

CATEGORY: ALL SERVICES**TOPIC: PRIVACY****POLICY**

South Burnett CTC Inc (CTC) are bound by, and champion, the *Privacy Act 1988*, including the Australian Privacy Principles (APPs). The APPs set out the standards, rights and obligations for how personal information is collected, stored, used, disclosed, quality assured and secured. CTC respects the privacy of all stakeholders and is committed to safeguarding the personal information that is provided to us.

Purpose

The purpose of this policy and procedure is to outline CTC's requirements with regards to information kept for the provision of services. CTC will:

- Make its policy on the management of personal information available to anyone who asks for it
- Ensure each staff member and each of their clients have knowledge about the control and the flow of that client's personal information
- Ensure premises provide for privacy for clients, including those with special needs
- Provide new staff with a copy of CTC's Privacy Statement and Policy and Procedure
- Ensure new staff complete the Office of the Information Commissioner Queensland (OICQ) online training to gain a Certificate of Completion of Queensland – Information Privacy Act
- Have a designated Privacy Officer
- Not use personal information of any type outside of which it was originally intended upon collection (without consent), but particularly not for direct marketing, email marketing or telemarketing to try and sell goods or services
- Ensure the organisation follows the below process for an identified data breach that meets all the requirements for managing Notifiable Data Breaches as required under the Privacy Act 1988 (Cth) and that it is accessible to staff
- Continue to review the organisation's Certificate of Insurance in relation to Cyber Liability
- Ensure open and transparent management of privacy by posting the CTC Privacy Statement on the website, where it is readily accessible and visible, as well as post the statement internally on the staff intranet and the Board of Governance portal.

The Privacy Act and this Privacy Policy does not apply to acts or practices which directly relate to employee records of CTC's current and former employees, as per the APP exemption provided to private sector employers.

Scope

This policy and procedure applies to all CTC staff (inclusive of employees, volunteers, contractors, visitors, or any other person engaged by CTC to perform work). This policy and procedure applies to all information held by CTC for the purpose of the provision of services (excluding employee records).

Related Legislation and Resources

The Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cwth). 13 APPs – Annexure A
 The Information Privacy Principles (IPPs) under the Queensland – Information Privacy Act 2009 as a de-facto agency (other than health agencies as outlined in Chapter 2 Part 4). 11 IPPs and 9 NPPs (only applicable if funding is provided by a Health Agency) – Annexure A

[Privacy Regulation 2013](#)

[Child Protection Regulation 2023 \(Section 29\)](#)

[Office of the Australian Information Commissioner – Data Breach Preparation and Response](#)

[The Domestic and Family Violence Information Sharing Guidelines 2023](#)

[Department of Families, Seniors, Disability Services and Child Safety - Information Sharing Guidelines](#)

[Department of Families, Seniors, Disability Services and Child Safety - Recordkeeping Guide for Funded Non-Government Organisations](#)

[Practice principles, standards and guidance | Department of Families, Seniors, Disability Services and Child Safety](#)

Related Policies and Procedures

Business Continuity Plan

[Code of Ethics](#)

[Complaints Management and Resolution Policy and Procedure](#)

[Induction, Orientation and Ongoing Training and Development Policy and Procedure](#)

[Information Technology Policy and Procedure](#)

[Privacy Statement](#)

[Privacy Policy and Procedure – Partners in Foster Care](#)

[Recordkeeping Policy and Procedure – Partners in Foster Care](#)

[Recordkeeping and Information Security Policy and Procedure – All Services](#)

Definitions

Australian Privacy Principles (APPs)	Replaced the National Privacy Principles and Information Privacy Principles. There are 13 APPs from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988.
Client	Those who access South Burnett CTC’s services.
Information Privacy Principles (IPPs)	The 11 Information Privacy Principles as extracted from section 14 of the Privacy Act 1988 (Cth)
Notifiable Data Breach	When a data breach involving personal information is likely to result in serious harm.
Staff	Any individual employed by CTC, regardless of employment status, performing duties on behalf of CTC.

PROCEDURE

The Service Deed/Contract is the primary source of CTC's privacy obligations in relation to its activities when under a Commonwealth Government contract. If a provision of a Commonwealth contract authorises CTC to do an act or practice that would otherwise breach the APPs, an act done or practice engaged in for the purposes of meeting that obligation does not breach the APPs. Service Managers who are responsible for a Commonwealth Contract/s will check the relevant documentation to ensure they understand the degree to which the privacy principles apply and also understand the circumstances in which the provisions of the Deed/Contract override the principles.

What is deemed Personal Information?

Personal information as defined by the *Privacy Act 1988 (Cwth)* is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not. Examples of personal information can include a person's name, address and date of birth, bank account details, photos, videos, digital identifiers such as IP address and metadata, and even information about what an individual likes, their opinions and where they work. Personal information as defined by the *Queensland Information Privacy Act 2009* is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Collection and Control of Individual Client's Personal Information

Each service/program has a specific Client Intake process/form which staff must use to ensure they and each of their clients have knowledge about the control and the flow of that client's personal information. Staff are able to seek further information or clarification of individual service/program practices from their relevant Service Manager and/or designated Privacy Officer.

Where possible, collection of personal and sensitive information will be directly from the individual. In some situations, we may also obtain personal information from a third-party source. If we collect information in this way, we will take reasonable steps to ensure the individual is aware of the purposes for which we are collecting personal information and the organisations to which we may disclose the information, subject to any exceptions under an Act.

If funding is received through a state Health Agency, when collecting health information, CTC will obtain consent to such collection and explain how the information will be used and disclosed.

If a person feels that the information that we are requesting, either on our forms or in our discussions, is not information that they wish to provide, they should raise this with us.

If anyone would like to access any CTC Services on an anonymous basis or using a pseudonym, they should tell us. If this is possible and lawful, we will take all reasonable steps to comply with the request. However, we may not be able to provide the services in question if we are not provided with the personal information requested.

The nature and extent of personal and sensitive information collected by CTC varies depending on the particular interaction with the organisation.

CTC collects personal and sensitive information from clients, business partners, staff, members and online users. Further information about the kind of information collected from each of these groups and the usage of such information is detailed below.

Clients

- contact details
- personal details including: date of birth, gender, income source
- employment details
- information on personal issues and experiences, relationships
- family background, supports clients may have in the community
- areas of interest
- sensitive information (eg. ethnic and racial origin, court orders/restrictions etc)
- health information

Primary purpose for which information is collected:

- to determine eligibility to access service/s based on guidelines
- to assess client needs
- to plan and provide services and supports
- to enable communication with emergency contacts, advocates, employers (if required), treating professionals, government departments
- to develop an individual support plan
- to provide reporting to Government

Secondary purpose for which information may be used:

- to comply with legal obligations
- to develop a service and track progress and outcomes of each intervention
- to determine appropriate referrals and management to other services within or outside the organisation
- to monitor and evaluate existing services and plan for future services
- to measure quality of service provision
- for data inputs for business, operations and resources
- to determine billing and invoice requirements
- to produce annual reports and for research purposes which may involve contracted organisations
- to apply for funding

Business Partners

- contact person's name, the name of the organisation which employs the person, telephone numbers, fax number, street and postal address, email address and position title
- bank details (if receiving payment or making payment for services received)
- Australian Business Number (ABN)
- type of support (e.g. workplace giving, goods in kind, program support, volunteering)

Primary purpose for which information collected:

- to provide services
- to pay for services
- to establish and manage partnerships
- to receive services

Secondary purpose for which information may be used:

- to manage the relationship with the business partner
- to provide information about the organisation's services

Staff (volunteers, employees, delegates) and applicants for volunteer work and prospective employees

- contact details
- personal details, including personal details of emergency contact person(s)
- date of birth
- identification details/documents required for the lodgment of suitability checks (eg. country of birth, citizenship, residency and/or visa details)
- details of current/previous employment or volunteer involvement
- skills, experience and training
- qualifications, drivers licence details
- information and opinions from referees for prospective employees and applicants for volunteer work
- Suitability Checks as required under relevant legislation

Primary purpose for which information is collected:

- to provide services
- to process an application to become a member, volunteer or employee of our organisation
- to facilitate a placement in an appropriate service or position
- to assist with services whilst the individual is employed or engaged as a volunteer
- to provide feedback on performance as a volunteer or employee
- to meet legislative responsibilities to all volunteers and employees
- to obtain feedback from individuals about their experiences

Secondary purpose for which information may be used:

- to assist in reviewing and improving programs and services to keep individuals informed about the organisation's developments and opportunities
- to provide information about the organisation's services
- to facilitate further involvement with the organisation

Members

- contact details
- date of birth
- areas of interest

Primary purpose for which information is collected:

- to provide services
- to provide communication updates and ensure transparency

Secondary purpose for which information may be used:

- to provide information about the organisation
- to receive invitations to upcoming events and activities
- to recognise your support of the organisation

Online Users

- contact details
- non-personal information eg. visitor navigation and statistics
- server address, browser type, date and time of visit
- personal information

Primary purpose for which information is collected:

- to analyse website usage and make improvements to the website

Use and disclosure of Personal Information

CTC only uses personal information for the purposes for which it was given to us, or for purposes which are related to one of our functions or activities. We may disclose personal information to other external organisations including:

- Government departments/agencies who provide funding for CTC services (statistics only, unless directly specified)
- Contractors who manage some of the services we offer. Steps are taken to ensure they comply with the relevant Privacy Principles when they handle personal information and are authorised only to use personal information in order to provide the services or to perform the functions required by CTC
- Other regulatory bodies, such as WorkCover
- As referees for past employees/volunteers, and referees of applicants for CTC positions
- Our professional advisors, including our accountants, auditors and lawyers

Except as set out above, CTC will not disclose an individual's personal information to a third party unless one of the following applies:

- the individual has consented
- the individual would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information – directly related to the purpose for which it was collected)
- it is otherwise required or authorised by law
- it will prevent or lessen a serious threat to somebody's life, health or safety, or to public health or safety
- a child is at risk of harm
- we are required to provide information under legislation when requested by a statutory body appropriately and in writing
- it is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities
- it is reasonably necessary to assist in locating a missing person
- it is reasonably necessary to establish, exercise or defend a claim at law
- it is reasonably necessary for a confidential dispute resolution process
- it is necessary to provide a health service
- it is necessary for the management, funding or monitoring of a health service relevant to public health or public safety
- it is necessary for research or the compilation or analysis of statistics relevant to public health or public safety
- it is reasonably necessary for the enforcement of a law conducted by an enforcement body

We do not usually send personal information out of Australia. If we are required to send information overseas we will take measures to protect personal information. We will protect personal information either by ensuring that the country of destination has similar protections in relation to privacy or that we enter into contractual arrangements with the recipient of your personal information that safeguards privacy.

Artificial Intelligence (AI)

Privacy obligations will apply to any personal information input into an AI system, as well as the output data generated by AI (where it contains personal information). If AI systems are used to generate or infer personal information, including images, this is a collection of personal information and must comply with APP 3.

If personal information is being input into an AI system, APP 6 requires entities to only use or disclose the information for the primary purpose for which it was collected. AI tools should never be used to access, store, or share personal or sensitive data beyond what is necessary for the specific purpose.

As a matter of best practice, CTC follows the OAIC recommendation that organisations do not enter personal information, and particularly sensitive information, into publicly available AI chatbots and other publicly available generative AI tools, due to the significant and complex privacy risks involved. Staff are to always use Microsoft CoPilot for AI use of internal CTC data.

AI should not be used to collect or analyse personal data without obtaining explicit, informed consent from the individuals involved.

Any data or content generated by AI systems, especially in research or strategic planning, must be treated as confidential unless otherwise directed.

Where appropriate, stakeholders should be informed about the role of AI in decision-making processes, and the rationale behind AI-driven outcomes should be explainable and understandable.

Security of Personal and Sensitive Information

CTC takes reasonable steps to protect the personal and sensitive information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.

These steps include password protection for accessing our electronic IT system, securing paper files in locked cabinets and physical access restrictions. Only authorised personnel are permitted to access these details.

When personal information is no longer required, it is destroyed in a secure manner, deleted appropriately or otherwise treated in relation to legislation or contractual requirements.

Access to and Correction of Personal Information

If an individual requests access to the personal information we hold about them, or requests that we change that personal information, we will allow access or make the changes unless we consider that there is a sound reason under the relevant Privacy Act or other relevant laws to withhold the information, or not make the changes.

Requests for access and/or correction should be made to the Privacy Officer. For security reasons, requests must be in writing and provide proof of identity. This is necessary to ensure that personal information is provided only to the correct individuals and that the privacy of others is not undermined.

In the first instance, CTC will generally provide a summary of the information held about the individual. It will be assumed (unless told otherwise) that the request relates to current records. These current records will include personal information which is included in CTC databases and in paper files, and which may be used on a day-to-day basis.

We will provide access by allowing a person to inspect, take notes or print copies of personal information that we hold about them. If personal information (for example, name and address details) is duplicated across different databases, CTC will generally provide one printout of this information, rather than multiple printouts.

We will take all reasonable steps to provide access to, or a copy of, the information requested within 14 days of a request. In situations where the request is complicated or requires access to a large volume of information, we will take all reasonable steps to provide access to the information requested within 30 days.

CTC may charge reasonable fees to reimburse us for the cost we incur relating to a request for access to information, including in relation to photocopying and delivery cost of information stored off site. For current fees, please contact the Privacy Officer.

If an individual is able to establish that personal information CTC holds about her/him is not accurate, complete or up to date, CTC will take reasonable steps to correct our records.

Access will be denied if:

- the request does not relate to the personal information of the person making the request
- providing access would pose a serious threat to the life, health or safety of a person or to public health or public safety
- providing access would create an unreasonable impact on the privacy of others
- the request is frivolous and vexatious
- the request relates to existing or anticipated legal proceedings
- providing access would prejudice negotiations with the individual making the request
- access would be unlawful
- denial of access is authorised or required by law
- access would prejudice law enforcement activities
- access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of CTC
- access discloses a 'commercially sensitive' decision making process or information
- any other reasons that are provided for in the Privacy Principles/Privacy Acts

If we deny access to information, we will set our reasons for denying access. Where there is a dispute about the right of access to information or forms of access, this will be dealt with in accordance with the complaints procedure set out below.

Complaints Procedure

If a person has a complaint about CTC's privacy practices or our handling of personal and sensitive information, they should contact our Privacy Officer who will direct them to our *Complaints Management and Resolution Policy and Procedure*.

Once the complaint has been made, we will try to resolve the matter in a number of ways such as:

- Request for further information.
- Discuss options: We will discuss options for resolution and suggestions about how the matter might be resolved
- Investigation: Where necessary, the complaint will be investigated. We will try to do so within a reasonable time frame. It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to progress a complaint
- Conduct of our employees: If a complaint involves the conduct of our employees, we will raise the matter with the employee concerned and seek their comment and input in the resolution of the complaint
- The complainant will be notified if their complaint is found to be substantiated. We will then take appropriate agreed steps to resolve the complaint, address concerns and prevent the problem from recurring
- If the complaint is not substantiated, or cannot be resolved to the complainant's satisfaction, CTC may either refer the issue to an appropriate intermediary or advise the complainant to elevate their complaint to a relevant external agency
- At the conclusion of the complaint, if the complainant is still not satisfied with the outcome they are free to take their complaint to the Office of the Australian Information Commissioner at <https://www.oaic.gov.au/> or the Office of the Information Commissioner Queensland at <https://www.oic.qld.gov.au/>.

We will keep a record of the complaint and the outcome.

We are unable to deal with anonymous complaints. This is because we are unable to investigate and follow up such complaints. However, in the event that an anonymous complaint is received we will note the issues raised and, where appropriate, try and investigate and resolve it appropriately.

DATA BREACH RESPONSE PLAN/PROCEDURE

A data breach is defined as a situation where:

- There has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or
- Such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure, or
- There is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure

Relevant data can include data such as personal information, credit information, case notes, tax file numbers etc. A real risk of "serious harm" can include physical, psychological, emotional, economic and financial harm, and also includes serious harm to reputation.

The following procedure must be followed in the event of a serious data breach or there is evidence that a serious data breach may have occurred:

- Staff members becoming aware of a situation contain the breach (e.g. stop the unauthorised practice, recover the records or shut down the system that was breached) and/or inform their Team Leader/Service Manager immediately so they can prevent access or minimise impact
- Team Leader/Service Manager meet as soon possible with the CEO and IT Manager and do a preliminary assessment:
 - What information does the breach involve?
 - What was the cause of the breach?
 - What is the extent of the breach?
 - What are the harms (to affected persons) that could potentially be caused by the breach?
 - What is the risk of harm to others (e.g. reputational damage, legal liability)
 - How can the breach be further contained?
- If it is assessed that the data breach creates a real risk of serious harm to a person, the Office of the Australian Information Commissioner (OAIC) as per the Mandatory Data Breach Notification Scheme and the affected person should be notified by a staff member nominated by the CEO. Notifications should include recommendations to take remedial steps to lessen the adverse impact that might arise from the breach.
- If appropriate, notify other third parties (e.g. Insurance Providers, Financial Institutions, Regulatory Bodies).
- Once immediate steps have been taken to mitigate the risks associated with a breach, investigate the cause of the breach and recommend outcomes (e.g. changes to policies and procedures, revise staff training practices, update this Response Plan if necessary)

VERSION CONTROL

1.0	02/08/2010	2.0	01/07/2012	3.0	01/03/2014	4.0	08/09/2014
5.0	13/03/2017	6.0	26/07/2017	7.0	18/10/2018	8.0	06/12/2019
9.0	23/09/2025						

AUTHORISATION

Name	Jason Erbacher
Position	Chief Executive Officer

ANNEXURE A – Privacy Principles Summary

IPP		APP	
1	Collection of personal information (lawful & fair)	1	Open & Transparent Management of Personal Information
2	Collection of personal information (requested from individual)	2	Anonymity and Pseudonymity
3	Collection of personal information (relevance etc)	3	Collection of solicited personal information
4	Storage and security of personal information	4	Dealing with unsolicited personal information
5	Providing information about documents containing personal information	5	Notification of the collection of personal information
6	Access to documents containing personal information	6	Use of disclosure of personal information
7	Amendment of documents containing personal information	7	Direct Marketing
8	Checking of accuracy of personal information only for relevant purpose	8	Cross-border disclosure of personal information
9	Use of personal information only for relevant purpose	9	Adoption, use or disclosure of government related identifiers
10	Limits on use of personal information	10	Quality of personal information
11	Limits on disclosure	11	Security of personal information
		12	Access to personal information
		13	Correction of personal information

- 1 NPP1 - Collection of personal information
- 2 NPP2 - Limits on use or disclosure of personal information
- 3 NPP3 - Data quality
- 4 NPP4 - Data security
- 5 NPP5 - Openness
- 6 NPP6 - Access to documents containing personal information
- 7 NPP7 - Amendment of documents containing personal information
- 8 NPP8 - Anonymity
- 9 NPP9 - Sensitive information