

	Issue Date:	October 2023
	Version Status:	Version 2
	File No:	67
	Authorised By:	Board / CEO
Section: Service Provision		

Privacy and Confidentiality

ASES Standard	<p>Standard 2: Governance</p> <ul style="list-style-type: none"> ▪ Requirement 2.3 Data and Knowledge Standard <p>Standard 6: Communication</p> <ul style="list-style-type: none"> ▪ Requirement 6.1 Communication Standard <p>Standard 8: Consumer Outcomes</p> <ul style="list-style-type: none"> ▪ Requirement 8.1 Consumer and Community Engagement Standards
Related Policies	<ul style="list-style-type: none"> ▪ Code of Conduct ▪ Case Management ▪ Complaints Management ▪ Communication ▪ Notifiable Data Breaches

1. Introduction

TFSS is committed to ensuring that information is used in an ethical and responsible manner and recognises the need to be consistent, careful and thorough in the way that information about clients, staff, Board members, students and volunteers¹ is recorded, stored securely and managed.

In terms of information, TFSS

- Collects personal information in private environments, as much as reasonably practicable, to protect the privacy and dignity of individuals.
- Collects and uses personal information only to fulfil its functions and purposes, or for another acceptable reason with the relevant person’s consent (unless exceptions covered in Section 6 in the Procedures Section apply); acceptable purposes for collection and use include
 - for **clients**—service provision, referral, consultation, advocacy, reporting aggregate data for funding bodies, external audits and research

¹ From here when the term ‘volunteer’ is used, it means or can mean client, volunteer, student, staff member, Board member or other stakeholders (e.g., consultants).

- for **staff, volunteers and students**—recruitment, selection, employment, induction, payroll and tax, leave, supervision, development, performance management and review, and any other legitimate work-related purpose
- for **consultants and contractors**—tendering, contract creation, monitoring and execution
- Ensures that all persons about whom personal information is being obtained are informed why the information is being collected and how it is and will be used, stored and administered
- Stores personal information securely, protecting it from unauthorised access
- Provides clients and other stakeholders access to their own information and the right to seek its correction in accordance with Australian Privacy Principle 13 – correction of personal information.
- Provides information to clients about their rights regarding privacy and ensure that they understand the mechanisms available to make a complaint

TFSS has a legal obligation to comply with the *Privacy Act 1988* (Cwlth) and with the Australian Privacy Principles. <https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles#part-5-access-to-and-correction-of-personal-information>

TFSS respects clients' rights to acknowledge or refuse their consent for the various purposes it seeks to collect personal information and share information. Clients who acknowledge their consent for any purpose, also have the right to withdraw their consent at any time during their service period.

TFSS obtains clients' consent in writing and if a client gives their verbal consent for any purpose, this must be recorded by the worker taking consent and then placed on file.

When a client refuses or withdraws their consent for any purpose the implications of this decision should be explained and explored with the client—with the goal of overcoming any concerns that have led to the withholding of consent that may inhibit or prevents effective service provision. The use of formal or informal advocacy may be helpful in such situations.

2. Procedure

The most important thing in relation to collecting and using personal information is that it must not be used or disclosed for any reason other than the primary purpose it was collected except in the instance of meeting our legal obligations as a mandatory reporter. TFSS must take steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

1. The purpose of collecting information

TFSS collects personal information if it is reasonably necessary or if it directly relates to the client's circumstances in the context of service provision.

Privacy statement

Clients must be made aware of the following:

- The purpose of collecting information.
- How the information will be used.
- The type of information that is collected.

- Limits to the privacy of personal information.
- How a client can access or amend his or her information.
- How a client can make a complaint about the use of his or her personal information.

2. How information is collected

TFSS collects personal information through several different mechanisms, including but not limited to:

- Client information management systems.
- Face-to-face meetings.
- Telephone and email communications.
- Case conferences.

3. Type of information collected

TFSS collects and holds personal information about a client when the information is relevant to providing services to the client. The type of information collected includes the following:

- Client names, addresses and contact details.
- Intake, assessment and reassessment documentation.
- Client case management plans and plan revisions.
- Referrals to other agencies.
- Consent to obtain and release information.
- Feedback including surveys and complaints from clients.
- Reports from other agencies.
- Case closure and service exit documentation.

TFSS will only use client information for the purpose of service promotion when the client has provided written consent.

3. Collection principles

The following principles guide data collection practice

- TFSS will only collect information that is necessary for the performance and primary function of the organisation.
- TFSS will explain to clients the purpose of collection and how the information is used.
- TFSS will advise clients that any data collected are accessible to the individual.
- TFSS collects personal information from the clients themselves whenever possible.
- If the information was collected from a third party, TFSS will notify the clients and advise them the purpose of the collection.

TFSS will ensure that the client has provided consent to the collection of sensitive information. Sensitive information includes information about mental health, religious beliefs and ethnicity.

4. Pre-collection tasks

It is important to complete the following:

- Make clients aware of their rights and the complaints process and provide them with a copy of relevant documents including the Client Charter and Complaint Procedure as required.
- Explain to each person the purpose of collecting data.
- Ensure that the Client Information Management Systems levels of consent are explained to all clients, and that consent is obtained.

When clients have identified/disclosed that they have difficulty reading or speaking English, TFSS takes the time to read the information to them and checks that they have understood the information. If there is doubt regarding whether the client has understood the information, TFSS worker will arrange interpreter services prior to requesting the client's signature.

5. Consent and decision-making

A client's personal information should only be collected with their 'express consent or implied consent' informed consent.

The individual:

- Has been adequately informed before giving consent.
- Gives consent voluntarily.
- The consent is current and specific and,
- The individual has the capacity to understand and communicate their consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf.

When the client does not have the capacity to provide informed consent, personal information is collected through appropriately supported decision-making or substitute decision-making processes.

Refer to app-guidelines, chpt. B Capacity

6. Informed consent

Informed consent refers to advising clients of several matters before obtaining their consent. These matters include:

- Why the information is being collected.
- What will happen to the information being collected.
- Clients' rights to be told about the support they will receive.
- What the likely outcomes of the support might be.
- The provision of information to and from other services with which the clients are involved, or to which clients are to be referred.
- What the consequences are for the client (if any) if he or she does not provide the information.

7. **Supported decision-making**

Decision-making capacity may be influenced by each person's unique social circumstances, emotional and intellectual abilities.

Where a person may not have the capacity to provide informed consent staff should seek additional support to ensure that the individual understands the information that is provided or to assist them to communicate their decisions.

For further information refer to The NSW Information and Privacy Commission has also developed the [Privacy and People With Decision Making Disabilities Guide²](#) to assist workers in this area.

8. **Substitute decision-making**

If the person has a formal guardian, with a current guardianship order, and if the order covers the areas of person's life that are in scope for service provision, then you should work with the guardian and the person to obtain necessary consent.

If you are still unsure if the person can provide informed consent, and he or she does not have support persons, advocates or guardians, then you should seek advice from the Guardianship Division of the NSW Civil and Administrative Tribunal.³

9. **Personal information integrity**

TFSS takes steps to ensure that the personal information collected, used and disclosed is accurate, current, complete and relevant.

TFSS takes reasonable steps to protect the personal information it holds. These include steps against loss, interference, unauthorised access, modification or disclosure and other misuse of information. Information is protected by the following mechanisms:

- Positioning computer terminals so that they cannot be observed or accessed by unauthorised people or members of the public.
- Securely storing, disposing, destroying or de-identifying information that is no longer required by the organisation.

The following technical safeguards are used to protect information

- Using passwords to restrict computer access, multi factor authentication, with regular changes to passwords required.
 - Client management systems require staff to reset their passwords every 90 days and as a safeguard they auto lock the account after 30 days inactivity and an administrator will then have to grant access.
- Establishing different access levels so that not all staff can view all information.
- Using electronic audit trails to detect if data has been compromised.
- Installing virus protection and firewall software.
- Staff logging off computer when not in attendance to restrict access when working onsite or working remotely.

For more information, refer to TFSS Code of Conduct

10. Access to personal information

Individuals have a right to access personal information under the Privacy Act 1988 (Cwlth) and may request access to information held about them.

Situations in which access to information may be withheld include that:

- Access may threaten the life or health of an individual.
- Access may leave an unreasonable effect on the privacy of others.
- The request is clearly frivolous or vexatious, or that access to the information has been granted previously.
- The information is relevant to existing or to anticipated legal proceedings.
- Denial of access is required, either by legislation or law enforcement agencies.

11. Using or disclosing personal information

The most important thing in relation to collecting and using personal information is that it must not be used or disclosed for any reason other than the primary purpose it was collected for.

It is important to make clients aware if their information is to be entered into a client information management system and their statistical data collected by the National Data Collection Agency and that their details entered will only be identified by a code.

12. Authority to exchange information and information sharing

12.1 Confidentiality and consent

Information pertaining either to an individual or to the organisation is generally considered confidential. TFSS ensures that a client signs an authority to Obtain and Release information form' prior to releasing information to other persons or organisations, such as through referral to another service. The client's consent is sought for different types of information exchanges separately. The 'obtain and Release information form' will list each specific service or persons with whom the information will be exchanged, without generalisations.

A client has the right to provide or to refuse consent for each specific type of information that the organisation wishes to exchange. A client can also withdraw the consent that they had previously provided at any time.

Staff may be required to share information with statutory bodies without a client consent when there are concerns in relation to illegal activities and/or child protection or domestic violence.

- Under chapter 16A of the Child and Young Persons (Care and Protection) Act 1998- Mandatory Reporting is a legal obligation for certain professionals and community members who "MUST" report incidents of child abuse and or neglect to Child Protection Services if they believe, on reasonable grounds, that a child (a person under 16 years) who is in need of protection or is at risk of significant harm.
- Under Part 13A of the Crimes (Domestic and Personal Violence) Act 2007 which allows service providers to share information for the purpose of providing victims with domestic violence support

services, and for the purpose of preventing or lessening a serious threat to a person's life, health or safety.

12.2 Reporting non-identifying information

TFSS may be required to report to funding bodies, or to other government departments, on large scale. This generally involves non-identifying data collections (e.g., minimum data sets). When this is the case, a person's consent to share their data should not be taken for granted on the grounds that the data is non-identifying. Consent from the person should be sought—which can be refused or withdrawn—to participate in data collections of this nature.

12.3 Providing access to personal information for service audits

When an organisation undertakes accreditation against any service standards that involve external auditors reviewing client files, it should obtain client consent in writing. (However, this is unnecessary if client consent for this purpose was previously obtained).

12.4 Sharing information without consent

Australian privacy legislation allows for sharing information under 16A and 13A without consent if failing to share information is believed to lead to certain risks. The disclosure of personal information without consent to government agencies, other organisations or individuals is permitted if

- It is authorised or required by law.
- It is unreasonable or impracticable to seek consent.
- Consent has been refused.
- The disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person or group of people.
- The organisation is a mandatory reporter, and it is legally obliged to release information to relevant authorities when making a report about a child who is believed to be at risk of significant harm.

Chapter 16a (child protection) supersedes Part 13a (domestic and family violence) when a child protection concern is involved as more information can be provided in relation to the concern. Where Chapter 16a doesn't apply please use Part 13a when there is a domestic and family violence serious threat.

The decision to share information without consent must be based on sound risk assessment and then approved by your manager.

13. Code of Conduct

All staff are required to abide by the TFSS Code of Conduct in relation to privacy and confidentiality.

14. Complaints

Clients have a right to make a complaint if they feel that there has been a breach of their personal information.

TFSS will:

- Inform clients of their right to make a complaint.

- Make the complaints procedure available to clients at the initial interview.
- Log complaints about information handling in the complaints register.
- Provide timeframe to investigate the concern and to attempt to find a resolution.

15. Archiving and destruction

TFSS has a legal obligation to appropriately store and destroy or de-identify information that is no longer needed within time frames. For specific periods for the retention of information, refer to the Records and Data Retention Guidelines.

Beyond Use

Where technical reasons make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information.

Personal information is 'beyond use' if you:

- Are not able, and will not attempt, to use or disclose the personal information.
- Cannot give any other entity access to the personal information.
- Surround the personal information with appropriate technical, physical and organisational security.
- This should include, at a minimum, access controls including logs and audit trails, and commit to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

Where it is not possible to irretrievably destroy personal information held in electronic format TFSS needs to take steps to put the information 'beyond use'.

It is expected that only in very limited circumstances would it not be possible for TFSS to destroy or de-identify personal information held in electronic format.

4. Responsibilities

Responsibility	Delegation
Obtain consent to collect information	All Staff
Obtain consent to disclose information	All Staff
Secure storage of information	Corporate services, Service Stream Managers
Manage information	Corporate services, Service Stream Managers
Archive information	Corporate Services
Manage the destruction of information	Corporate services

5. Legislation

Privacy Amendment (Enhancing Privacy Protection) Act 2012

- [Privacy Amendment \(Enhancing Privacy Protection\) Bill 2012 – Parliament of Australia \(aph.gov.au\)](http://aph.gov.au)
- Privacy Act 1988 (Cwlth) - <https://www.legislation.gov.au/Details/C2018C00034>
- Notifiable Data Breach Scheme- [About the Notifiable Data Breaches scheme | OAIC](#)
- Australian Privacy Principles - <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>
- Fact Sheet The Information Protection Principles (IPPs) explained for members of the public [fact sheet \(nsw.gov.au\)](#)

6. Appendices

Appendix 1: Obtain and Release Client Information Form

Appendix 2: TFSS Complaints Procedure

Where to go for more Information

- TFSS CEO
- Your Manager

Policy Review

This policy replaces TFSS prior policy that relates to Privacy and Confidentiality and will be reviewed and will be updated every three years unless a review is triggered earlier due to legislative changes, or changes in business needs.

TAMWORTH FAMILY SUPPORT SERVICE LTD. ONLY:	
Document:	Privacy and Confidentiality Policy
Last Date Issued:	October 2023
Next Review Date:	October 2026
Version Number:	Version 2
Authorised by:	Board /CEO

RECORD OF REVISIONS:				
Revision	Date	Section	Page	Details
Version 1	July 2020	All	All	Original
Version 2	October 2023	All	All	Refer to Policy Index