Althea PROJECTS

Supporting Townsville since 1974!

FAMILIES | CHILDREN | COMMUNITY

PRIVACY POLICY

Contents

Privacy Statement

Althea Projects is a community service organisation funded by both the Commonwealth and State Governments to deliver a range of programs and support services to individuals, families, and children. To be able to provide these services effectively, we sometimes need to collect personal information from you. Your privacy is very important to us, and we take that responsibility seriously. We want you to feel assured that your information is secure and used only for the purpose of delivering the services you need. In meeting our commitment to protecting your personal information, we comply with Australian privacy laws, which includes:

- The **Privacy Act 1988 (Cth)**, which includes the **Australian Privacy Principles**, and
- The **Information Privacy Act 2009 (Qld)**, which includes the **Queensland Privacy Principles**.

These Acts govern how personal information is collected, handled, used, and disclosed. This policy explains what personal information we collect, why we collect it, who we may share your information with and when, how we keep your information secure, and your privacy rights, including how to make a complaint.

Policy Definitions

Privacy is a human right that, for the purposes of this policy includes the right to control who receives and uses an individual's personal information, and how an individual's personal information is handled.

Personal Information is information or an opinion about an identified individual who is reasonably identifiable from the information or opinion, whether the information or opinion is true or not; and whether the information or opinion is recorded in material form or not. Common examples of personal information under this definition include:

- name, signature, age, gender, postal address, email address, phone number,
- language spoken
- identifiers such as Medicare number or driver's licence number
- financial details, bank details, tax file number
- employment details such as CV/resume
- medical records
- images, photographs or video of individuals (including CCTV footage).

As a rule, the presence of an individual's name in a document is sufficient to make it personal information.

Sensitive information is a specific category of personal information that includes sensitive information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association or trade union
- sexual orientation or practices
- criminal record
- health, genetic and biometric information.

Sensitive information generally requires the individual's written consent for its collection.

Collect/ion refers to acquiring information directly from an individual or from other sources, and in doing so triggering a set of legal obligations for an organisation, such as ensuring the collection is lawful, fair, and done for a purpose that is directly related to their functions. Organisations must also notify individuals at or before the time of collection about what information is being collected, why, and how it will be used.

Collection notice is a document that explains how an organisation will collect, use, and handle an individual's personal information usually provided in writing on forms and/or read aloud as part of obtaining consent prior to collecting the individual's personal information, especially sensitive information.

Consent in relation to solicited information means a voluntary agreement. The individual is adequately informed before giving consent (verbal and/or in writing) and must have the capacity to understand and communicate their consent. This is a freely given, informed, and an explicit agreement by an individual to the collection, use, or disclosure of their personal information for specified purposes. Individuals can withdraw their consent at any time.

Use refers to the internal handling of personal information within Althea Projects including the inclusion of personal information in a publication, taking personal information into account in the making of a decision, or transferring the information from one part of the organisation, with particular functions, to another part of the organisation having different functions.

Disclosure means sharing personal information with an external party outside the organisation. An organisation is considered to have disclosed personal information when:

- It provides the information to another external party who did not previously know it and could not have discovered it independently; and
- The organisation no longer has control over who may access or learn that personal information in the future.

Disclosure does not include situations where an individual is given access to their own personal information.

Access refers to providing an individual with access to their personal information held by an organisation. This may include allowing the individual to inspect the personal information or to obtain a copy of the personal information. This includes the right to make corrections to the information held about them by an organisation.

Information Collection, Use, Storage and Disclosure

Why we collect your personal information

The primary purpose for collecting personal information is to enable us to:

- Assess eligibility
- Complete intake
- Undertaking a needs assessment
- To develop a support or case plan
- To deliver a support service

- To make appropriate referrals
- As required by legislation
- As required by a funded service agreement
- Report to government or other funding bodies on how funding is being used
- For fundraising events and sponsorship arrangements:
- Process a donation or purchase and provide receipts
- Carry out corporate business administrative and financial activities
- Respond to feedback or complaints
- For recruitment purposes including undertaking required legislated suitability checks
- To provide students a placement opportunity

We will only collect information that is necessary, lawful, and required to provide you a service or to carry out our business functions.

Types of information we collect

The type of personal Information we collect will depend upon your relationship with us i.e. client/service user, donor, business partner, employee, volunteer, student or member. Examples of the type of personal information we may collect includes:

- Name, date of birth, gender identity
- Contact details (address, phone, email) and emergency contact details
- Government Identifiers i.e. tax file number, Medicare number, client reference number
- Employment history, qualifications and identification, background/suitability checks, CV/resume
- Photos, video recordings, CCTV footage
- Sponsor details
- Family composition and relationships
- Child protection information
- Housing status
- Financial information/details (e.g. banking details)
- Income and expense information
- Health, disability, or cultural background (where relevant)

How we collection your information

We mostly collect personal information directly from you through the completion of forms, through face-to-face intake or assessment, over the telephone or through email communications. As a contracted service provider, we will also receive personal information contained within referrals received by our services. Further ways in which we may collect information might include:

- Social media comments made on our social media pages
- Through our website contact facilities
- Written correspondence and emails
- Through the CCTV systems at our worksites
- Photos / videos taken during our events and activities

In collecting personal information, and particularly sensitive information, we ensure this is managed in an open and transparent manner through a collection notice. Collection notices are program or service specific. The privacy principles obligate us to only collect personal information

that is necessary for the purpose of carrying out our functions and activities, and in as non-obtrusive way as possible. Individuals do have the right to withhold information for privacy reasons.

How we deal with unsolicited information

Unsolicited information is any personal information we might receive that we did not purposely collect, for example:

- Job applications sent to us when we have not advertised or are hiring
- Extra details in a form that was not required, i.e. an individual using our services writes their medical history in a feedback form that only asked for service feedback.
- Social media messages, i.e. an individual sends personal details through a direct message that the organisation did not ask for.
- Third-party referrals without consent, i.e. another organisation forwards someone's personal information to us without prior agreement to do so.
- CCTV footage, i.e. incidental footage captured of individuals by our building CCTV cameras that is not required for the reason for why the system is in place.

When we receive unsolicited information, we will assess and determine if we could have lawfully collected it within the privacy laws and if it was not lawfully collected and if it is not considered a public record, then we will destroy or de-identify it as soon as practicable. If it is assessed to have been lawfully collected, it will be handled in accordance with the privacy principles and our personal information handling procedures.

How we store and protect your information

We store your personal information in paper form or electronically. Paper records are stored in locked cabinets and electronic records are stored in databases and cloud-based platforms. To keep your personal information safe from loss, unauthorised access, or misuse, we have strong security measures in place, including:

- Locked cabinets for paper records and password-protected systems for electronic records.
- Multi-factor authentication and regularly updated cybersecurity tools including device and network protections.
- Access controls so only authorised staff can view personal information.
- IT Access Register maintained regarding individual staff access and permissions levels.
- A "clean desk" policy requiring information to be stored securely when not in use.
- Staff training on privacy, confidentiality, and cyber security.
- Policy and procedures regarding the handling of information and conduct standards regarding the appropriate use of organisational devices.
- Personal information kept only for as long as necessary or as required by law and in accordance with our Record Management, Retention and Destruction policies.
- Secure disposal of documents when they are no longer needed in locked shred bins.

How we use and may disclose personal Information

We only use or share your personal information for the purpose that it was collected. We will only use it for secondary purposes if you give consent (for example, for research). Otherwise, we would only disclose your personal information if directed by law, such as:

- When someone's safety is at risk.
- When we believe a serious crime has happened or may happen.
- Reporting workplace incidents to safety regulators.
- Child protection requirements, such as:
    - When harm to a child or young person is suspected or disclosed.
    - When it is in the best interests of a child or young person.
- Requests from courts, tribunals, government agencies, or other lawful authorities.

We may use government-issued identifiers (such as numbers) to confirm identity when required by law or funding agreement or required as part of us carrying out our business and functions and providing a service. Staff will never use or share your identifiers for any other purpose.

We may also disclose by consent when making a referral on your behalf and at your request.

Disclosure outside of Australia

Under the privacy laws, we can only disclose personal information overseas in limited circumstances. This may occur if data is stored on cloud servers located outside Australia. We would only share personal information outside Australia if:

- You have agreed to the disclosure.
- The disclosure is required or authorised by law.
- It is necessary to prevent or reduce a serious threat to someone's life, health, or safety, or
- We have taken reasonable steps to ensure the overseas recipient protects the information in line with Australian privacy laws.

We can also not disclosure your information outside Australia without written consent from our funding bodies, therefore, it not likely we would disclose your personal information overseas.

Destroying personal information

We securely destroy or permanently de-identify personal information when we no longer need it or when we are no longer legally required to keep it. This includes:

- Complying with legal and regulatory retention requirements before disposal.
- Using secure destruction methods
- De-identifying data by removing personal details so it cannot identify anyone.
- Using only trusted third-party services for secure document disposal.
- Keeping registers of when and how information was destroyed.
- Regularly reviewing to identify opportunities for secure disposal.

Use of Artificial Intelligence

We use secure Artificial Intelligence (AI) tools, such as Microsoft Copilot, to help with internal administration tasks like preparing or summarising documents and improving operational efficiency. These tools, however, are never used in case management circumstances or in the

handling of sensitive information. We would only enter personal information into an AI system if it was necessary, and only by consent. If we do, the same privacy safeguards apply under the Privacy Act 1988 (Cth) and the Information Privacy Act 2009 (Qld).

How we respond to data breaches

We take data breaches very seriously. If a breach occurs, we follow our Data Breach Response Plan Policy in meeting all legal requirements, which includes taking immediate action to remedy, undertake an assessment and investigation and to notify those affected. This includes notifying affected individuals and, where required, informing the Australian Information Commissioner and/or the relevant funding body.

Direct Marketing

We do not undertake direct marketing activities, therefore, would not disclose any personal information for the purpose of direct marketing.

Website Cookies and the Use of Google Analytics

We use cookies and similar tools to ensure our website works properly and to understand how people use it. We keep this use minimal and avoid collecting personal information wherever possible.

We use Google Analytics to improve our website. This tool is configured to protect your privacy and as such:

- IP addresses are anonymised.
- No personal or sensitive information is collected or linked to client records.
- Data is retained for two months, then automatically deleted.

The information collected is general, such as time spent on the site, pages visited, and device type. It is combined and used only to improve services, not to identify individuals. Google may store anonymised data on servers outside Australia, which is standard for analytics services. No personal information is shared with Google. You can opt out of analytics cookies through your browser settings or Google's opt-out tools. This will not affect your access to our website. We do not use cookies for advertising, profiling, or tracking across other websites.

Links to External Websites

Our website may include links to third-party websites. These sites operate under their own privacy policies, which may differ from ours. We are not responsible for the privacy practices or content of any linked websites.

CCTV

We use CCTV systems at most of our program sites. The purpose of these surveillance systems is to monitor for safety and to record data for retrieval purposes when there is a serious reportable incident involving the threat or actual harm of staff, clients, visitors, or property, and/or in the pursuance of criminal prosecution. In compliance with privacy laws regarding the use of CCTV, we must:

- Give you notice that your image may be captured before you are recorded, and
- Make sure recorded personal information is secure and destroyed or de-identified when it is no longer needed.

We give notice about our CCTV through signage displayed at program entrances and near each camera site. By entering our premises, you are giving implied consent for your personal information to be collected through surveillance footage.

We do not disclose any personal information gained from our CCTV for any other purpose than which it is obtained. Footage that is not used or disclosed for that purpose, is deleted (or written over) within a set timeframe which is usually between 30 to 90 days.

Footage disclosed for the purpose it was obtained is kept in line with retention timeframes until required to be archived or destroyed.

Please request a copy of our Camera Surveillance Privacy Statement if you would like further information.

Your Rights

Anonymity and using a pseudonym

You have the right to withhold your personal information or to use a pseudonym when accessing services. However, but under privacy laws there are exceptions where we may need to identify you, such as:

- Where it is impracticable for us to provide you with a service without knowing your identity
- The law requires identification.
- Health or safety reasons if someone's life, health, or safety is at risk, we may need an individual's personal information to act appropriately if we are providing a care environment.
- When Government-related identifiers are required to access specific services i.e. Medicare or Centrelink numbers to verify identity for funded programs or legal compliance.

While anonymity is a right, it cannot apply where **legal, safety, or operational requirements make identification necessary**. Where the above applies, we will clearly explain these in our collection notices for the relevant service.

Access and Correction

You have the right to access your personal information that is held by us unless it is restricted by law. You can make this request through the manager of the program area you are engaged with or through Althea Projects Privacy Officer. You also have the right to request that your personal information be amended or corrected if you believe it is inaccurate, out of date, incomplete, irrelevant or misleading. This may include the information being destroyed and updated or you providing a written statement to be placed in your personal information held by us.

Upon request for access or correction, you will be provided with an **Information Request form** to complete in which to outline the specific documents you want access to or to correct. If your access request is not approved, you will be given the reasons for this in writing. If approved, a nominated person will be allocated to assist you with your access.

Privacy Concerns and Complaints

If you have any concerns or questions in relation to this privacy policy or the collection of your personal information, please contact the relevant Program Manager.

If you believe we have breached the privacy laws in relation to how we have handled of your personal information, you can make a privacy complaint to our Privacy Officer via the details below. All privacy complaints will be investigated and finalised within 45 days and in accordance with our **Complaints policy**, which you can view on our website.

Althea Projects Privacy Officer
Email: ceo@altheaprojects.org.au
Phone: 4779 3332
Address: PO Box 905, Aitkenvale Q 4814

You may also submit your concern or complaint via our website using the electronic feedback form at www.altheaprojects.org.au.

If you are not satisfied with the outcome of your complaint, you may then refer your privacy complaint to any of the following:

- Office of the Information Commissioner on (07) 3234 7373 or www.oic.qlg.gov.au,
- Office of Information Commissioner Queensland on (07) 3234 7373 or 1800 642 753 or www.oic.qld.gov.au, or
- Contacting the relevant program's funding body.

Policy Updates

This policy will be reviewed and updated periodically to ensure it remains current and compliant with applicable laws and organisational requirements.

Policy last updated 16.12.2025
Policy Authorised by Paula La Rosa, Chief Executive Officer