MONEY

OVER 50

FINANCIAL ADVISERS

Privacy Policy

Dated 25 August 2026 – Version 1.7

Lighthouse Financial Advisers (Townsville) Pty Ltd trading as Money Over 50 Financial Advisers.

ABN: 26 146 225 505

45 Ingham Road West End QLD 4810

PO Box 1457 Townsville QLD 4810

Tel: 07 4772 0938

Email: admin@mo50.com.au

www.mo50.com.au

Australian Financial Services Licence Number: 471826

Table of Contents

Amendment Schedule

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
1.3	September 2020	• Amendment of paragraph 4.2 Disclosure of information in Australia to reflect change of use of Midwinter to AdviserLogic, amendment of sub- heading in paragraph 4.2 to "Use or disclosure of information in Australia" Amendment of sub-heading in paragraph 4.3 to "Use or disclosure of information overseas"
1.4	October 2020	• Trading name change from Lighthouse Financial Advisers Townsville to Money Over 50 Financial Advisers
1.5	June 2024	• Updated the business email address from **mail@mo50.com.au** to **admin@mo50.com.au**. • Added a **Table of Contents**. • Updated **Section 2 – What is personal information?** to include phone numbers as an example of personal information. • Made a minor wording amendment to **Section 3.1 – Collection of personal information** regarding the ways personal information may be stored. • Updated **Section 4.2 – Use or disclosure of information in Australia** to reflect that **AdviserLogic was no longer used** for providing financial services. • Updated **Section 4.3 – Use or disclosure of information overseas** to reflect that **FaxTo was no longer used**. • Expanded **Section 4.3 – Use or disclosure of information overseas** to include information about the use, data handling and overseas processing arrangements of **HubSpot, JotForm, Qwilr, CloudFiles and Zapier**.
1.6	August 2024	• Updated **Section 3.1 – Collection of personal information** to clarify that personal information is collected and held for the primary purpose of providing financial services efficiently. • Revised **Section 4 – Use or disclosure of personal information** to clarify when personal information may be used or disclosed for purposes connected with providing financial services and where an exception under the Australian Privacy Principles applies. • Added **Section 4.1 – Third parties such as your accountant, lawyer and banker**, including examples of circumstances where relevant information may be disclosed to assist with taxation, estate planning and lending matters. • Added **Section 4.2 – Your spouse**, addressing the collection and disclosure of relevant information where financial services are provided to members of a couple. • Renumbered the existing sections dealing with **Direct Marketing**, **Use or Disclosure of Information in Australia** and **Use or Disclosure of Information Overseas** to Sections 4.3, 4.4 and 4.5 respectively. • Updated **Section 6 – Contact Us** to include access and correction requests, opting out of direct marketing, privacy complaints and withdrawal of consent relating to disclosures to third parties or a spouse. • Added **Section 7 – Australian Privacy Principles**, including a reference to further information published by the Office of the Australian Information Commissioner.
1.7	August 2026	• Comprehensive review and restructure of the Privacy Policy to improve readability, transparency and alignment with current Australian privacy requirements and guidance. • Expanded **Section 2 – What is personal information?** to more accurately describe the types of personal and sensitive information we may collect and hold, including identity and verification information, government identifiers, employment and taxation information, financial and insurance information, family and beneficiary information, records of interactions, website information and biometric information where biometric identity verification is used. • Updated **Section 3 – Collection of personal information** to clarify how information may be collected, how unsolicited information is handled, notification requirements, anonymity and pseudonymity, and the consequences of not providing requested information. • Revised **Section 4 – Use or disclosure of personal information** to clarify the circumstances in which information may be disclosed to accountants, lawyers, bankers and other professional advisers, and how information is handled between joint clients, spouses and partners. Wording relating to implied consent and disclosure without express consent was replaced with wording based on authorisation, reasonable expectation and other circumstances permitted by Australian privacy law. • Updated provisions relating to **direct marketing, artificial intelligence and generative AI tools, service providers and overseas disclosures**. • Updated provider information for **HubSpot, Qwilr and CloudFiles**, and reviewed and reformatted existing information relating to **JotForm and Zapier**. • Added information relating to **DocuSign, ChatGPT (OpenAI), Claude AI (Anthropic), Annature and Stripe**. • Added **Appendix A – Service Provider and Technology Details**, containing more detailed information about relevant technology providers, their purposes, data handling and security arrangements, overseas processing and use of subprocessors. Provider-specific detail was moved to the Appendix to improve the readability of the main Privacy Policy. • Removed a historical reference to the former use of **FaxTo** and **AdviserLogic**. • Updated **Section 5 – Security and access to personal information** to refer expressly to reasonable technical and organisational security measures, clarify retention and destruction or de-identification practices, improve access and correction wording, and update the Notifiable Data Breaches assessment and notification provisions.

Version	Date	Amendment
		• Expanded the **Privacy Complaints** provisions to explain how privacy complaints may be made and handled, including contact with the Privacy Officer and escalation to the Australian Financial Complaints Authority (where within its jurisdiction) or the Office of the Australian Information Commissioner. • Updated the policy review wording to provide that the Privacy Policy is reviewed **periodically and updated where necessary**, rather than stating that it is reviewed annually. • General formatting, terminology, numbering and drafting amendments made throughout the document to improve consistency and readability. • Reformatted and condensed historical amendment entries for readability, without changing the substance of the amendments previously recorded.

1 Overview

Lighthouse Financial Advisers (Townsville) Pty Ltd trading as Money Over 50 Financial Advisers (we, us or our) is committed to protecting your privacy and handling personal information in accordance with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), and other applicable privacy laws.

This Privacy Policy explains the kinds of personal information we collect and hold, how we collect, use, disclose and protect that information, how you can access or correct information we hold about you, and how you can make a privacy complaint.

Our business is to provide financial advice and related financial services. To do this, we need to understand your identity, circumstances, financial position, goals and preferences. We also collect and use information to administer our client relationships, operate our business and meet legal, regulatory, compliance, audit and record-keeping obligations.

We review this Privacy Policy at least annually and earlier where our practices, systems or legal obligations change.

2 What personal information do we collect and hold?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information is true and whether or not it is recorded in a material form.

Depending on the services we provide, the personal information we collect and hold may include:

- identity and contact information, such as your name, date of birth, address, phone number, email address, nationality and residency status;
- identity verification information and documents, including details from passports, driver licences and other identification documents, and biometric information where biometric identity verification is used;
- government identifiers where required or authorised, including Tax File Numbers;
- employment, occupation, income and taxation information;
- bank account, superannuation, pension, investment, insurance, asset, liability, cashflow and other financial information;
- family, dependant, beneficiary, estate planning and relationship information relevant to the services we provide;
- information about products and services you hold, applications, transactions and instructions;
- correspondence, meeting notes, call records, forms, documents and other records of our interactions with you; and
- website and technical information where applicable, such as device, browser, IP address, website activity and information submitted through online forms.

Some information we collect may be sensitive information under the Privacy Act, including health information, racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal record information and certain biometric information. We only collect sensitive information where you consent and the collection is reasonably necessary for our functions or activities, or where collection is otherwise permitted or required by law.

Tax File Numbers and other government identifiers are handled in accordance with the specific laws and rules that apply to them.

3 How we collect personal information

3.1 How we collect information

We usually collect personal information directly from you, including during meetings and telephone or video calls, through client data forms and questionnaires, by email, through our website or online forms, and when you give us documents or instructions.

Where permitted, authorised or reasonably necessary, we may also collect information from third parties, including your spouse or partner, family members, authorised representatives, accountant, lawyer, banker, employer, health professionals, insurers, superannuation funds, investment or platform providers, financial institutions, government agencies, identity verification providers and other service providers.

We may hold personal information in electronic systems, cloud services, email, document management systems, secure file-sharing systems and, where required, paper records.

3.2 Unsolicited personal information

If we receive personal information that we did not request, we will determine within a reasonable period whether we could have collected it under the APPs. If we could not have collected it, and it is lawful and reasonable to do so, we will destroy or de-identify the information as soon as practicable.

3.3 Notification when we collect information

At or before the time we collect personal information, or as soon as practicable afterwards, we take reasonable steps to make you aware of relevant matters required by APP 5. This may be done through this Privacy Policy, a collection notice, a form, an engagement document or another appropriate notice.

3.4 Anonymity and pseudonymity

You may deal with us anonymously or by using a pseudonym where this is lawful and practicable. However, this will generally not be practicable where we provide personal financial advice or implement financial products because we must identify our clients and obtain sufficient information to provide appropriate services and meet legal obligations, including customer due diligence obligations under anti-money laundering and counter-terrorism financing laws.

3.5 If you do not provide requested information

You may choose not to provide personal information we request. However, if we do not have the information reasonably required to understand your circumstances, verify your identity, meet our legal obligations or provide the requested service, we may be unable to provide some or all financial services to you.

4 How we use and disclose personal information

4.1 Purposes of use and disclosure

We use and disclose personal information for the purpose for which it was collected and for related purposes permitted by the APPs. These purposes may include:

- verifying your identity and meeting anti-money laundering, counter-terrorism financing and other legal requirements;
- understanding your circumstances, goals, needs and preferences and providing financial advice and related services;

- preparing advice documents, applications, forms and other documentation;
- implementing your instructions and arranging or administering financial products and services;
- communicating with you and responding to enquiries, requests and complaints;
- working with product providers, professional advisers and other third parties where required to provide services to you;
- maintaining client records, conducting compliance reviews, audits, training, quality assurance and risk management;
- meeting legal and regulatory obligations and responding to regulators, courts, tribunals, law enforcement bodies or government agencies where required or authorised; and
- operating, improving and securing our business, systems and services.

If we wish to use or disclose your information for another purpose, we will obtain your consent where required or rely on another basis permitted by the Privacy Act, such as where the secondary purpose is related to the primary purpose and you would reasonably expect the use or disclosure, or where the use or disclosure is required or authorised by law.

When relying on a related-purpose exception, we seek to use or disclose only the information reasonably necessary for that purpose.

4.2 Accountants, lawyers, bankers and other professional advisers

As part of providing financial services, it may be useful or necessary to provide relevant information to another professional involved in your affairs. For example, your accountant may require investment statements or deductible contribution information, your estate planning lawyer may require asset ownership information, or your banker may require current investment or superannuation balances for a loan application.

We may disclose relevant information to these parties where you have authorised us to do so, where you would reasonably expect the disclosure and it is related to the purpose for which the information was collected, or where the disclosure is otherwise permitted or required by law. We will not disclose more information than is reasonably necessary for the relevant purpose.

4.3 Joint clients, spouses and partners

Where we provide financial services to you jointly with your spouse or partner, information relevant to the joint advice, jointly held products or implementation of joint instructions may be shared between joint clients where you have authorised us to do so, where the disclosure would reasonably be expected and is related to the purpose for which the information was collected, or where otherwise permitted by law.

We do not disclose information that relates solely to you merely because another person is your spouse or partner. If you want particular information handled separately, please tell us. In some circumstances this may affect our ability to provide joint advice or act on joint instructions.

4.4 Direct marketing

We may use personal information to tell you about financial products, services, educational content or other information that we reasonably believe may be relevant to you. Where required, we will obtain consent before sending direct marketing. You can opt out at any time by using an unsubscribe function or contacting us. We will action opt-out requests within a reasonable period.

4.5 Artificial intelligence and automated tools

We may use approved artificial intelligence (AI) and generative AI tools to assist our staff with activities such as summarising information, drafting or reviewing documents, extracting information, conducting analysis and supporting administrative processes associated with providing financial services.

AI tools are support tools and do not replace the professional judgment and responsibility of our advisers and staff. We apply appropriate human review to AI-assisted work and do not intend to use AI tools to make financial advice decisions, or other decisions that could reasonably be expected to significantly affect a person's rights or interests, without meaningful human involvement.

Where personal or sensitive information is processed through an AI provider, we only do so where the use is reasonably necessary and permitted under applicable privacy requirements and our internal controls. Some AI providers may process information outside Australia; see section 4.6.

4.6 Service providers and overseas disclosures

We use third-party service providers to help us operate our business and provide financial services. These may include cloud hosting, customer relationship management, online forms, document generation, file sharing, electronic signatures, payment processing, workflow automation and approved artificial intelligence services.

Our current service providers include HubSpot, JotForm, Qwilr, CloudFiles, Zapier, DocuSign, ChatGPT (OpenAI), Claude AI (Anthropic), Annature and Stripe. Additional provider-specific information, including the purpose for which we use each provider and relevant published information about security, hosting, data location and subprocessors, is set out in Appendix A.

Some of these providers operate or use infrastructure and subprocessors outside Australia. Overseas recipients are likely to be located in the United States, the European Union or European Economic Area, Canada and other countries in which the relevant provider or its subprocessors operate. Provider arrangements and locations may change from time to time.

Where APP 8 applies to an overseas disclosure, we take reasonable steps in the circumstances to ensure the overseas recipient handles personal information in a manner consistent with the Australian Privacy Principles, unless an exception under the Privacy Act applies. We also consider privacy and information-security arrangements when selecting and reviewing service providers.

5 Security, retention, access and correction

5.1 Information accuracy

We take reasonable steps to ensure personal information we collect, use and disclose is accurate, up to date, complete and relevant, having regard to the purpose for which it is being used or disclosed. Please tell us if your details or circumstances change or if you believe information we hold is incorrect.

5.2 Security and retention of personal information

We take reasonable technical and organisational measures to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Depending on the circumstances, these measures may include access controls and authentication, encryption and secure transmission where appropriate, secure cloud and document systems, staff confidentiality obligations and privacy training, physical security, provider due diligence, system monitoring and incident-response procedures.

No method of storage or transmission is completely secure. We therefore review our privacy and information security practices and seek to use layered controls appropriate to the sensitivity and volume of information we hold.

We retain personal information for as long as reasonably required for the purposes for which it may be used or disclosed and to meet legal, regulatory, professional and record-keeping obligations. When personal information is no longer required and we are not required by law or a court or tribunal order to retain it, we take reasonable steps to destroy or de-identify it.

5.3 Access to and correction of personal information

You may ask us to give you access to personal information we hold about you or to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Please contact us using the details in section 6. We will respond within a reasonable period. We do not charge for making access or correction requests.

If we correct personal information that we previously disclosed to another APP entity, you may ask us to notify that entity of the correction. We will take reasonable steps to do so where required by the APPs, unless it is impracticable or unlawful.

5.4 Data breaches

A data breach can occur when personal information is lost or is subject to unauthorised access, disclosure, modification, misuse or interference. Examples include a lost device, a compromised account or system, or information being sent to the wrong person.

We maintain processes for identifying, containing, assessing and responding to suspected data breaches. Under the Notifiable Data Breaches scheme, if we have reasonable grounds to suspect that an eligible data breach may have occurred, we must carry out a reasonable and expeditious assessment and take all reasonable steps to complete the assessment within 30 calendar days.

If we have reasonable grounds to believe an eligible data breach has occurred, we will notify affected individuals and the Office of the Australian Information Commissioner as required by law, unless an exception applies. Where appropriate, we will also take remedial action to reduce the risk of harm.

6 Privacy complaints

If you believe we have mishandled your personal information or breached the APPs, you may make a privacy complaint to us. Complaints should preferably be made in writing so we can understand and investigate the issue, but you may also contact us by telephone.

Please contact our Privacy Officer using any of the following details:
- Email: admin@mo50.com.au
- Telephone: 07 4772 0938
- Post: PO Box 1457, Townsville QLD 4810
- Office: 45 Ingham Road, West End QLD 4810

Please include enough information for us to identify the issue, including your contact details, what occurred and the outcome you are seeking. We will acknowledge and investigate privacy complaints and aim to provide a substantive response within 30 days where practicable. If additional time is required, we will keep you informed.

If you are not satisfied with our response, you may be able to take the complaint to an external dispute resolution scheme or regulator. As a financial services firm, complaints may be referred to the Australian Financial Complaints Authority (AFCA), where the complaint is within AFCA's jurisdiction. AFCA is a free and independent service. You can contact AFCA at www.afca.org.au or on 1800 931 678.

You may also contact the Office of the Australian Information Commissioner (OAIC) about a privacy complaint. The OAIC generally expects you to first complain to us and allow us a reasonable opportunity to respond. Further information is available at www.oaic.gov.au/privacy/privacy-complaints or by calling 1300 363 992.

7 Further information

Further information about the Australian Privacy Principles is available from the Office of the Australian Information Commissioner at www.oaic.gov.au/privacy/australian-privacy-principles.

If you have questions about this Privacy Policy or how we handle personal information, please contact our Privacy Officer at admin@mo50.com.au or 07 4772 0938.

Appendix A Service Provider and Technology Details

This appendix forms part of this Privacy Policy and provides additional transparency about selected technology and service providers referred to in section 4.6. It summarises information published by those providers about their privacy, security, hosting and subprocessor arrangements as at the dates stated below.

Provider systems, certifications, subprocessors, data locations and published terms may change. The current information published by the relevant provider will apply to its services, and we review provider arrangements as part of our privacy and information-security governance.

A.1 HubSpot

Purpose: Customer relationship management and related software used to support the provision and administration of financial services.
Published information: HubSpot's Privacy Policy (last modified 14 April 2026) describes the use of security technologies and procedures intended to protect personal data from unauthorised access, use or disclosure. HubSpot's Independent Service Auditor's SOC 3 Report for 1 May 2025 to 30 April 2026 states that HubSpot uses cloud storage and compute services from Amazon Web Services (AWS) and Google Cloud Platform (GCP), together with data-centre hosting services from TierPoint, LLC. It also describes core infrastructure across multiple availability zones in the United States, European Union, Canada and Australia. HubSpot may engage subprocessors, which are identified on HubSpot's Sub-Processors Page and incorporated by reference into Annex 3 of its Data Processing Agreement (last modified 14 April 2026).

A.2 JotForm

Purpose: Online forms used to collect personal and, where required, sensitive information, including as an integration with HubSpot.
Published information: JotForm's Privacy Policy states that form responses submitted to a JotForm customer may be collected and stored using third-party server providers such as AWS or GCP. It also states that this may involve overseas disclosure and that Australian resident personal information may be transferred to cloud providers based in the United States of America.

A.3 Qwilr

Purpose: Document creation and presentation, including documents provided as part of the financial services we provide and integration with HubSpot.
Published information: Qwilr's Security and Compliance webpage (version dated 28 February 2025) states that customer data is hosted on MongoDB Atlas and refers to PCI, GDPR and SOC 2 compliance. Qwilr also states that it is PCI-DSS compliant and accredited via Stripe, has completed a SOC 2 Type 2 audit with ongoing automated monitoring of controls, policies and infrastructure powered by Drata, and is compliant with GDPR requirements.

A.4 CloudFiles

Purpose: Secure sharing of information, files and folders, including as an integration with HubSpot.
Published information: CloudFiles' Privacy Policy (updated 11 August 2026) states that it engages trusted third-party service providers for services including cloud infrastructure and hosting (for example AWS), payment processing, email delivery, analytics, customer support and marketing platforms, and that those providers are contractually bound to process data on CloudFiles' behalf. CloudFiles also states that it maintains SOC 2 Type II, ISO 27001, HIPAA and GDPR compliance. Its subprocessors are described in Annex III of its Data Processing Agreement.

A.5 Zapier

Purpose: Workflow automation and integrations between third-party applications we use, including systems such as HubSpot, JotForm and Qwilr.
Published information: Zapier's Privacy Policy states that information it collects may be transferred to and processed in the United States and in other countries where Zapier, its affiliates, subsidiaries or third-party service providers maintain facilities or personnel.

A.6 DocuSign

Purpose: Electronic signature and agreement management services.
Published information: DocuSign's Privacy Notice (version dated 9 October 2025) states that DocuSign has implemented an Information Security Management System and uses technical, physical and organisational measures to protect personal information. Its Data Management and Privacy Practices for DocuSign (last modified 14 April 2026) state that Agreement Data is encrypted at rest using AES 256-bit encryption (or equivalent), data in transit is secured using TLS 1.2 protocols, and access controls limit access to the sender and designated recipient(s). DocuSign may engage subprocessors, details of which are set out in its Data Protection Attachment and Data Processing Agreement.

A.7 ChatGPT (OpenAI)

Purpose: Approved generative AI assistance used by our staff to support activities connected with providing financial services and operating our business, such as summarising, drafting, reviewing and analysing information and supporting administrative processes.
Published information: OpenAI's Privacy Policy (updated 6 February 2026) states that OpenAI implements commercially reasonable technical, administrative and organisational measures designed to protect personal data from loss, misuse and unauthorised access, disclosure, alteration or destruction. OpenAI's Enterprise Privacy page (last updated 8 January 2026) states that data is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher, and that strict access controls are used. It also states that infrastructure supporting the API and ChatGPT Enterprise, Business, Edu and Healthcare products has been evaluated under an independent SOC 2 Type 2 examination. OpenAI may engage subprocessors, which are identified in its Sub-Processor List and Data Processing Addendum. The controls applicable to information we process depend on the OpenAI product and configuration used by us.

A.8 Claude AI (Anthropic)

Purpose: Approved generative AI assistance used by our staff to support activities connected with providing financial services and operating our business.
Published information: Anthropic's Privacy Policy (effective 8 July 2026) states that Anthropic implements technical and organisational measures to protect personal data and provides further security information through its Trust Center. Anthropic identifies AWS and GCP as cloud storage and compute providers, with Microsoft Azure included as a subprocessor for certain third-party integrations. Anthropic may also engage other subprocessors, which are identified in its published Subprocessor List and referenced in its Data Processing Addendum.

A.9 Annature

Purpose: Electronic signature services.

Published information: Annature’s Privacy Policy states that personal information is unlikely to be disclosed to, or stored with, an overseas recipient other than third-party providers of website hosting, data storage and similar services. Annature’s Trust & Security documentation states that Annature data is stored with AWS in the ap-southeast-2 region, with physical data centres in Sydney, Australia, and replicated across three availability zones. Annature also states that it is ISO 27001 certified and has completed a SOC 2 Type I report covering security, privacy and operational controls. Subprocessor information is set out in the “Sub processors” section of Annature’s Subscriber Agreement documentation.

A.10 Stripe

Purpose: Payment processing services.

Published information: Stripe’s Privacy Policy (last updated 28 April 2026) states that Stripe maintains organisational, technical and administrative measures designed to protect personal data from unauthorised access, destruction, loss, alteration or misuse. Stripe’s security documentation states that Stripe is certified annually by an independent PCI Qualified Security Assessor as a PCI Level 1 Service Provider and maintains SOC 2 Type II and ISO 27001 certifications. It also states that data is encrypted using AES-256 at rest and TLS in transit. Stripe may engage subprocessors, which are identified in its Sub-Processors List and referenced in its Data Processing Agreement.