen's premises, policies on document storage and security, personnel security (including restricting the use of personal information by Araluen employees) and training and workplace policies.

Website security

While Araluen strives to protect the personal information and privacy of users of the organsiations website, Araluen cannot guarantee the security of any information that individuals disclose online and individuals disclose that information at their own risk. If individuals are concerned about sending their information over the internet, individuals can contact Araluen by telephone or post.

Individuals can also help to protect the privacy of their personal information by letting Araluen know as soon as possible if individuals become aware of any security breach.

How Araluen handles personal information

Araluen employees must only access and use personal information for a valid work purpose. When handling personal information, employees should:

- confirm recipient details before sending faxes or emails
- always store any hard copies of confidential information that is not being used in a secure cabinet or room
- be aware of the surroundings and people nearby
- limit taking hard copy information away from secure sites
- secure information when travelling e.g. in briefcase, folder etc.
- dispose unneeded copies of information securely
- ensure the information is only available to people who need to access it

Sharing personal information

Araluen employees may only share personal information as set out under this policy and in circumstances permitted under law. To minimise the risk of unauthorised disclosure, employees should:

- check with a manager before sharing confidential information if the basis for sharing is not clear
- not use Internet-based file sharing software to share confidential information (e.g. BitTorrent, Dropbox).

When sharing information with authorised persons via email, employees should:

- where possible, ensure all confidential information is attached to the email in a password protected zip folder
- enable encryption where available
- not include confidential information in the subject line or body of the email
- not send information to or from free web-based email accounts such as Gmail, Hotmail or Yahoo!
- not share or discuss confidential information on social networking applications such as Facebook and Twitter

Passwords

User IDs and passwords for access to computer services are for the sole use of the person to whom they are allocated. Araluen employees should:

- make passwords difficult to guess
- keep all passwords secret and not provide them to another person
- change passwords regularly

Downloading software and applications

Software and applications downloaded from the Internet can contain viruses that threaten the security of information stored on users' computers. Employees should:

- not download unauthorised software from the Internet onto a computer
- lodge a formal request with a manager if software needs to be installed in order to complete work activities

Unsolicited and suspicious emails

Unsolicited emails can contain viruses that threaten the security of information stored on users' computers. If an employee receives an email from an unknown sender and it looks suspicious, an employee should:

- not open the email or click on links contained in its subject line or body
- report the email to a manager and delete the email immediately.

Clear desks and screens

Work environments should be clear of personal information when unattended. This means employees should:

- not leave documents containing confidential information unattended on photocopiers, fax machines or printers
- lock a computer's screen when leaving it unattended
- only print documents when absolutely necessary
- store portable storage devices and hard copies of confidential information in a secure drawer or cabinet, not on a desk.

Information disposal

When disposing of personal information, employees should:

- Place unneeded working documents or copies of information in secure bins or adequate shredders.
- Ensure any electronic media including computers, hard drives, USB keys etc. are sanitised when no longer required.

Visitors

To help minimise the risks to the security of personal information, employees should:

- ensure all visitors are registered and accompanied at all times
- be aware of unaccompanied people who are not known
- notify a manager if an unauthorised person is present on premises.

Portable storage devices

Portable storage devices are usually small and capable of storing large amounts of information, and in some cases can be used to copy, transmit or share information. Examples of portable storage devices include:

- removable media (e.g. CD-ROMs, DVDs, USB drives)
- digital MP3 players (e.g. iPods)
- laptops, tablet computers and slates (e.g. iPads)
- smartphones
- mobile phones.

Using portable storage devices to access, store or transport personal information involves considerable risk because:

- they can be easily lost or stolen, and then accessed by unauthorised people
- using portable storage devices in public or non-work premises increases the chance of accidentally disclosing personal information to unauthorised people.

To minimise the information security risks associated with using portable storage devices, employees should:

- only use encrypted portable storage devices to store personal information
- avoid storing personal information on portable storage devices, where possible
- secure portable storage devices when unattended e.g. lock in a drawer
- be careful of what is said and what information is viewed in public
- report lost or stolen portable storage devices immediately to a manager.

Privacy incidents

Privacy incidents may result from unauthorised people accessing, changing or destroying personal information. Examples of situations from which incidents may arise include:

- accidental download of a virus onto an agency computer
- discussing or sharing of personal information on a social networking website such as Facebook

- loss or theft of a portable storage device containing personal information
- non-secure disposal of hard copies of personal information (i.e. placing readable paper in recycle bin or hard waste bin)
- documents sent to the wrong fax number or email address
- documents sent to a free web-based email account such as Yahoo!, Gmail or Hotmail.

Privacy incidents can:

- occur due to accidental or deliberate actions
- result from human error or technical failures
- apply to information in any form, whether electronic or hard copy.

Incident reporting

It is vital all privacy incidents are reported as soon as possible so that their impact may be minimised. Employees should be aware of:

- how to identify potential privacy incidents
- the reason for reporting incidents is so their impact can be minimised - not to punish individuals
- the need to report all incidents to their manager as soon as they become aware of them.

Araluen must report all participant related privacy incidents to the Office of the Australian Information Commissioner within one business day of becoming aware of, or being notified of a possible privacy incident, or within one business day of an allegation being made of a potential breach by completing Araluen's Incident form (as per the organisation Incident Management policy).

Complaints

If individuals have a complaint about how Araluen has collected or handled their personal information, they should contact Araluen's Quality Team (QualityTeam@araluen.org).

Araluen will ask individuals to explain the circumstances of the matter that they are complaining about, how they believe their privacy has been interfered with and how they believe their complaint should be resolved.

Araluen's Quality Team will complete a review of the complaint in accordance with the organisations Feedback and Complaints procedure. This may include, for

example, gathering the relevant facts, locating and reviewing relevant documents and speaking to relevant individuals.

If the person is unhappy with Araluen's response, they can refer their complaint to the Office of the Australian Information Commissioner (1300 363 992) or, the National Disability Insurance Agencies, Quality and Safeguards Commission (1800 800 110).

Related Documents

Araluen Privacy Statement
Araluen Privacy Document (Easy English)
Documents and Records Management
Code of Conduct