Privacy and Consent Policy

ARALUEN

Imagining and achieving better lives

Scope

This policy applies to all Araluen participants, employees, stakeholders, and anyone who engages with Araluen in the ways specified in section 1.

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 they may only want some people to know. Araluen will never collect information about anyone in ways that they do not know about or that is unlawful.

This policy explains how Araluen collects, uses, handles participants personal information. Failure to appropriately collect, store, use and disclose information can leave Araluen unable to support participants effectively and exposes staff and participants to risk. In relation to privacy, consent and information security, this policy aims to assist employees to:

- Understand their obligations.
- Become familiar with how Araluen is monitored by regulatory frameworks.
- Develop a 'privacy conscious' culture.

Contents

Application

1. Collecting Information

Araluen collects a range of information about individuals, depending on their involvement with the organisation. If the person is a participant at Araluen, we may need to collect their:

General details:	• Name, address, date of birth, phone, email, NDIS number, Medicare number.

Support needs:	• Information about their disability and support needs. • Health and medical information.
Financial details:	• Billing and funding information
Araluen services:	• Notes and records of conversations with Araluen employees. • What services Araluen provides and how it is provided.

Araluen may also need to collect information about people who engage with the organisation that are not participants. This may include people who:

Relatives, carers, next of kin or external support staff of people who attend Araluen	• Name, relationship to Araluen participant, contact details, services received, communications preferences, information provided in an online form or survey.
Attend an Araluen event:	• Name, organisation, contact details, payment details (if applicable), any dietary or accessibility requirements.
Engage in Araluen surveys and focus groups:	• Name, organisation, contact details, their responses.
Send Araluen an enquiry:	• Name, contact details, the details of their enquiry.
Visit Araluen's website:	• How individuals arrived at the website, which pages they use, and data to enable the organisation to personalise a webpage or pre-fill a form with their details.
Provide feedback or a complaint:	• 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.
Apply for a job or volunteer role at Araluen:	• Their application, including their cover letter, resume, contact details and referee reports. • Their tax file number and other identifiers used by Government Agencies. • 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.

The main purposes for Araluen collecting, storing, using, and disclosing personal information are set out below.

Providing Support Services:	• Providing individuals with information about Araluen's services and supports. • Record and answer enquiries. • Delivering Araluen's services and supports and to process payments. • Conducting activities including surveys, internal audits, 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 improvement activities, and regulation. If individuals do not wish for their de-identified data to be used this way, they inform Araluen.

2. Consent

Participants

All Araluen participants must be informed and provide consent about when and how information about them is collected, used, and stored. When participants commence service with Araluen, they are provided a Consent Form to sign. This form asks for consent and explains the following:

- What information Araluen requires.
- Why Araluen requires it.
- How and where it will be stored.
- Who will have access to it.
- How they can access it.

Employee's must explain this form to participants and ensure they understand it before signing. Araluen's Privacy and Consent policy and Consent form must be revisited with participants every year during annual service reviews.

Staff

Araluen employees must be informed when information is collected about them and for what purpose. Please refer to the Recruitment and Selection policy and Performance Management policy for information about when and how the collection, storage and use of employee's personal information is required.

Community Members

Where Araluen collects personal information about individuals from outside of the organisation, such as at an event or via the organisation's website, employees must take reasonable steps to notify them about this. Employees must do this at or before the time of collection, or as soon as practicable afterwards.

When someone does not consent

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).

3. Disclosing Information

Third Party Disclosure

Araluen may disclose personal information to the following third parties where appropriate or required:

- Government 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 behalf of participants including their nominated representatives, legal guardians, executors, trustees, and legal representatives.
- The Victorian Police, 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 while providing the relevant products or services.

Cross-border Disclosure

Araluen uses cloud-based technology 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.

4. Employee Conduct

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

- Confirm recipient details before sending emails.
- Only print hardcopies of confidential information when absolutely necessary
- 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 must:

- Check with their manager or practice leader 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., Dropbox).

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

- Where possible, ensure all confidential information is sent via a onedrive link with limited access.
- 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 media applications.

Passwords

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

- Make passwords difficult to guess.
- Not provide their passwords 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 must:

- Not download unauthorised software from the Internet onto a computer.
- Lodge a request with CT if software needs to be installed to complete work activities.

Unsolicited and Suspicious Emails

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

- Not open the email or click on any links contained within it.
- Report the email to CT and delete it immediately.

Desks and Screens

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

- Not leave documents containing confidential information unattended on photocopiers, fax machines or printers.
- Lock computer screens when leaving unattended.
- Only print documents when absolutely necessary.
- Store portable storage devices and hard copies of confidential information in a locked drawer or cabinet.

Information Disposal

When disposing of personal information, employees must:

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

Visitors

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

- Ensure all visitors are registered and always accompanied.
- Be aware of unaccompanied people who are not known.
- Notify their manager if an unauthorised person is present on premises.

Portable Storage Devices

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 security risks associated with using portable storage devices, employees must:

- Only use encrypted portable storage devices to store personal information.
- Avoid storing personal information on portable storage devices, where possible.
- Lock up portable storage devices when unattended.
- Be careful of what is said and what information is viewed in public.
- Report lost or stolen portable storage devices immediately to a manager.

5. Digital Marketing and Communications

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.

Bulk Digital Communications

Araluen utilises Digital Marketing and Communications platforms, to manage bulk (group) electronic messaging, including emails and SMS. These platforms enables the efficient distribution of:

- Critical service updates
- Important organisational information
- News and announcements
- Occasional marketing and fundraising communications

To facilitate this, Araluen provides any Digital Marketing and Communication platforms with limited personal data strictly necessary for message delivery. This includes name, contact details, connection to Araluen and other information provided to us by the individual for communications purposes.

Recipients have the right to opt out of receiving group communications, either entirely or by message type. However, due to resource constraints, Araluen is unable to offer alternative communication channels for each message type. Therefore, a full opt-out may result in recipients not receiving important updates or information.

Araluen cannot guarantee the security of information within Digital Marketing and Communications platforms. Recipients who enter information while interacting with Araluen via email and SMS generated by Digital Marketing and Communication platforms do so at their own risk.

Users can opt out of receiving Digital Marketing and Communication generated group emails and/or SMS from Araluen by 'unsubscribing' via the links within an SMS or email or notifying Araluen directly.

Website Cookies

Araluen uses 'cookies' to manage and improve users' experience on the organisation's 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 organisation's 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.

6. Security

- The steps Araluen takes to secure the personal information the organisation holds include:
- Website protection measures (such as encryption, firewalls, and anti-virus software).
- Restrictions on access to Araluen computer systems (such as login and password protection).
- Controlled access to Araluen's premises, policies, and documents.
- Personnel security (including restricting the use of personal information by Araluen employees) and training and workplace policies.

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.

Data Quality

Araluen holds personal information in several 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.

Photography and Image Capture

Araluen is committed to safeguarding the privacy and dignity of all participants.

- No Photographs Without Approval
  Employees must not take photographs or videos of participants including to record injuries, incidents, or related matters unless prior approval is granted by a Senior Manager. This restriction applies to all devices, including personal and work-issued equipment.
- Legal and Ethical Basis
  Under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), photographs that identify an individual are considered personal information, and if they include health details, they are classified as sensitive information. Collecting such information requires:
    - A lawful and fair process.
    - Informed consent from the individual or their legal guardian, unless an exception applies (e.g., serious threat to life or health). [oaic.gov.au]
    - Compliance with NDIS Practice Standards and the Incident Management and Reportable Incidents Rules 2018, which require providers to record and manage incidents while respecting participant rights.
- Exceptions
  Photography may only occur without prior consent if:
    - It is necessary to prevent or lessen a serious threat to life, health, or safety, and obtaining consent is impracticable.
    - Directed by law enforcement or regulatory authorities.

- Approval Process
  Where photography is deemed necessary:

1. Obtain approval from a Senior Manager.
2. Ensure the participant (or their guardian) is informed of:
    - Why the image is required.
    - How it will be stored and used.
    - Who will have access.
3. Document consent in the incident report.

- Storage and Security
  Approved images must be:
    - Stored securely in Araluen's incident management system.
    - Never shared via personal devices, social media, or unapproved platforms.
    - Deleted once no longer required for compliance or investigation purposes.
- Prohibited Practices
    - No use of images for marketing, training, or any purpose unrelated to the incident without separate, explicit consent.
    - No uploading to third-party or cloud services unless authorised and compliant with Araluen's data security standards.

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.

7. 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.

Reporting Privacy Incidents

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

8. Access to Your Information

You have the legal right to access the personal information we hold about you. To do so, we ask that requests be made in writing to Araluen's privacy officer.

Araluen reserves the right to request individuals to verify their identity before processing any access or correction requests. This measure ensures that the personal information held by Araluen remains adequately protected.

Typically, we won't charge you for accessing your information. We will provide access within a reasonable time and in the manner you request. However, there are exceptions:

- If we no longer hold or use the information.
- If granting access would unreasonably impact others' privacy.
- If the request is frivolous or unlawful.
- For other reasons allowed by the Privacy Act 1988 (Cth).

If we cannot provide access to all your personal information, we will explain why.

Related Documents

- Araluen's Code of Conduct
- Araluen's Privacy Statement: https://www.araluen.org/privacy/
- Araluen's Consent Form
- Easy English Privacy and Consent policy
- Policy, Documents and Records Management policy
- Computers and Electronic Data policy

Legislation

- NDIS Practice Standards

Review and Authorisation

This policy should be reviewed every two years. The Quality Team along with the Executive Leadership Team will be responsible for reviewing and where necessary updating this policy.

Person responsible: Quality Team
Effective Date: Apr 26
Review Date: Apr 28
Version: 6