

Treehouse FP Pty Ltd - AFSL 559915

Privacy Management Policy

Document Control:	Version 4.1
Document created by:	Tim Smith – Responsible Manager on 1 st of November 2024
Last reviewed by:	Tim Smith – Responsible Manager on 1 st of November 2024
Last adopted by governing body representative:	N/A

Disclosure, disclaimer and licence terms

Holley Nethercote Pty Ltd trading as Holley Nethercote Lawyers and trading as Holley Nethercote Compliance ('Holley Nethercote') believes that this document complies with the law as at the date of its preparation. The contents of this document do not constitute legal advice or the provision of a legal service.

This document is an incomplete template which requires the input of user-specific information. It also includes sections that are optional or mutually exclusive with other provisions and which require the user to exercise their judgement concerning the completion of the document. Further, the person who supplies this document to you may have made their own amendments to it.

There is a risk that altering this document in a manner that is not expressly indicated by Holley Nethercote in the document will not achieve the result intended by the user and may result in other, unintended consequences. Holley Nethercote recommends that the user obtain specific legal advice before making such alterations.

Accordingly, and to the extent permitted by law:

- no representation or warranty is given as to the suitability or applicability of this document for the user's particular business;*
- Holley Nethercote and its directors and employees disclaim all or any contractual, tortious or other form of liability to any person arising out of or in connection with reliance upon or use of this document, including without limitation, any liability arising or in connection with changes made to this document by a person other than Holley Nethercote.*

© Holley Nethercote Pty Ltd is the owner of copyright in this document. Only the organisation which purchased this document from Holley Nethercote Pty Ltd can use this document and alter it so that it suits their business.

Last updated: April 2024

At a glance

Responsibility, review and breaches of this policy

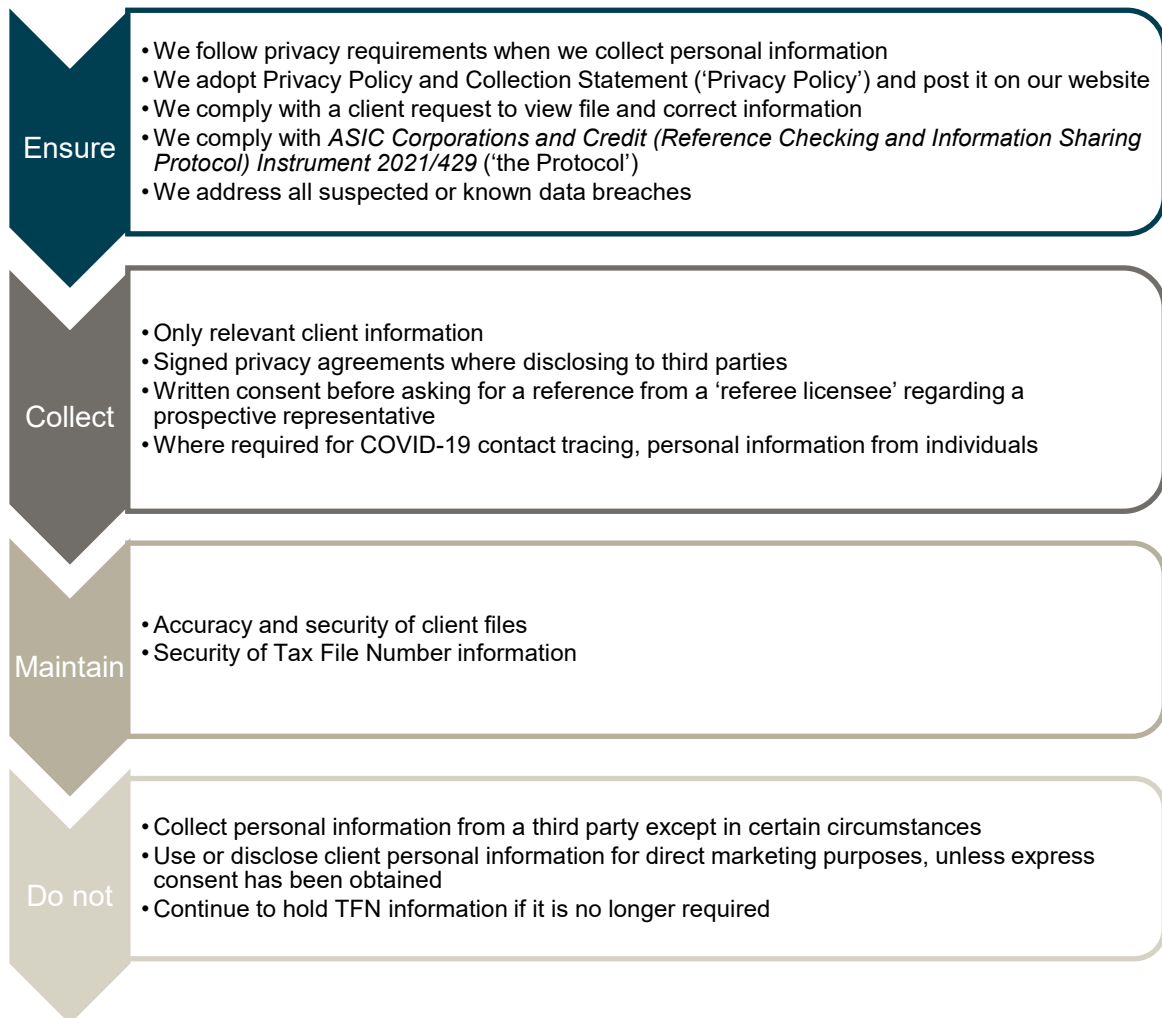
Tim Smith is the 'Responsible Person' who oversees this policy.



The policy is reviewed periodically in accordance with our Compliance Diary & Checklist.




If a breach of the policy occurs, we follow the procedure set out in our Breach (Reportable Situation) and Events Reporting Policy.




Key requirements

Licensee

Do	When
 Develop, adopt and post a Privacy Policy and Collection Statement (Privacy Policy) on our website	Immediately

Representative

Do	When
 Provide our client a Privacy Policy and Collection Statement (Privacy Policy)	Before collecting personal information
Only collect, use and hold relevant client information which we have disclosed in our Privacy Policy and Collection Statement (Privacy Policy)	At all times

DO NOT	
Do not collect personal information from a third party	Unless it is unreasonable or impractical to collect it directly from our client

Introduction and scope

When we collect **personal information** from a client or potential client, we need to comply with the privacy laws. Personal information is any information or an opinion about a person which is reasonably capable of identifying them and includes (for example) information relating to the client's financial, taxation, health, employment and estate planning matters.

Note that information can be personal information whether or not it is recorded in a material form. An opinion or information about a person can be personal information even if it is not true.



This policy has been designed in accordance with our risk appetite, which is set out in our Risk Appetite Statement.

Develop and implement a Privacy Policy and Collection Statement (Privacy Policy)

We have adopted, and posted on our website, a clearly expressed and up-to-date policy about how we manage personal information we collect, hold, use and disclose. This policy includes information about:

- the **kinds** of personal information that we collect and hold as an entity, and **how** we collect and hold it;
- the **purposes** for which we collect, hold, use and disclose personal information;
- how an individual can **access** the personal information about them that we hold, and if necessary, seek to have that information corrected;
- how we secure our clients' personal information, and ensure that it is protected from misuse, interference, or unauthorised access, modification or disclosure;
- how an individual can **complain** about a breach of the Australian Privacy Principles (APPs);
- whether we are likely to disclose personal information to **overseas recipients**, and, if so, the countries in which those recipients are likely to be located; and
- whether we are required to comply with the EU General Data Protection Regulations (GDPR), and, if yes, the way in which we comply with those obligations.¹

Give the client a privacy statement

Before collecting personal information from a new client, we give them a privacy statement. This is a document which summarises our privacy obligations, and sets out key information about who is collecting personal information about them, why it is being collected, who it may be disclosed to (including us) and how their personal information will be handled. The statement also refers the client to the privacy policy posted on our website. Typically, this statement will be included in our FSG (although it can be given separately) and acknowledged in our client application processes.

Only collect relevant client information



We only collect the type of personal information about our clients which is described and included in our Privacy Policy.

We do not collect personal information about a client from a third party unless it is unreasonable or impractical to collect it directly from the client.

When gathering information about a client, the information must be relevant for our purpose of providing financial services, as well as our obligation to comply with requirements imposed by law. For instance, questions about a client's job and income are directly relevant to their financial position, whereas in most circumstances, their religion or ethnic background is irrelevant. Details about religion, ethnic background, political beliefs, criminal record, trade union membership, and sexual orientation are all types of sensitive information for the purposes of the privacy legislation, and heightened obligations apply to the management of sensitive information. This is another reason to avoid collecting this information in the first instance.

Health information (including Covid-19 information) is also sensitive information, and this is discussed further below.

Using and disclosing our client's information



We only collect, hold, use and disclose personal information for the purposes disclosed in our Privacy Policy.

Generally, this will be for the purpose of providing the financial products and services requested by our client. If we disclose a client's personal information for a secondary purpose, then subject to some limited exceptions, that purpose must be related to the primary purpose **and** one that the client would **reasonably expect**. Disclosure of sensitive information for a secondary purpose must be **directly** related to the primary purpose for which it was provided. Sensitive information includes disclosure of information about mental or physical health, or genetic or biometric data, which may have been collected for advice on insurance cover.

For example: it may be necessary for us to disclose some of a client's health information to an external compliance auditor for the purpose of auditing the quality of the advice we provided to them. This is allowed. However, if we disclosed our client's health information to a marketing company which wanted to sell the client medical equipment, this would breach the privacy legislation.

Use or disclosure of client personal information for **direct marketing purposes** is not permitted, unless either **express consent** has been obtained (e.g. at the time of client onboarding) or the person would reasonably expect their personal information to be used or disclosed for this purpose.

It is **not** sufficient to assume that the client would reasonably expect to receive the marketing material because of the client's profession, interest or hobby. The Australian Information Commissioner's view is that a person is not likely to have a reasonable expectation that their personal information will be used or disclosed for direct marketing purposes if the person has been notified that their personal information will only be used for a particular purpose unrelated to this.

If we wish to use our clients' personal information for the purpose of direct marketing, we include a consent to direct marketing in our standard fact finder, and always provide a means by which a client may request not to receive direct marketing communications (also known as 'opting out'), and that we comply with that request. This means that we must have a policy in place to track which clients do not want to receive direct marketing, and if a client has opted out of receiving direct marketing communications, we must ensure that they do not, in fact, receive direct marketing materials.

We may disclose a client's personal information for a purpose unrelated to providing financial advice if we have obtained our **client's written consent** to the disclosure.²

Disclosing client's information to a third party (e.g. accountant)

When we disclose **personal information** of a client to a third party (e.g. accountant or lawyer), we ensure that the third party recipient signs a privacy agreement or acknowledgement whereby they agree to treat the personal information in accordance with the obligations set out in the privacy laws.

Disclosing and providing information under the new reference checking protocols

We ensure that we comply with *ASIC Corporations and Credit (Reference Checking and Information Sharing Protocol) Instrument 2021/429* ('the Protocol') when employing/authorising representatives or responding to a reference request. Compliance with the Protocol is required when there are reasonable grounds to suspect that a prospective AFSL representative will provide personal advice to retail clients about relevant financial products.³ Similarly, the Protocol will also apply to prospective ACL representatives when there are reasonable grounds to suspect that the potential representative will provide credit assistance in relation to credit contracts secured by mortgages over residential property, and be a mortgage broker or a director, employee or agent of a mortgage broker.⁴

As a 'recruiting licensee', we take reasonable steps to seek a written consent, in the form set out in the Protocol, from a prospective representative before we ask for a reference from a 'referee licensee'. If consent is refused, we cannot request a reference from a referee licensee under the Protocol. Consents will cease after 12 months from when they are given, or earlier if withdrawn. Information we obtain is handled consistently with the consent given and used only for:

- considering a prospective representative's suitability for employment or authorisation, and
- complying with the general conduct obligations of a licensee.

Keep information up-to-date

We ensure that client files are regularly checked and the client's information is kept accurate and up-to-date. We build this policy into our regular review with clients.

Compliance tip: If we use any standard form checklists in our annual review, we ensure that they include a check that the client's contact, financial and medical records (if applicable) have not changed.

Keep information secure

APP 11 requires that reasonable steps must be taken to protect personal information that we hold from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

The steps we take to protect personal information are:

- we store each client's file in a secure cloud-based location accessible to authorised personnel only, which adequately protects it from misuse or loss
- hard copy filing systems are under lock and key, and all electronic files are password protected, with security software installed and regular back-ups taken
- client files are not left lying around on desks or taken home, and access is only available to appropriate persons

Where some or all of our employees are working remotely and are accessing clients' personal information, we ensure that the employees' devices have the necessary security updates installed, and can only access our computer system via a secure remote desktop application. We also consider whether to implement multifactor authentication procedures for remote access to systems and resources.

It is also a requirement of APP 11 that reasonable steps are taken to destroy or de-identify personal information when it is no longer required.

The destruction and de-identification of personal information is undertaken in accordance with our Information Management Policy, including:

- Retaining documents required by law for the statutory period (e.g. 7 years for some transaction data under AML/CTF law), but de-identifying it and restricting access.
- Having or improving high levels of encryption on sensitive data (e.g. passwords or tax file numbers).
- Not retaining credit card or payment information, unless allowed by PCI-DSS requirements.

We also shred or use secure paper disposal services for hard copy documents, and have information destruction processes in place to securely dispose of electronic files.

We think the steps taken to protect personal information are reasonable for a business of our size and nature.

Allow client access to their file

The law requires us to provide our client with access to their file upon receiving a reasonable request. The client also has a right to correct the personal information in their file. The exception to this rule is where the information is relevant to current or anticipated legal proceedings or a criminal investigation.

We respond to the client's request 'within a reasonable period after the request is made'. In responding, we either give access to the personal information that is requested, or notify the individual of our refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

We may have grounds to refuse an access request in some limited circumstances including where giving access to personal information would:

- unreasonably impact on the privacy of other individuals;
- be reasonably likely to pose a serious threat to the life, health or safety of any individual (or more broadly);
- be relevant to a legal dispute you are having, or may have, with the person making the request; or
- amount to a breach of any relevant law.



Before responding to a request for access, we should seek further guidance from the AFSL Responsible Manager in these situations. Refer to our Privacy Access Request Refusal Letter tool.

Transferring information overseas



Our Privacy Policy must set out if we are likely to disclose client personal information to overseas recipients (including IT service providers if our website is hosted overseas, or we use cloud-based or web-based data storage, software or applications), and the countries where the personal information is likely to be sent.

We are likely to disclose client personal information to overseas recipients and the countries where personal information is likely to be sent are:

- Philippines

If, for whatever reason, we need to transfer a client's personal information outside of Australia (including because our website is hosted overseas, or we store information on a cloud-based or web-based server located overseas, or we use web-based software or applications that are hosted overseas), and the privacy laws equivalent to the *Privacy Act 1988* ('the Privacy Act') do not apply, we take reasonable steps to ensure that the overseas recipient complies with the APPs. The steps we take to ensure that overseas entities that receive personal information from us comply with the APP obligations⁵ are:

- ensuring this as a term of our contractual arrangements;
- due diligence when appointing and ongoing monitoring of outsourced providers;
- not disclosing information to entities based overseas, unless we are happy that their privacy controls are at least as rigorous as Australian-regulated entity privacy controls;

(i.e. by including this obligation in our contractual arrangements).

Treat tax file numbers with care

The *Privacy (Tax File Number) Rule 2015* ('TFN Rule') regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act.

If a client file includes a **tax file number** ('TFN'), then the file must also include a **written authority** from the client for us to use the TFN.

We explain the **legal basis** and **intended purpose** for collecting the client's tax file number (for example, collecting the TFN as required under taxation legislation in order to provide the client with professional services connected with that legislation). We also make the client aware that declining to provide it is not an offence, as well as the consequences of not quoting the TFN.

Where an **accountancy practice is** operated in conjunction with our financial services business and a client is referred to us from the accountancy side, then a **new authorisation** from the client for the TFN is **obtained**. This is because the tax file number is now required for a different and separate purpose.

We ensure that the TFN is protected by security safeguards to prevent unauthorised access, use or disclosure.

If we no longer require TFN information, we do not continue to hold it and we destroy it securely.

For example: if we collect TFN information from a client for the purpose of reporting that information to the Australian Tax Office, then after that report is made, the relevant TFN information is not retained. One way of achieving this is by 'blacking out' the TFN data in the relevant documents on file.

Unauthorised use or disclosure of a tax file number is an offence which carries significant penalties.

Addressing a suspected or known data breach

A **data breach** occurs when **personal information** is accessed or disclosed in an unauthorised way or is lost.

A **data breach** could occur in a number of ways. Some examples include:

- a mobile phone, laptop or removable storage device containing personal information is lost or stolen;
- sending an email containing personal information to the wrong recipient;
- accessing or disclosing personal information outside the requirements or authorisation of their employment;
- databases or an email account containing personal information are 'hacked' into or otherwise illegally accessed by an individual;
- a client file is lost or stolen;
- paper records are stolen from insecure recycling or garbage bins.

Data breaches can give rise to a range of actual or potential harms to individuals and entities.



There are data breach reporting obligations that apply to any organisation covered by the privacy legislation (which may include an individual who is an authorised representative, or a corporate authorised representative). If we suspect or know that a data breach has arisen, we consult the Data Breach Response Policy.

Each breach is dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

The actions taken following a data breach generally follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach and evaluate the potential harm to affected individuals and, where possible, take action to remediate any risk of harm.

Step 3: Notify individuals and the OAIC if required. If the breach is an 'eligible data breach', such notification may be mandatory.

Step 4: Review the incident and consider what steps can be taken to prevent future breaches.

If remedial action is successful in preventing a likely risk of serious harm to individuals, the notification obligations may not apply.

An **eligible data breach** occurs when each of the following **three criteria** are satisfied:

- a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
- b) this is likely to result in **serious harm** to one or more individuals; and
- c) the entity has not been able to prevent the likely risk of serious harm with remedial action.

'**Serious harm**' is not defined in the legislation. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

We take into account the following (non-exhaustive) list of 'relevant matters' in assessing the likelihood of serious harm:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures, the likelihood that any of those security measures could be compromised
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security, technology or methodology:
 - was used in relation to the information; and
 - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
 - have obtained, or who could obtain, the information;
 - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates; and
 - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology

- the nature of the harm
- any other relevant matters.



See the Data Breach Response Policy for more information.

References

Related policies and tools

Policies	Breach (Reportable Situation) and Events Reporting, Credit Information, Data Breach Response, Risk Management.
Tools	Privacy Access Request Refusal Letter, Privacy Policy and Collection Statement (Privacy Policy).

Legislative requirements and references

Law	<i>Corporations Act 2001</i> <i>Privacy Act 1988</i>
Legislative Instruments	<i>ASIC Corporations and Credit (Reference Checking and Information Sharing Protocol) Instrument 2021/429</i>

¹ The EU General Data Protection Regulations (GDPR) can apply to companies outside of the EU. You will need to understand whether you must comply with the GDPR. Examples of when a company situated outside of the EU will have to comply with the GDPR are:

- If you process personal data of an EU citizen on behalf of, or in connection with another business, or an office situated in the EU;
- If you offer of goods or services to EU citizens (this requires some type of actively marketing goods or services to EU citizens); or
- You have website cookies and/or use website analytics.

If you do not have to comply with the GDPR requirements you can delete this obligation

² If you are a credit provider, you must comply with additional requirements when disclosing credit information.

See Sections 21D, 21E, 21F, 21G, 21H, 21J, 21K, 21L, 21M, 21N and 21NA of the *Privacy Act*.

³ Section 912A(3C) of the *Corporations Act 2001*.

⁴ Section 912A(3D) of the *Corporations Act 2001*.

⁵ Australian Privacy Principle 8.