

Privacy Policy

Think Community Services (TCS)

Version 2.0 | 31 August 2026 | 31 August 2029

Document ID	DAT-POL-02
Domain	Data
Type	Policy
Service	All TCS Services
Status	Active

Record of Document Control

Version	Approval Date	Approved By	Owner	Summary of Changes	Next Review Date
1.0	23 September 2022	Think Management Team	Directors	Nil, first version	23 September 2025
2.0	31 August 2026	Board of Directors	Executive Directors	Structure updated. Board added as approval authority. Scope table added per service. Monitoring section added.	31 August 2029

Think Mental Health acknowledge the Traditional custodians on the land on which we live and work, and of the many different nations across the wider regions from which we all come. In Canberra this is the Ngunnawal people. We pay our respects to the Elders past, present and emerging as the holders of the memories, the traditions, the culture and the spiritual wellbeing of the Aboriginal and Torres Strait Islander peoples across the nation.

Contents

Contents	2
1.0 Purpose	3
2.0 Scope	3
3.0 Policy Statement	3
4.0 Guiding Principles	4
5.0 Responsibilities	4
5.1 Policy Development or Review	6
6.0 Policy Requirements	6
6.1 Collection of Personal Information	6
6.2 Storage and Access	6
6.3 Use and Disclosure — With Consent	7
6.4 Use and Disclosure — Without Consent (Exceptions to Confidentiality)	7
6.5 Consumer Rights — Access, Correction, and Complaints	7
6.5.1 Notification of Changes to Privacy Policy	8
6.6 Data Breach Response	8
6.7 Professional Supervision and Peer Consultation	8
7.0 Implementation	8
8.0 Compliance Monitoring	9
8.2 Privacy Impact Assessments	9
9.0 Related Documents	10
10.0 References and Legislation	11

1.0 Purpose

This policy establishes Think Community Services (TCS's) approach how to collect, store, use, disclose, and manage personal information in the delivery of health services. It establishes the obligations of all staff and the rights of all individuals whose information is collected and managed by TCS.

The purpose of this policy is to:

- Define how TCS collects, stores, uses, discloses, and manages personal information.
- Ensure compliance with the Privacy Act 1988 (Cth), Australian Privacy Principles, and Health Records (Privacy and Access) Act 1997 (ACT).
- Establish consumer rights regarding access to, correction of, and complaint processes relating to their personal information.
- Define TCS's obligations in the event of a data breach, including under the Notifiable Data Breaches Scheme.
- Ensure all staff understand their individual and organisational privacy obligations across all services and channels.
- Ensure policies reflect best practice, legislative obligations, and applicable standards and accreditation requirements.

2.0 Scope

This policy applies to all Think Community Services staff, contractors, and governing body members involved in the collection, access, use, or disclosure of personal information. It applies across all services, programs, and operational areas. All staff are bound by the legal requirements of the Australian Privacy Principles under the Privacy Act 1988 (Cth) and the Health Records (Privacy and Access) Act 1997 (ACT).

This policy applies to all TCS policy documents, including policies, procedures, guidelines, and protocols. It does not apply to individual consumer support plans, clinical documentation, or operational work instructions that fall outside the policy suite.

3.0 Policy Statement

Think Community Services is committed to protecting the privacy and confidentiality of all consumers, carers, staff, and other individuals whose personal information is collected and managed. Privacy is a fundamental consumer right and a core component of ethical, person-centred mental health service delivery. TCS collects only the information necessary to provide safe, high-quality services and uses it only for the purposes for which it was collected.

This policy aligns with:

- The principles of recovery, trauma-informed care, and human rights
- The organisation's mission, values, and applicable legislative, regulatory, contractual, and accreditation requirements relevant to the services delivered by TCS
- The Information and Data Governance Framework
- The Data Governance and Records Management Policy

- The Consent and Confidentiality Policy
- The Code of Conduct
- Privacy Act 1988 (Cth) and the Australian Privacy Principles
- Health Records (Privacy and Access) Act 1997 (ACT)
- Information Privacy Act 2014 (ACT).

4.0 Guiding Principles

This policy is guided by the following principles:

Table 1 – *Guiding principles of this policy*

Principle	Description
Consumer Participation	Consumers are informed about how their personal information is collected, used, stored, shared, and protected. Consumers are supported to access, correct, and understand their personal information and privacy rights
Safety and Quality	Personal information is collected, used, and managed to support the safe, effective, and coordinated delivery of services. Information is protected from unauthorised access, disclosure, loss, or misuse through appropriate privacy and security controls
Evidence-Informed	Privacy practices are guided by applicable legislation, regulatory requirements, recognised standards, and best practice approaches to information management and consumer rights
Cultural Responsiveness	Privacy practices are culturally safe, respectful, and responsive to the diverse needs, values, and expectations of Aboriginal and Torres Strait Islander peoples, culturally and linguistically diverse communities, and other priority populations
Transparency and Accountability	TCS is transparent about how personal information is collected, used, stored, and disclosed. Staff are accountable for protecting privacy, maintaining confidentiality, and complying with organisational, legal, and ethical obligations. Privacy breaches are managed, documented, and investigated in accordance with organisational requirements
Continuous Improvement	Privacy practices, security controls, and information management processes are regularly reviewed and improved through audits, incident reviews, legislative updates, consumer feedback, and organisational learning
Accessibility	Consumers are supported to access their personal information, request corrections, and understand privacy-related information in a timely, equitable, and accessible manner

5.0 Responsibilities

Table 2 – *Responsibilities of specific roles in TCS*

Role	Responsibility
------	----------------

Board of Directors	• Hold ultimate accountability for TCS's compliance with privacy legislation • Approve this policy • Receive reports on privacy breaches and compliance
Executive Directors — Think Community Services	• Hold ultimate executive accountability for the policy suite and its alignment with governance obligations, accreditation standards, and legislative requirements • Escalate strategic or high-risk policies to the Board for approval
Senior Management Committee (SMC)	• Endorse and approve policies within delegated authority • Monitor data governance compliance • Receive reports on breaches and compliance
Quality Improvement Committee (QIC)	• Review draft policies for compliance, clarity, and alignment with quality and safety frameworks • Monitor the Document Register to ensure policies are reviewed on schedule • Identify policy gaps arising from incidents, audit findings, or accreditation requirements
Consumer Advisory Group (CAG)	• Contribute consumer perspectives on privacy practices and consumer-facing privacy materials. • Review the consumer privacy notice.
People and Administrative Services Manager	• Ensure personal information collected through recruitment, employment, credentialing, training and workforce processes is only collected, used and disclosed for authorised purposes
Policy Owner	• Draft, consult, and review policies within their area of responsibility • Ensure the policy uses the standard TCS template and record of document control • Coordinate consultation with relevant stakeholders including staff, consumers, and external advisors as appropriate • Submit the completed draft to the QIC for quality review
Systems and Performance Team	• Maintain the Document Register, including review dates, version history, and document status • Send alerts when policies are approaching their review date • Ensure policies are accessible to all staff via internal systems • Coordinate logistics of the policy development and review cycle • Manage privacy compliance across all digital platforms • Coordinate data breach response • Maintain backup and recovery mechanisms • Ensure system security and access controls are current
Service Managers	• Communicate policy changes to all affected staff through team meetings and internal communication systems
All Staff, Students, and Contractors	• Implement and act in accordance with policies relevant to their role • Participate in policy consultation processes when invited • Report concerns about policy gaps, inconsistencies, or implementation issues through appropriate channels

	• Collect, access, use, and disclose personal information only for authorised purposes • Provide the privacy notice to consumers at the commencement of the episode of care • Report any suspected privacy breach immediately to the Service Manager and Regional Manager
--	---

5.1 Policy Development or Review

This policy is reviewed on a three-year cycle, consistent with the Document Review Alert System. A review is also triggered by:

- Changes to legislative obligations, applicable standards, accreditation requirements, or organisational needs.
- Incidents, complaints, or audit findings that identify a gap in or non-compliance with this policy
- Consumer feedback, complaints, or audit findings
- Strategic or operational priorities identified by the Board, Executive Directors, SMC, or QIC
- Significant organisational change affecting the scope or application of this policy.

Reviews are managed in accordance with the Policy Development Policy. The next scheduled review date is recorded in the Document Register.

6.0 Policy Requirements

6.1 Collection of Personal Information

Personal information is collected in the following ways:

- When information is provided directly to the treating health professional, whether verbally or in writing (e.g. letters, emails, text messages)
- During interaction with TCS staff, including administration personnel
- Through referrals, correspondence, and reports from other health practitioners, such as general practitioners
- From third parties such as public, community, or private sector services with appropriate consent.
- CCTV cameras operate in common areas at TCS physical sites for workplace safety purposes. Footage is retained for 30 days and accessed only by authorised personnel consistent with this policy and the Workplace Health, Safety, and Wellbeing Policy.

The information collected includes personal details such as name, address, and contact phone numbers. As part of the provision of health services, additional personal information relevant to the presenting concerns will also be collected and recorded including records of session content, test material and results, and information provided by third parties such as medical specialists and general practitioners.

6.2 Storage and Access

- All personal information is stored securely in the endorsed electronic client management platform.

- Access is restricted to staff with a direct clinical or operational role in relation to the consumer.
- Staff must not access consumer records without a legitimate clinical or governance reason any breach is treated as a Code of Conduct violation.
- System access requires multi-factor authentication across all platforms.
- All consumer-facing correspondence uses the consumer's client identification number, not their name, when communicating with external systems.

6.3 Use and Disclosure — With Consent

Where consent is required for the use or disclosure of personal information, TCS obtains and documents appropriate consent in accordance with the Consent and Confidentiality Policy. Consent is sought before:

- Sharing information with a family member, guardian, or carer
- Discussing relevant matters with third parties such as general practitioners, employers, or funding agencies
- Providing written reports to other professionals or agencies including legal representatives, schools, and universities
- Any other disclosure not explicitly referenced in this policy.

6.4 Use and Disclosure — Without Consent (Exceptions to Confidentiality)

In certain circumstances, personal information may be disclosed without consent. These exceptions are limited and occur only when required or authorised by law, or when there is a serious risk to safety:

- When a court issues a subpoena or disclosure is otherwise required by law
- When mandatory reporting obligations apply such as reporting concerns related to child protection or abuse
- When there is a reasonable belief that a person is at risk of serious harm to themselves or others, and disclosure is necessary to prevent that harm
- For de-identified reporting to the Department of Health and Aged Care under the TCS funding agreement with Capital Health Network per Privacy Act 1988 (Cth) requirements.

In all cases, only the information relevant to the specific situation is disclosed, and all reasonable steps are taken to maintain the privacy and dignity of the individual.

6.5 Consumer Rights — Access, Correction, and Complaints

- Consumers may request access to or correction of their personal information in accordance with applicable privacy and health records requirements. Requests for access to or correction of health information are managed within applicable statutory timeframes and in accordance with TCS access and records management processes.
- If personal information is found to be inaccurate, out of date, or incomplete, reasonable steps are taken to correct it promptly.
- Consumers may request that records be made inactive supporting disengagement from the service but records cannot be deleted until the applicable retention period has elapsed.

- Concerns about the management of personal information are managed in accordance with the Service User Feedback Policy.
- If a concern cannot be resolved within TCS, a formal complaint can be lodged with the ACT Human Rights Commission (Health Services Commissioner): Phone (02) 6205 2222 | Online: hrc.act.gov.au | Email: human.rights@act.gov.au | Mail: GPO Box 158 Canberra ACT 2601.

6.5.1 Notification of Changes to Privacy Policy

Where TCS makes changes to its Privacy Policy that affect how consumer personal information is collected, used, stored, or disclosed, consumers are notified in a timely manner. Notification may occur through one or more of the following methods, depending on the nature of the change:

- Direct communication to consumers currently engaged with TCS services, via their preferred contact method (email, letter, or phone)
- Updated information provided at the point of service intake for new consumers following the change
- Publication of the updated Privacy Policy on TCS's consumer-facing information materials and website where applicable.

Where a change is significant, for example, a change to how information is shared with third parties or to the purposes for which it is collected. TCS will ensure affected consumers are notified directly before the change takes effect and given the opportunity to review and respond. Minor administrative updates to the policy do not require individual consumer notification.

6.6 Data Breach Response

In the event of a suspected or actual data breach including any unauthorised access, disclosure, or loss of personal information, the Data Breach Response process is activated immediately. All staff must report suspected breaches to the Service Manager, Regional Manager and Systems and Performance Team as soon as they become aware. If the breach is assessed as likely to result in serious harm, affected individuals and the Office of the Australian Information Commissioner (OAIC) are notified under the Notifiable Data Breaches Scheme.

6.7 Professional Supervision and Peer Consultation

Health professionals engage in clinical supervision and peer consultation as part of the quality assurance process. Information must be limited to what is reasonably necessary and de-identified wherever practicable. Supervision and consultation must occur through appropriate confidential arrangements, and information must not be disclosed beyond what is necessary for the purpose of the consultation.

7.0 Implementation

This policy is implemented and communicated in accordance with the Policy Development Process. Implementation is the responsibility of the Policy Owner, Systems and Performance Lead and Service Managers.

Table 3 – Implementation mechanisms for this policy

Mechanism	Description	Responsible
Induction and mandatory training	This policy is included in all-staff induction and relevant mandatory training, ensuring new and existing staff are aware of their obligations	People and Administrative Services Manager and Administrative Team
Staff communication	This policy is tabled at relevant staff meetings following approval or revision. Changes are communicated via internal systems	Service Manager
Document Register	This policy is uploaded to the Document Register and accessible to all staff via internal systems	Systems & Performance Lead
Consumer privacy notice	Privacy notice provided to all consumers at the commencement of their episode of care across all services	Clinical / Intake / Wellbeing staff

8.0 Compliance Monitoring

Compliance with this policy is monitored through the following indicators. Results are reported to the QIC and, where required, escalated to the SMC.

Table 4 – Compliance monitoring for this policy

Indicator	How Monitored	Frequency	Reported To
% of consumers with privacy notice provided at intake	Service Compliance Register	Quarterly	QIC
Number of privacy complaints or concerns received and managed	Complaints and Feedback Register/ Incident Register	Quarterly	SMC / QIC
Number of NDB-reportable breaches and compliance with reporting timeframes	Incident Register	Quarterly	SMC / Board

8.2 Privacy Impact Assessments

Where TCS introduces a new service, system, or significant change to information handling practices, a Privacy Impact Assessment (PIA) is conducted prior to implementation to identify and mitigate privacy risks. TCS maintains PIAs for each of its programs:

- ACT Medicare Mental Health Phone Service covering the collection, use, storage, and transfer of consumer information via telephone and the national PMHC-MDS reporting system.
- Medicare Mental Health Centres covering clinical information handling practices across face-to-face and digital service delivery.

PIAs are maintained as separate governance documents, reviewed as part of the regular policy review cycle consistent with the review schedule of this policy, and updated where there is a significant change to information handling practices or the introduction of new systems or service delivery modalities.

9.0 Related Documents

The following documents should be read in conjunction with this policy.

Table 5 – Related internal documents

Doc ID	Document Title	Type	Relationship to this Policy
Parent governance documents			
GOV-FRM-01	Governance Framework	Framework	Overarching governance structure and accountability model
GOV-FRM-02	Quality, Safety & Clinical Governance Framework	Framework	Safety and quality system this policy must support
GOV-POL-01	Policy Development Policy	Policy	Governs the development, approval and review of this policy
Related framework			
GOV-FRM-10	Information and Data Governance Framework	Framework	Privacy sits within the DAT governance system
Supporting policies and guidelines			
DAT-POL-01	Data Governance and Records Management Policy	Policy	Data storage, retention, access, and disposal requirements
CLN-POL-01	Consent and Confidentiality Policy	Policy	Consent requirements and processes for information sharing
DAT-GUI-01	Records Management Guidelines	Guideline	Operational guidance for records management across all programs
SAF-POL-02	Mandatory Reporting Policy	Policy	Mandatory reporting — a permitted disclosure without consumer consent
CON-POL-02	Consumer Participation and Feedback Policy	Policy	Complaints about privacy are managed under this policy
RSK-POL-04	Incident Management Policy & Procedure	Policy	Privacy and data breaches are reported and managed as incidents
GOV-POL-02	Code of Conduct	Policy	Consent requirements
Registers and records			
QLT-REG-01	Document Register	Register	This policy is listed and tracked in the Document Register
QLT-REG-02	Service Compliance Register	Register	Tracks audit findings, improvement actions, trends, and corrective actions

RSK-REG-01	Incident Register	Register	Safeguarding concerns, incidents, breaches, or reportable events identified under this policy are recorded, monitored, and managed
CON-REG-01	Complaints and Feedback Register	Register	Records privacy-related complaints, access requests, concerns, feedback, and outcomes arising from the management of personal information

10.0 References and Legislation

This policy should be read in conjunction with applicable legislation, regulatory requirements, organisational frameworks, and relevant standards that support governance, quality, safety, and service delivery across TCS:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles
- Health Records (Privacy and Access) Act 1997 (ACT)
- Information Privacy Act 2014 (ACT)
- Administrative Record Keeping Guidelines for Health Professionals, Department of Health
- ACT Human Rights Commission — Health Services Commissioner complaints information
- Australian Charities and Not-for-profits Commission Act 2012 and ACNC Governance Standards
- Office of the Australian Information Commissioner (OAIC) — Privacy guidance
- Applicable national standards and accreditation requirements relevant to TCS services
- Applicable contractual, regulatory, quality, and safety requirements.