Privacy Policy

Togethr Financial Planning Pty Ltd

(ABN 84 124 491 078) (AFSL 455010)

trading as
Equip Financial Planning

	Document information
Applies to	All employees and directors of Togethr Financial Planning
Version	1
Approval State	Approved by the Board on 21 October 2019
Replaces Version	V2 (18 February 2019)
Author/s	Executive Officer, Member Engagement

This document is current at 21 October 2019

Contents

1. Introduction

Togethr Financial Planning (TFP), trading as Equip Financial Planning and MyLife MyAdvice, has an obligation to comply with the Privacy Act 1988 (Act) and the associated Australian Privacy Principles. The provisions of the Act apply to TFP because it may hold personal information (which includes sensitive information) about its clients.

TFP will ensure that it complies with the Australian Privacy Principles prescribed in the Act and will ensure that its Privacy Collection Statement is provided to all clients prior to any services being provided.

Employees and Directors play an important role in protecting the privacy of members. Any employee or Director who misuses a client's personal information will be subject to disciplinary action up to and including dismissal.

2. Roles and Responsibilities

2.1 TFP Staff

All TFP staff must ensure that they comply with this policy and protect the personal information of TFP clients.

TFP staff are expected to maintain the confidentiality of client information by not leaving personal or sensitive information lying around on their desks and in view of other staff, and by complying with TFP policies on IT and data security information. This would include not discussing clients' information with any other entity, other than with the clients' permission.

2.2 Compliance Manager

The Compliance Manager is responsible for;

1. Ensuring that TFP staff are aware of their obligations with respect to privacy and for ensuring that all TFP staff have undertaken the required annual compliance refresher training, which includes privacy;
2. Keeping abreast of regulatory changes with respect to privacy that may require action from TFP;
3. Reporting privacy breach notifications to Togethr Trustees Pty Ltd's (Togethr) Head of Risk who is responsible for assessing data breaches as described in the Togethr Data Breach Response Plan; and
4. Reporting breaches of Privacy Law to the TFP Board in the quarterly Compliance Report.

2.3 Privacy Officer

The Privacy Officer for Togethr has also been allocated the position of Privacy Officer for TFP. The Privacy Officer is responsible for:

1. Ensuring that the Privacy Collection Statement is up to date at all times;

2. Notifying the Compliance Manager of material changes to the Privacy Collection Statement or Policy;
3. Investigating breaches of the Privacy Policy and Privacy Collection Statement; and
4. Investigating complaints and incidents that relate to possible breaches of Privacy Law in order to help determine whether they are notifiable.

2.4 TFP Board

The TFP Board is responsible for:

- Approving changes to this Privacy Policy; and
- Oversight of the implementation of the Privacy Policy.

3. Requirements

3.1 General Requirements

In order to conduct its business, TFP is required to hold a significant amount of personal information on its clients. The utmost importance is placed on protecting the privacy of clients' personal information. This policy has been developed to ensure that clients' information is held securely and is only used for intended purposes.

Personal information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) Whether the information or opinion is true or not; and
b) Whether the information or opinion is recorded in a material form or not.

Sensitive information specifically includes:

a) Information or an opinion about an individual's:
    i. racial or ethnic origin; or
    ii. political opinions; or
    iii. membership of a political association; or
    iv. religious beliefs or affiliations; or
    v. philosophical beliefs; or
    vi. membership of a professional or trade association; or
    vii. membership of a trade union; or
    viii. sexual orientation or practices; or
    ix. criminal record; or
b) Health information about an individual; or
c) Genetic information about an individual that is not otherwise health information; or
d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
e) Biometric templates.

3.2 What kinds of personal information does TFP collect?

TFP must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. Consideration of what is 'reasonably necessary' is objective and consists of whether a reasonable person who is properly informed would agree that the collection is necessary.

TFP must not collect sensitive information about an individual unless the individual consents to the collection of the information. In any case, TFP must take reasonable steps to ensure that clients are aware their personal information is being collected.

The sorts of personal information held by TFP include a member's:

- Personal particulars (name, date of birth, gender);
- Tax file number;
- Proof of identity (for example, certified copies of a valid driver's licence, birth certificate or passport);
- Contact details (including addresses, email and phone numbers);
- Details of assets and liabilities of all types;
- Centrelink and other government agency information;
- Details of estate planning, including will and nominated beneficiaries;
- Bank details;
- Superannuation membership, balance and contribution history;
- Family details (including dependants);
- Occupation and salary details;
- Level of insured death and disablement cover; and
- Level of general insurance held.

TFP may also have access to a member's sensitive information if they have sought insurance cover through Togethr or lodged a claim for a disablement benefit. The sensitive information which Togethr holds will usually be health information about a member which is typically used to determine eligibility for insurance. This may include medical reports, work experience and qualifications.

3.3 Dealing with unsolicited personal information

TFP must be cautious with any unsolicited information that it has obtained. Unsolicited personal information is defined as information that TFP has received but has not taken active steps to collect. For example, if an individual completes an application form provided by TFP, but attaches financial records that have not been requested, these will be treated as unsolicited personal information.

In cases where TFP has received unsolicited information that it could not have collected through its standard (solicited) collection process, TFP must destroy the information or ensure that it is de-identified.

3.4 Why is personal information collected?

Personal information about a client is collected for the following purposes, to:

- Establish and verify the person as a client of TFP;
- Establish the identity of the client;
- Provide advice to the client about investments and strategies;

- Prepare a financial plan for the client;
- Assist in implementing investment recommendations for the client;
- Manage and resolve complaints relating to the client; and
- Conduct research regarding TFP clients generally.

3.5 How is information collected and stored?

TFP must take steps to ensure the personal information is protected from misuse, interference or loss and from unauthorised access, modification or disclosure.

To facilitate this, TFP collects information directly from clients. Information will be collected from a third party where a client has provided their consent or where disclosed on the Privacy Collection Statement.

All personal information is stored securely and is only used by authorised employees for the purposes set out in the Privacy Collection Statement. Information may be either stored electronically on Togethr's computer systems or may also be held in paper files.

When TFP no longer needs the information for any purpose and is not required under Australian law to retain the information, it must be destroyed in a secure manner or de-identified.

3.6 How is personal information used and disclosed

TFP must not use or disclose the personal information it has collected other than for the reason it was collected, unless the individual consents to this additional use or disclosure.

TFP uses a client's personal information for the purposes outlined in this policy and this information may, therefore, be disclosed by TFP to third parties such as:

- Insurers, medical consultants, professional advisers, financial institutions, lawyers, mailing houses, auditors and external service providers who are contracted to TFP for the purpose of providing the services;
- Dispute resolution bodies such as the Australian Financial Complaints Authority (AFCA) and the Office of the Australian Information Commissioner (OAIC);
- Togethr Trustees Pty Ltd, because it provides business services to TFP;
- International government agencies where expressly required by law; and
- Government agencies such as Centrelink, the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission, the Australian Taxation Office, the Australian Transaction and Reports and Analysis Centre and other bodies where authorised by law.

Whenever TFP discloses a member's personal information to a third party, TFP seeks to ensure that the member's privacy is protected:

- By the existence of a fiduciary relationship with the third party (such as Togethr's lawyers); or
- By a confidentiality agreement with the third party (such as mailing or research houses); or
- Because the third party has its own obligation not to disclose the information (such as government agencies); and
- By use of safe and secure methods of data transmission, such as encryption.

3.7 Adoption, use or disclosure of government related identifiers

TFP does not adopt government related identifiers and instead uses its own unique identifiers in order to satisfy the Australian Privacy Principles.

3.8 Direct marketing

TFP must ensure that it does not use or disclose a client's personal information for the purpose of direct marketing unless:

- TFP collected the information directly from the individual or in another matter disclosed on the Privacy Collection Statement;
- The individual would reasonably expect the organisation to use or disclose the information for that purpose;
- TFP provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- The individual has not made such a request to the organisation.

Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising.

3.9 Access to personal information and correction

A client has certain rights with respect to their personal information, including access to that information, the right to correct any personal information and the right to complain about any breaches of the Act. There is currently no charge to a client for the provision of personal information about them.

Clients are instructed to advise TFP if they think their personal information is incorrect so that this can be corrected.

A request for access to, or correction of, personal information will be acknowledged within 14 days and must be responded to within 30 days. However, if a client requests access to sensitive information, there may be a delay in providing this information. TFP will inform the client when this occurs.

All reasonable requests for access to personal information will be granted provided that they do not unreasonably impact the privacy of other individuals, are not frivolous or vexatious and would not undermine any legal proceedings or negotiations currently in progress relating to that individual. If a request is refused, the client must be notified of the reasons why and the mechanisms available to complain about the refusal.

If a client wishes to obtain further information concerning TFP's privacy obligations or wishes to make a complaint about the collection, use or disclosure of their personal information, the member can contact the Manager – Financial Planning, who will in turn notify the Privacy Officer about the complaint.

3.10 Rights to anonymity and pseudonymity

Individuals must have the option of not identifying themselves or of using a pseudonym when dealing with an APP entity in relation to a particular matter (unless it is deemed impracticable for the entity to

deal with individuals who have not identified themselves). TFP staff must consider the practicality of any such request before proceeding.

3.11 Complaints

If a client has a privacy related complaint they should direct their compliant to the Privacy Officer.

If a client believes that TFP or the Officer has not adequately dealt with their complaint, they may make a complaint to the Privacy Commissioner at the OAIC, or through TFP's external dispute resolution process (AFCA).

All complaints received are to be recorded in the Complaints Register.

3.12 Overseas disclosure

TFP does not provide your personal information to, or collect personal information about you from, persons located overseas. In the event that this changes in the future, we will still only disclose and collect your information in accordance with Australian laws and standards, including the Australian Privacy Principles.

4. Breaches

TFP must be compliant with Part IIIC of the Act in relation to notification of eligible data breaches.

According to the Act, an eligible data breach happens if:

a) There is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
b) The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

All data breaches are managed in accordance with Togethr's Data Breach Policy.

In the event a privacy breach has occurred, TFP must follow the Togethr's Data Breach Response Plan which sets out how to determine whether a notifiable data breach has occurred.

In the event that it is determined that the privacy breach is notifiable (i.e. it is assessed as likely to result in serious harm), a notification must be sent to the OAIC and the individual impacted by the breach must be informed of the breach. Notification is to be provided by way of a statement that complies with the requirements of the Privacy Act, namely that it contains:

a) the identity and contact details of the entity; and
b) a description of the eligible data breach that the entity has reasonable grounds to believe has happened; and
c) the kind or kinds of information concerned; and
d) recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

Refer to Togethr's Data Breach Response Plan for more information.

If the notifiable privacy breach relates to multiple individuals and it is deemed impractical to notify each one individually, TFP may publish a copy of the statement to the website and take reasonable steps to publicise its contents, in accordance with the provisions of the Act.

5. Reporting

Quarterly reporting to the TFP Board includes information on any complaints received relating to privacy and any known privacy breaches and subsequent remedial actions.

6. Policy Review

This Policy will be reviewed every 3 years or on any change to business processes or legislation that impacts how member's personal information is managed.

For specific enquires about privacy please contact:

The Privacy Officer
Equip Financial Planning
Level 12, 330 Collins Street
Melbourne Victoria 3000
Phone: 1800 682 626

Togethr Financial Planning Pty Ltd
Privacy Collection Statement
for Equip Financial Planning

Togethr Financial Planning Pty Ltd, trading as Equip Financial Planning and MyLife MyAdvice, is required to comply with the Privacy Act (Cth) 1988, the Australian Privacy Principles and Health Records Act (Vic) 2001 in relation to the privacy of your personal information. In this document Togethr Financial Planning Pty Ltd is referred to as "we", "our" and "us".

We are committed to complying with privacy law obligations and protecting and maintaining the privacy of your personal information. This Privacy Collection Statement sets out how and why we collect your personal information, the kinds of personal information we collect, how we keep it secure, how you can access and correct your personal information and how to make a complaint regarding your privacy.

1. How and why we collect personal information

In providing financial advice to clients, we hold personal, and sometimes health, information about you. This information is held in both hard copy and electronic format.

Personal information about you is collected to:

- establish and verify you as a client;
- establish your identity;
- provide advice to you about investments and strategies;
- prepare a financial plan for you;
- assist in implementing investment recommendations for you;
- manage and resolve complaints relating to you; and
- conduct research regarding our clients generally.

Personal information is collected directly from you when your member profile is created and when you meet or talk with us about your financial planning needs. We also obtain information about your super account balance, membership status, contribution history and related details from Togethr Trustees Pty Ltd, the trustee of the Equipsuper and MyLife MyMoney Superannuation Funds. We will only collect sensitive information with your consent.

We may also collect information from other third parties, but only when you have provided your consent to this. Third parties may include authorised representatives or agents, or other financial product providers.

2. The kinds of personal information that we collect

Personal information is any information or opinion that identifies you or enables you to be reasonably identified. Personal information also includes sensitive information, which includes information about your health.

The kinds of information that we hold and collect includes:

- personal particulars (name, date of birth, gender, etc.);
- tax file number;
- proof of identity (for example, certified copies of a valid driver's licence, birth certificate or passport);
- contact details (including addresses, email and phone numbers);
- details of assets and liabilities of all types;
- Centrelink and other government agency information;
- details of estate planning, including wills and nominated beneficiaries;
- bank details;
- superannuation membership and contribution history;
- occupation and salary details;
- family details (including dependants);
- level of insured death and disablement cover; and
- level of general insurance held.

We may also hold sensitive information about you if you have sought insurance cover through Togethr Trustees Pty Ltd, personally through an insurance company, or lodged a claim for an insurance benefit with Togethr Trustees Pty Ltd or an insurer. The sensitive information that we hold in relation to this is typically restricted to health information about you.

3. Consequences if information is not provided

If any required information is not provided, or is incomplete or inaccurate, it may:

- delay the provision of financial advice or services;
- result in the provision of inappropriate financial advice or services;
- result in you paying more tax than might otherwise apply;
- prevent us from being able to contact you; and
- prevent us from assisting you to implement any financial plans.

4. Direct Marketing

From time to time we may communicate with you about our services or changes that may impact your superannuation or financial planning arrangements. We may also use your personal information to send you direct marketing communication that we think may be of interest to you.

At any time, you are able to opt out of these marketing communications by updating your details on our website or by unsubscribing via the link on the communication received.

5. Organisations to which information may be disclosed

We use your personal information for the purposes outlined above and this information may therefore be disclosed by us to third parties such as:

- insurers, medical consultants, professional advisers, financial institutions, lawyers, mailing houses, auditors and external service providers who are contracted by us for the purpose of providing the services;
- dispute resolution bodies such as the Australian Financial Complaints Authority (AFCA) and the Office of the Australian Information Commissioner (OAIC);
- Togethr Trustees Pty Ltd, because it provides business services to Togethr Financial Planning;
- international government agencies where expressly required by law; and
- government agencies such as Centrelink, the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), Australian Taxation Office (ATO), Australian Transaction and Reports and Analysis Centre (AUSTRAC) and other bodies where authorised by law.

Whenever we disclose a client's personal information to a third party, we seek to ensure that your privacy is protected.

6. Overseas disclosure

We do not provide your personal information to, or collect personal information about you from, persons located overseas. In the event that this changes in the future, we will still only disclose and collect your information in accordance with Australian laws and standards, including the Australian Privacy Principles.

7. How we keep your information secure

We have security measures in place and take all reasonable steps to ensure that your information in both hard copy and electronic format is stored in a secure environment and protected from misuse, interference or loss and from unauthorised access, modification or disclosure. Our information technology systems use up-to-date security software and hardware and virus protection.

Your personal information is also protected through the use of secure passwords, usernames and security procedures.

Although in certain circumstances we are required to collect government identifiers such as tax file numbers, Medicare number or pension card number, we do not use or disclose this information other than when required or authorised by law or unless you have voluntarily consented to disclose this information to any third party.

As required under the Privacy Act, when we no longer need the information for any purpose and it is not required under Australian law to retain the information, it is destroyed in a secure manner or de-identified.

8. How you can access your personal information

You will, with limited exceptions, be able to access the personal, sensitive and health information that we hold about you by either making an appointment to come to our office to view it personally, or by calling to request a copy of the information. You will not be charged for accessing your personal information.

We will respond to requests for access within 30 days. Requests should be made to the Manager, Financial Planning (see contact details below). In certain circumstances, we may not be able to grant you access to the personal information that we hold about you if doing so would unreasonably impact the privacy of other individuals, or would undermine legal proceedings or negotiations currently in progress. If your request is refused, we will notify you with reasons for the refusal.

9. How you can correct your personal information

In order to provide financial planning services to you, we rely on your personal information being complete, up-to-date and accurate. If you believe that any of the personal information that we hold about you is incorrect, you may request that we amend the information. Requests can be made to the Manager, Financial Planning (see contact details below). We will take reasonable steps to ensure that the information is corrected.

10. How to make a complaint regarding your privacy

If you wish to make a complaint about a possible breach of your privacy, please contact the Manager, Financial Planning (see contact details below). The Manager, Financial Planning will work together with our Complaints Officer to ensure that the matter is resolved. Please provide sufficient details for your complaint to be investigated.

If your complaint is not resolved to your satisfaction within 30 days, you may be able to lodge a complaint with our external dispute resolution agency, the Australian Financial Complaints Authority (AFCA) or with the Office of the Australian Information Commissioner (OAIC).

11. Contact Details

You can contact us in relation to any client rights as follows:

The Manager – Equip Financial Planning
Level 12, 330 Collins Street
Melbourne Victoria 3000
Phone: 1800 065 753

12. Changes to this Privacy Collection Statement

We may amend this Privacy Collection Statement from time to time. Changes will be published on our website.

For specific enquires about privacy please contact:

The Privacy Officer
Equip Financial Planning
Level 12, 330 Collins Street
Melbourne Victoria 3000
Phone: 1800 682 626

Document last updated: 21 October 2019