


| | | |
|--|------------------------|-----------------------------|
|  Tamworth Family Support Service | Issue Date: | 1 June 2016 |
| | Version Status: | Version 2 |
| | File No: | E.5 |
| | Authorised By: | Management Committee |
| Section E – Employment Standards | | |

Privacy Policy

| | |
|--------------------------|---|
| Related Policies | <ul style="list-style-type: none"> ▪ Code of Conduct ▪ Electronic Systems Usage and Communications ▪ Managing Complaints ▪ Social Media |
| Related Documents | <ul style="list-style-type: none"> ▪ Complaints Procedure ▪ Client file Management and Record Keeping |
| Related Forms | <ul style="list-style-type: none"> ▪ Employee Photo Consent Form ▪ Client/Child Photo Consent Form |

1. Introduction

Tamworth Family Support Service Inc (TFSS) respects the protection of personal information and privacy rights of all individuals and is committed to ensuring that the Management Committee, all managers and employees working at TFSS comply at all times with their obligations under the *Privacy Act 1988 (Cth)* and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*, including the *Australian Privacy Principles 2014* and the *Privacy and Personal Information Protection Act 1998 No 133 (NSW)*.

Policy purpose: This *Privacy Policy* summarises the standards of privacy and confidentiality applicable at TFSS. It is to be used as a guide by Managers and employees to set up and maintain systems and procedures that promote ethical and professional conduct.

Policy scope: This Policy applies to all persons including: senior management; full-time, part-time, casual employees, contractors and volunteers who are engaged to work or volunteer at any TFSS locations and at any other location on behalf of TFSS. They are collectively referred to as employees or volunteers in this Policy, unless specifically referenced.

2. Australian Privacy Principles

The Australian Privacy Principles (APP) established by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* applies to all organisations and Government agencies. TFSS therefore adheres to the principles as set out in the APP in the way it collects, manages and uses information provided to TFSS from employees, clients and other parties associated with TFSS.

3. Collection of Information

TFSS collects personal information from a number of sources for varying reasons. Personal information is only collected by lawful means where it is necessary for TFSS to collect and use this information.

A client's personal information is collected when referrals are made through TFSS Central Intake line. The Intake worker completes an assessment with the client and information gathered is used to ensure that the client is connected to the right service or program. Information gathered is shared with the knowledge or consent of the client. Personal information can be collected directly from the individual concerned or from other services with the consent of the person.

At the time of collection, the individual will also be informed as to the purpose for the collection of the information and that they are able to access any information provided to TFSS.

TFSS' Client Charter informs clients that their personal privacy will be respected and confidentiality protected except where TFSS has a legal obligation to disclose information in relation to them.

4. Data Security

TFSS undertakes to adequately protect the personal information held by the organisation from misuse, loss and unauthorised access, modification or disclosure.

Where it is necessary to record personal information, you should make every effort to ensure that there is a legitimate legal need to record the information, that the recording is factual and that information of a confidential nature is kept secure and not discussed with anyone who does not have a legitimate right to know.

All employees are required to respect private information held by the organisation and to ensure all TFSS procedures in relation to the security of information are adhered to, as follows:

- To ensure that internal documents are only accessible to our organisational employees, they should be password protected on the terminal server and/or placed in restricted or locked access in desk file draws or filing cabinets
- Employees must ensure confidential and sensitive information in any form (e.g. physical documents, case files, computer files, USB files, and client report forms, personal diaries, notebooks) cannot be accessed by unauthorised persons
- Employees are responsible to ensure confidential and sensitive material is securely stored overnight or when unattended such as when you are not in your office, as it may be able to be viewed by others (clients or colleagues)
- Employees should only release information that they are authorised to release in the course of their duties
- Employees should not release information in a manner which is misleading or which is likely to be misused
- Employees do not talk about clients in common spaces
- Employees do not talk about the client outside the program without client consent
- Employees do not discuss personal issues of one client with another without their consent
- Employees will speak with client about concerns in private

Unauthorised access, misuse, modification or disclosure of this personal information held by the organisation by any of its employees will be considered a serious breach of TFSS policy and will lead to appropriate disciplinary action.

Employees will be trained in the TFSS procedures for management and security of personal information. If an employee is unsure of any of these procedures or are unsure in a particular situation then they must initially consult their Direct Line Manager for guidance.

5. Use and Disclosure

Our organisation collects, records, stores, processes, files, and disposes of a lot of very personal, private and confidential information of individuals, on families and of an organisational nature.

TFSS will only use personal information it collects for its original purpose which is disclosed at the time of collection. However, the organisation may disclose personal information it holds where there is a legal duty to do so, including circumstances where a lawful duty of care to disclose information exists.

At times there is a need to share information in relation to the safety and well-being of children through a 16A request or Child Protection Helpline. Information may also be shared as outlined in the Domestic Violence Sharing Protocol.

TFSS aims to work transparently with clients and ordinarily any information shared or reported in relation to the client is discussed with them if it is safe to do so.

Personal information collected may be disclosed to other branches/departments/ divisions within TFSS provided it is used in a manner which is in line with its original purpose of collection and use.

Where the information provided is used to communicate with a client, the client will be provided with the opportunity to decline receiving communication from the organisation.

5.1 Type of Personal Information Held

Personal and/or sensitive information that is collected and held by TFSS usually falls into the following categories:

Clients

- Information and files on our clients and their families and children, which contain information on identification, financial, physical and mental health issues, assessments, case plans and case worker notes

Potential/Existing Employees

- Candidate information submitted and obtained from the candidate and other sources in connection with applications for employment, for example:
 - Working with Children Check, which remains valid for 5 years
 - National Criminal History check
- Information and files on our employees and their families and children, which include identification, home addresses and contact details, financial records (bank accounts, superannuation accounts, salary sacrifice details, tax file numbers), next of kin, qualifications, certifications, and resumes
- Information about incidents in the workplace
- Documentation in relation to Performance appraisal, management and improvement
- Training and Development
- Employee departures - Exit interview

5.2 Purposes for Which Personal Information is Held

There is a variety of reasons why TFSS is required to hold personal information. Primarily these reasons include:

- For contact purposes
- To comply with legislation and government requirements
- To set up clients' accounts
- To identify clients when they request services or change their details
- To answer client queries
- To ensure the continual improvement of TFSS, its employees and its products and services offered
- To customise advertising and marketing content
- To conduct research and collect statistics.

When clients utilise TFSS' services, they consent to their personal details being used.

5.3 Types of Organisational Information Held

- Information and files on our internal relationships, such as our strategic plan, our operational and business plans, financial budgets, financial reports, management reports, and our Management Committee meeting papers
- Information and files on our external relationships, such as our expressions of interest, our service specifications, and our funding agreements, and our consortium and memorandum of understanding partners etc.

6. Misuse of Information

Employees must not misuse information gained in their capacity as an employee of our organisation. Misuse of information (including unauthorised or inappropriate disclosure) may be an act of corruption or even a criminal offence.

Section 8(1) of the *Independent Commission Against Corruption Act 1988* (NSW) includes in the definition of corrupt conduct, "any conduct of a public official or former public official that involves the misuse of information or material acquired in the course of his or her official functions, whether or not for his or her benefit or for the benefit of any other person".

Section 309 of the *Crimes Act 1900 (NSW)* also makes misuse of information a criminal offence.

Misuse includes:

- Inappropriately disclosing confidential information held in our records
- Seeking to take advantage, for personal reasons, of another person on the basis of information about that person held in our records
- Speculation in shares on the basis of confidential information about the affairs of an enterprise or of proposed government actions, programs or projects.

6.1 Impact of Inappropriate Disclosure of Information

Unauthorised disclosures of such sensitive and confidential information may:

- Cause or contribute to people, families or their children's harm
- Give an individual or agency an improper advantage
- Damage our organisation's integrity and reputation.

It is a serious offence to deliberately release confidential documents or information to unauthorised persons.

Employees should not reveal personal information such as home addresses, telephone, mobile numbers or personal email addresses of clients or colleagues to enquirers, even when they claim to be a relative or friend. You should offer to take the enquirer's details and pass them on to the person concerned.

7. Access

Subject to some exceptions that are set out in the Australian Privacy Principles, all persons may gain access to their personal information that is held by TFSS. Access may be refused, if it would interfere with the privacy rights of other persons or if it breached any confidentiality that attaches to that information.

Access to another person's personal information will not be provided in any circumstances except:

- An agent that a client/employee has provided consent to requests such information
- Where we are required to by law
- If we believe it is necessary to protect TFSS property or rights, another TFSS client or a member of the public
- To another party if we transfer our services or part of our services to that other party

Employees will be regularly trained by their Direct Line Manager in TFSS procedure in how to respond to requests for access to personal information.

In certain circumstances, TFSS may charge an administration fee to cover the cost of accessing such personal information.

8. Data quality

On a regular basis TFSS will make a request directly to individuals for them to check and update records of their personal information.

9. Information Destruction Policy

9.1 Employee Information

TFSS hold all required personnel information usually for a minimum period of 7 years in keeping with State Records NSW record-keeper retention and disposal rules.

All non-current information or information deemed no longer to be required by TFSS shall be destroyed. Items shall be destroyed by being placed into a shredder and removed from the premises of TFSS.

9.2 Client Records

Client Records are retained and disposed of in keeping with Family and Community Service (FACS) Guidelines.

- In general Client's records must be retained for 7 years after delivery of service
- Minor's records should be kept for 7 years from the last date of service or until the minor reaches the age of 25 years, whichever is the later.
- However if the service provider is of the opinion that certain records must be kept longer. Records used as evidence under Section 16 K of the Royal Commissions Act 1902 (Cth) which makes it an offence to destroy them.
- Providers are encouraged to retain records of Aboriginal clients born before 1970 indefinitely.
- Any other records for which the provider has sought and received legal advice that they are required for a longer period of retention or indefinite retention. It is the provider's responsibility to ensure they have sought any such advice.

Prior to destruction, notations from the information may be made for later reference.

10. Video Surveillance

To assist in the security of our assets and safety of our employees and clients, TFSS uses video surveillance. The use of video surveillance is recognised as a tool in reducing theft of organisational assets. Video surveillance recordings can assist police to identify offenders.

The use of video surveillance at TFSS' workplaces is for the purposes of ensuring the security of the workplace and people in the workplace, for example from threats outside the business. TFSS will make known to all employees the location of video cameras throughout the workplace (by the display of conspicuous signage) and agrees to consult with employees if and when the location of video surveillance cameras is altered. Private areas, such as toilets and washrooms are prohibited from being under video surveillance.

Access to video surveillance tapes and footage is restricted to the personnel nominated by the General Manager. Parties external to the workplace will not have access to tape recordings or video footage unless that access is authorised by law, or required for the purpose of legal proceedings, or installation or maintenance of video surveillance equipment.

11. Consent for the use of Photographs/Images

There are many reasons why TFSS may want to use images of people to illustrate advertisements, reports, promotional documents or videos etc. In a published photograph it is important to recognise and respect the importance of privacy. Privacy law in Australia protects images as well as written documents.

It is particularly important that images of children should be treated with special care and parental consent obtained prior to use.

11.1 Obtaining consent from Employees

Employees have the same privacy rights as any other individual in relation to the use of their photograph.

Employees must be advised prior to their photograph being taken what the image/s will be used for and an *Employee Photo Consent Form* must be signed and kept on their personnel file.

If an employee refuses consent TFSS will not take or use their photograph.

11.2 Obtaining consent from Adults

If a person is identifiable in a photograph, the ideal approach in all cases is to obtain the informed and voluntary consent of the people in the pictures. A *Client/Child Photo Consent Form* must be signed and kept on file.

To demonstrate respect for our clients and visitors, TFSS will, where possible, give notice to people attending an event that photos will be taken and used for specified purposes.

If a person expressly requests that their image is not to be published, TFSS will not do so unless it is required or allowed by law.

11.3 Obtaining consent when taking photographs of children

You must get consent from the parent, guardian or carer of any child or young person up to the age of 18.

If you need to get consent for children, you should send a consent form to the parent, guardian or carer. You must allow sufficient time so that you get permission before you take or use any photographs of children. The signed *Client/Child Photo Consent Form* must be kept on file.

11.4 Using Photographs provided by a third party

Before using photographs from an agency or other third party, it is your responsibility to obtain from them a written guarantee that permission has been granted for use of the photographs. You should also tell the agency or third party how you will use these photographs.

12. Complaints

Anyone who feels that there has been an unwarranted invasion of their privacy should contact TFSS to discuss the complaint and obtain a complaints procedure.

13. Responsibilities

Employees must always:

- Use official information only for the work-related purpose as it was intended
- Not disclose or use any confidential information without appropriate written approval, unless authorised to do so
- Comply with Chapter 16A of the *Children's and Young Persons(Care and Protection)Act 1998 (NSW)*
- Comply with SHS providers responsibilities and requirement Part 13A of the *Crimes (Domestic and Family Violence)Act 2007 (NSW)*
- Obtain completed and signed Consent Forms before taking or using photographs and images of any individuals
- Make sure that confidential information, in any form, cannot be accessed by unauthorised people
- Sensitive information should only be provided to people, either within or outside our organisation, who are authorised to have access to it
- Exercise caution and sound judgment in discussing other people's personal information with other organisational employees and other agency's employees
- Limit information to those who need to know in order to conduct their duties, or to those who can assist us in carrying out our work because of their expertise
- Refuse to give access to confidential information to former employees
- Destroy records only in accordance with policy and procedure and only with appropriate managerial authority to do so
- Surrender diaries and notebooks to managers at the end of the year or when leaving the organisation for archiving or disposal

Where to go for more information

- Your General Manager
- Your Direct Line Manager or Business Development Manager
- Australian Privacy Principles 2014 - www.oaic.gov.au
- www.check.kids.nsw.gov.au
- Mandatory Reporter Guide (MRG)
- Specialist Homelessness Services- Practice Guidelines


Legislation


National


Privacy Act 1988 (Cth) - www.comlaw.com.au


Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) – www.comlaw.gov.au


New South Wales


Children and Young Persons (Care and Protection) Act 1998 (NSW)  www.legislation.nsw.gov.au


Child Protection (Working with Children) Act 2012 (NSW)  www.legislation.nsw.gov.au

Child Protection (Working with Children) Regulation 2013  www.legislation.nsw.gov.au


Crimes Act 1900 (NSW)  www.legislation.nsw.gov.au

Crimes (Domestic and Family Violence) Act 2007 (NSW)  www.legislation.nsw.gov.au

Crimes (Domestic and Personal Violence) Act 2007 (NSW)  www.legislation.nsw.gov.au

Health Records and Information Privacy Act 2002 (NSW)  www.legislation.nsw.gov.au

Independent Commission Against Corruption Act 1988 (NSW)  www.legislation.nsw.gov.au

Privacy and Personal Information Protection Act 1998 No 133 (NSW)  www.legislation.nsw.gov.au

| TAMWORTH FAMILY SUPPORT SERVICE INC ONLY: | |
|---|----------------------|
| Document: | Privacy Policy |
| Last Date Issued: | 1 June 2016 |
| Next Review Date: | 1 June 2017 |
| Version Number: | 2 |
| Authorised by: | Management Committee |

| RECORD OF REVISIONS: | | | | |
|----------------------|-------------|---------|------|----------------------------------|
| Revision | Date | Section | Page | Details |
| Version 1 | 1 June 2015 | All | All | Original |
| Version 2 | 1 June 2016 | All | All | Refer Executive Summary 1/6/2016 |
| | | | | |
| | | | | |
| | | | | |