Privacy Policy

Version	***Date***	***Amendment***
1.1	April 2017	-
1.2	March 2019	• Inclusion in Section 1 Overview of "the Privacy Act 1988 which includes" before the Australian Privacy Principles (APPs), and after (APPs), inclusion of "(which may be referred to collectively in this Privacy Policy as Australian privacy laws)" • Inclusion of paragraph 4.2 Disclosure of information in Australia • Amendment to paragraph 4.3 Disclosure of information overseas

1. Overview

Lighthouse Financial Advisers Townsville adheres to the Privacy Act 1988 which includes the Australian Privacy Principles (APPs) (which may be referred to collectively in this Privacy Policy as Australian privacy laws) and is committed to protecting your privacy. The purpose of this Privacy Policy is to outline how we collect, use, disclose and retain personal and sensitive information. It also sets out how you can make a complaint and how you can access the personal information we hold about you.

Our business is to help you understand and achieve your financial goals.

To do this, we need to understand who you are, what you want to achieve and what your circumstances are. We therefore need to collect personal information about you. This is so we can determine what services you require and what products suit your needs. We collect, use, retain and disclose your personal information so we can help you achieve your goals and at the same time operate our business and meet the legal and regulatory requirements.

We may also use and disclose your information for purposes related to those mentioned above, such as:

- assisting with your questions and complaints;
- arranging for services to be provided by third parties; and
- record keeping, compliance training and auditing.

This privacy policy is reviewed annually (unless an update is required earlier).

2. What is personal information?

Personal information means 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. For the purposes of this policy, personal information may include:

a) name;
b) address;
c) nationality;
d) residency status;
e) e-mail address;
f) Tax File Number; and
g) financial information.

3. Collection of personal information

3.1 Collection of personal information

We may collect and hold personal information for the purposes of enabling us to provide financial services to you. For example, in order for us to provide personal advice to you, we are required to verify your identity and obtain information relating to your financial situation and your personal goals and objectives – this is so we can assess your personal situation and provide you with appropriate financial advice. This information is generally collected directly from you as our client.

Any personal information collected by us is solely for the purpose of providing services to its clients and will not be disclosed unless the disclosure is required in the performance of those services (for example, disclosing your information to a financial institution in order to place an investment on your behalf). Where we obtain sensitive information (eg. racial or ethnic origin, political opinions, religious beliefs or affiliations or criminal record), we will only do so with your consent and where the collection of such information is reasonably necessary for us to perform our function. For example, we may also collect sensitive information (eg. your health records) for the purposes of arranging insurance for you or assisting you with insurance claims.

We will only collect personal information by lawful and fair means. In general, we collect personal information about you from you unless you consent to the collection of your personal information from someone else or it is unreasonable or impracticable to do so. In some instances, we may collect this information through third parties such as your family members, people authorised by you or health professionals (eg. in the case of income protection insurance).

Any personal information held by us may be held in a number of ways including via hard copy, soft copy or offsite on electronic servers. For example, we may collect personal information from you when you complete our client data form for the purposes of allowing us to provide you with financial advice or we assist you to acquire or dispose of a financial product (eg. invest in a managed fund or rollover your superannuation).

3.2 Dealing with unsolicited personal information

If we receive unsolicited personal information, we will within a reasonable period after receiving the information, determine whether or not we could have collected the information under Australian Privacy Principle 3. If the information could not have been obtained under APP 3 we will take steps to destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so.

3.3 Notification of the collection of personal information

At or before the time we collect personal information about you, or if that is not practicable, as soon as practicable after, we will take reasonable steps to ensure you are aware of:

a) who we are and our details;
b) how we collect your personal information and whom from;
c) whether the collection of your personal information is required or authorised by or under an Australian law or a court/tribunal order;
d) the purposes for which we collect your personal information;
e) the main consequences (if any) if we do not collect all or some of the personal information;
f) any other person or body to whom we would disclose the personal information that we have collected;
g) information about how you may access the personal information held by us about you and how you may seek correction of such information;
h) how you may complain about a breach of the Australian Privacy Principles and how the entity will deal with such a complaint;
i) whether we are likely to disclose the personal information to overseas
j) recipients (if so where).

3.4 Anonymity and pseudonymity

Whilst you may wish to deal with us anonymously. However, this is likely to limit the services we provide to you as our principal business relates to the provision of financial services (and in most cases, the provision of personal advice) which would require individuals to provide personal information. We are also required under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* to conduct customer due diligence and appropriately identify clients.

3.5 If you don't provide us with the information we request

It is your choice as to whether you wish to provide us with the information we request. However, given the nature of our business, we may not be able to provide you with the financial services you require if you don't provide us with the relevant personal information to help us review your personal circumstances.

4. Use or disclosure of personal information

If we collect personal information for a specific purpose (eg. to provide financial services to you), we will not use or disclose the information for another purpose unless you consent to the use or disclosure of the information or an exception in the APPs applies.

4.1 Direct Marketing

We may use and disclose your personal information to keep you informed about the range of financial products and services that we think may be relevant or of interest to you. You can opt out of receiving direct marketing information from us at any time by contacting us.

4.2 Disclosure of information in Australia

We may disclose your personal information to our service providers or other third parties who operate or hold data within Australia where Australian privacy laws regulate the handling of personal information.

Currently, we use Midwinter, a cloud-based financial planning software program, for the purposes of providing financial services to you. Midwinter's Privacy Policy states that personal information supplied to Midwinter is stored on servers located in Sydney, Australia which are operated by hosting service, Amazon Web Services, and that this information always remains within Midwinter's effective control. We are satisfied that Midwinter has appropriate data protection and security arrangements in place.

4.3 Disclosure of information overseas

From time to time we may send your information overseas to our service providers or other third parties who operate or hold data outside Australia where Australian privacy laws do not apply. Where we do this, we make sure that appropriate data handling and security arrangements are in place.

Currently, for the purposes only of sending faxes to Vanguard, an investment manager, we use FaxTo, an internet-based fax service. FaxTo's Privacy Policy states that FaxTo's website is hosted on various cloud-based storage providers such as Amazon and Google, which store data on secure servers located in the EU and the US with data protection and security protocols in place, and that FaxTo complies with the EU General Data Protection Regulation (as amended from 25 May 2018).

5. Security and access to your personal information

5.1 Information accuracy

We take reasonable steps to ensure that all personal data collected is accurate, up to date and complete. You can ask us to correct any inaccurate information we hold or have provided to others by contacting us using the details in this policy. If the information that is corrected is information we have provided to others, you can ask us to notify them of the correction.

5.2 Security of personal information

We take care to protect the security of your personal information. We may hold your personal information in a combination of secure computer storage facilities, paper-

based files and other formats. We take reasonable steps the to protect personal information from misuse, loss, unauthorised access, modification or improper disclosure. These include instructing our staff and financial advisers who handle personal information to respect the confidentiality of customer information and the privacy of individuals. Please note, we are required by law to retain your personal information for a specific amount of time. We will generally destroy or de-identify personal information if it is no longer required.

5.3 Access to and correction of personal information

You can contact us to access or correct any personal information we hold about you. However, in certain situations, we are permitted to refuse access to personal information. These situations include where:

a) giving access would have an unreasonable impact on the privacy of other individuals
b) giving access would be unlawful, or where denying access is required or authorised by an Australian law or a court order
c) giving access is likely to interfere with law enforcement activities.

For other situations, please consider Australian Privacy Principle 12.

If we receive a request to access personal information, we aim to respond to that request in a reasonable timeframe. In general, we will not impose an access charge unless the request of access and correct personal information is excessively onerous.

If we refuse access to personal information, we will provide you with reasons as to why access was refused and provide you with information on how to lodge a complaint about the refusal.

5.4 Data breach

A data breach occurs when personal information held by us is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, or when a database containing personal information is hacked or if we mistakenly provide personal information to the wrong person.

Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, we have an obligation to assess within 30 days whether a data breach amounts to an 'eligible data breach' if we become aware that there are reasonable grounds to suspect that data breach may have occurred.

If we form the view that the data breach would likely result in serious harm to any of the individuals to whom the information relates despite any remedial action taken by us, then the data breach will constitute an 'eligible data breach'. If an eligible data breach occurs, we have an obligation to notify you and the Office of the

Australian Information Commissioner and of the details of the eligible data breach.

6.Contact us

You may wish to contact us for the following:

a) find out what personal information we hold about you;
b) update or correct the personal information we hold about you;
c) opt out of receiving direct marketing material
d) make a privacy related complaint.

Should you wish to do so, please contact us on 07 4772 0938.