Oreana
FINANCIAL SERVICES

Oreana Privacy Guidelines

Date: 4 March 2022 (Version 1.0)

Relevant legislation and principles

- Privacy Act 1988 (legislation.gov.au)
- Australian Privacy Principles - Home (oaic.gov.au) (acronym APP)

Introduction

The Privacy Policy Act 1988 (Cth) and the Australian Privacy Principles (APPs) govern the handling of personal information and informs of the privacy implications when using and storing client information.

Effective management of personal information is an important component of the advice process. You must comply with the regulations and Licensee requirements when collecting, storing and maintaining your records.

Information is a valuable asset in a financial planning context, especially given the increased use of the internet and mobile devices as a form of communication. There are real concerns in the community about how information is used and shared.

These concerns are even stronger where the information is sensitive or very personal. However, these concerns must be balanced against the competing interests of commercial organisations to handle and use personal information in the course of conducting business.

Oreana Financial Services Pty Ltd recognises the importance of clients understanding how we deal with their personal information.

This is outlined below.

Compliance with this policy ensures that Oreana Financial Services Ltd employees, advisers and support staff comply with the relevant provisions of the Privacy Act 1988 and the APP's.

Oreana Financial Services Privacy Policy

Oreana is required to have a privacy policy in place which addresses the following:

- the kind of personal information that is being collected;
- how that information is being collected and for what purpose;
- how an individual may access personal information or make a complaint; and whether the personal information is likely to be disclosed overseas, and if so where.

Compliance with this policy ensures that Oreana Financial Services Pty Ltd employees, it's advisers and support staff are aware of, and follow the relevant provisions contained in the Privacy Act 1988 and the APP's.

If a client requests for a copy of the Privacy Policy, you can direct them to here: Privacy Policy - Oreana Financial Services. You should have the Oreana privacy policy (or your own approved version of a privacy policy) on your practice website. You can also furnish them with a hard copy found on the adviser portal here: Home Landing Page – Oreana Advisor Portal (oreanafinancial.com) or refer them to your FSG.

Only collect relevant client information

You must only collect the type of personal information about your clients which is described and included in the Privacy Policy.

You must 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 your purpose of providing financial planning services, as well as your 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 is also sensitive information, and this is discussed further below.

Using and disclosing your client's information

You must only collect, hold, use and disclose personal information for the purposes disclosed in your Privacy Policy.

Generally, this will be for the purpose of providing the financial products and services requested by your client. If you 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 you to disclose some of a client's health information to an external compliance auditor for the purpose of auditing the quality of the advice you provided to them. This is allowed. However, if you disclosed your client's health information to a marketing company which wanted to sell the client medical equipment, this would breach the privacy legislation.

Direct Marketing

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 you wish to use your clients' personal information for the purpose of direct marketing, you should add a consent to direct marketing the fact find process/template, and always provide a means by which a client may request not to receive direct marketing communications (also known as "opting out"), and comply with that request. This means that you 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, you must ensure that they do not in fact receive direct marketing materials.

You may disclose a client's personal information for a purpose unrelated to providing financial advice if you have obtained your **client's written consent** to the disclosure.

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

When you disclose **personal information** of a client to a third party (e.g. accountant or lawyer), you should ensure that the third party recipient receives and acknowledges our privacy policy or acknowledgement whereby they agree to treat the personal information in accordance with the obligations set out in the privacy laws. The provision of your FSG is a demonstration point that you have actioned this point.

You should also have the client consent to you providing personal information to a requested third party. You can find the template for this here: Home Landing Page – Oreana Advisor Portal (oreanafinancial.com) (refer to 'Client Authorisation for Additional Information **to** other institutions or advisers).

The above form should also be used where you are passing a partner's information to the other partner.

Collecting information from a third party

If you are gathering information about a client from third parties, such as the client's super provider or accountant), you will need to seek consent from the client first. You can do this via the Oreana Information Release form found here: Home Landing Page – Oreana Advisor Portal (oreanafinancial.com)

Existing clients

You must provide your client with the updated FSG and the Privacy Policy (should it change – and as found in the FSG) at the earliest opportunity and at the latest when you next interact with them.

Keep information up-to-date

You must ensure that client files are regularly checked and the client's information is kept accurate and up-to-date. This remains a critical part of your review process.

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

Keep information secure

Ensure that your client's file is stored in a secure location which adequately protects it from misuse or loss. Hard copy filing systems should be under lock and key, and all electronic files should be password protected, with security software installed and regular back-ups taken. Client files should not be left lying around on desks or taken home, and access should only be available to appropriate persons. Your business should have a **clean desk policy.**

Where some or all of your employees are working remotely, and are accessing clients' personal information, ensure that the employees' devices have the necessary security updates installed, and

can only access your computer system via a secure remote desktop application. You should also consider whether to implement multifactor authentication procedures for remote access to systems and resources.

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

Use password secure technology

Please ensure you have some technology in place to save your passwords and share internally. A free tool can be utilised via www.lastpass.com

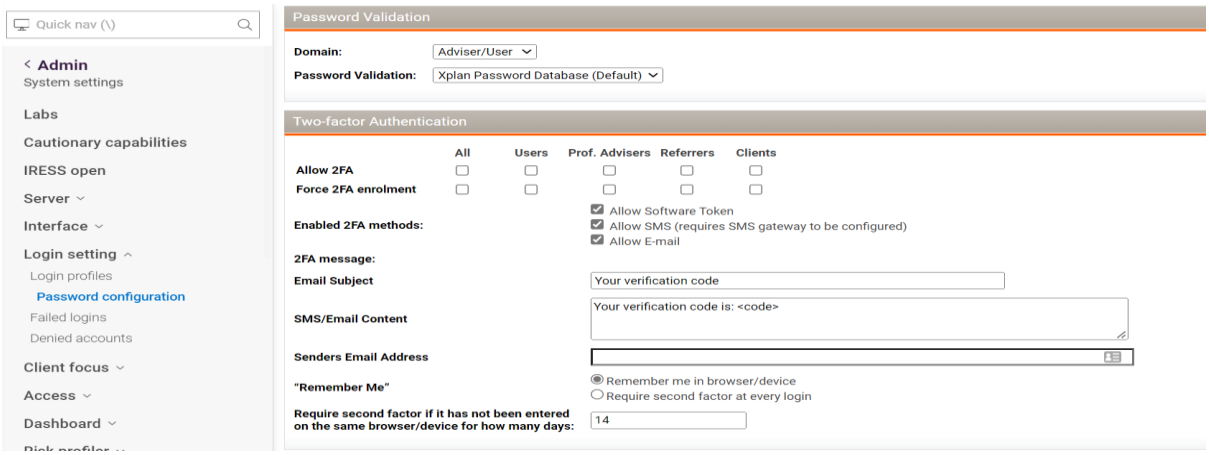
It is crucial you do not share passwords over email, text, internal chat.

Xplan 2 Factor Authentication

You may wish to apply 2 factor authentication when logging into xplan.

You will need to navigate to: Admin > System Settings > Login Settings > Password configuration (see screenshot below)

This must be set up on a user-by-user basis and is at the discretion of each practice



You also have the ability to select the 2FA method being either a software token (authenticator app), SMS (if they have SMS gateway configured) or email.

Allow client access to their file

The law requires you to provide your 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.

You must respond to the client's request "within a reasonable period after the request is made". In responding, you must either give access to the personal information that is requested, or notify the individual of your 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.**

You 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, you should seek further guidance from the compliance team in these situations.

Transferring Information Overseas

If, for whatever reason, you need to transfer a client's personal information outside of Australia (including because your website is hosted overseas, or you store information on a cloud-based or web-based server located overseas, or you use web-based software or applications that are hosted overseas), and the privacy laws equivalent to the *Privacy Act 1988* do not apply, you must take reasonable steps to ensure that the overseas recipient complies with the Australian Privacy Principles (i.e. by including this obligation in your contractual arrangements).

Oreana can assist with this process. Where you are utilising an outsource provider, you should notify the Licensee (Head of Operations), of this. The Licensee maintains a record of outsource providers, where their data is stored, and their privacy standards. **Please refer to the Oreana Outsourcing Guidelines.**

Privacy Policy statement – Sending Information Overseas

It is for the above reason that Oreana references data possibly being held offshore. You can reference the statement with regards to data being held offshore here: Privacy Policy - Oreana Financial Services

Should your website not link into Oreana's privacy policy page because you have white labelled it, please ensure your template matches that of Oreana's.

The below template must be in the privacy policy made available to all clients:

Sending information overseas

Depending on the nature of the engagement or purpose of collection, we may disclose your personal information to other entities and suppliers overseas in accordance with the Privacy Act. These countries may include (though not limited to) Singapore, Hong Kong and the United States.

We may store, process or back-up your personal information on servers that are located overseas (including through third party service providers). In some circumstances, Oreana Financial Services Pty Ltd also uses third party service providers located overseas to carry out its functions and provide services. By submitting your personal data to us, you acknowledge and agree with your data being processed on Oreana Financial Services behalf by its suppliers. While we have made reasonable efforts to secure your information, some of our suppliers may not provide privacy protection at a level consistent with the Australian Privacy Principles.

We have taken reasonable steps to ensure that the recipient does not breach the Act and the Australian Privacy Principles.

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 you to use the TFN. This OFS TFN Authority form can be found here: Home Landing Page – Oreana Advisor Portal (oreanafinancial.com)

You must 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). You must 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 your financial planning business and a client is referred to you from the accountancy side, then **a new authorisation** from the client for the TFN **must be obtained**. This is because the tax file number is now required for a different and separate purpose.

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

If you no longer require TFN information, you must not continue to hold it and must destroy it securely. As such, once the client is no longer an ongoing fee-paying client, you must delete the TFN from xplan before archiving. This includes ensuring TFN's in application forms are blanked out.

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

Xplan TFN retention

Once you have a TFN Authority signed by the relevant client saved to file, you may wish to adopt one of the below options with respect to TFN retention within xplan:

1. **Update TFN -** Allows user to update but not view, merge or export client TFN
2. **View TFN -** Allows user to view, merge and export client TFN

Each practice will need to inform the licensee of the user access per person within each practice.

To hence make the process of removing TFN from files over time, you may wish to utilize the TFN fields in xplan and blank out TFN's in other documents (such as application forms) once no longer required (such as once the submission with a provider has been finalized).

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.

If you suspect or know that a data breach has arisen, you must contact the licensee immediately. You may also wish to visit the website of the OAIC to consult resources on dealing with a data breach, or seek professional advice, found here: Notifiable data breaches - Home (oaic.gov.au)

Each breach will need to be 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 should 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.

The licensee will 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

You can notify the licensee of data breaches via the Potentially Reportable Situations link found here: Reporting a Complaint or Incident (openafsl.com) This information is stored and managed by the Licensee via the Assured Support system; Open AFSL.