Privacy Policy

Overview

"This document outlines the Privacy ('Policy') of Xplore Wealth Ltd ACN 128316441 Limited and all related entities (Collectively referred to as 'Group' or 'Xplore').

Xplore and its subsidiaries are committed to protecting the privacy of all clients and personal (and sensitive) information we collect when doing business and are committed to ensuring we uphold both the rules and intent of the Privacy requirements.

As part of this commitment and as a mechanism to ensure compliance with the Privacy Act 1988 (Cth) (Privacy Act) and Privacy Amendment (Notifiable Data Breaches) Act 2017 (Privacy Amendment Act), we have developed and implemented a Privacy Policy (the Policy).

This Policy sets out our practices with respect to the collection and management of personal and sensitive information in all areas, and has been developed under the Australian Privacy Principles (APPs) (established under the Privacy Act) which provides the standards, rights and obligations for the handling, holding, accessing and correction of personal (including sensitive) information.

This Policy also sets out our practices with respect to Data Breaches and has been developed under the Notifiable Data Breaches (NDB) scheme (established under the Privacy Amendment Act) which outlines Xplore's data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

What is personal information?

Personal information is defined in law as "information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not". Examples include an individual's name, address, contact number and email address.

Special provisions apply to the collection of personal information which is sensitive information. Sensitive information includes, for example, information about a person's health, membership of a professional or trade association.

What personal information do we collect?

We may collect and hold personal information for the purposes of managing our business, providing products and services, in administering products and services, and making information available about other products and services.

The financial products and services provided by us include both direct to client services and services provided through financial advisers and fund managers.

The information we collect directly from clients, financial advisers, fund managers, and other AFS Licensees, may include name and contact information (including email address), residential and or postal address, date of birth, tax file number (TFN), occupation, employer, bank account details, financial information, data required for anti-money laundering counter-terrorism financing purposes; and any other information required to administer the products and services we provide (including information required by law).

Much of this information is collected using online facilities or through ongoing communications.

There may be specific circumstances in which we will ask for sensitive information. We will only collect sensitive information where we have consent to the collection of the information and it is reasonably necessary for us to administer your business or employment with us.

The sensitive information we may collect may include:

- details of dependents,
- personal health information
- income information
- marital status; and
- membership of professional associations and trade unions.

How do we collect and hold personal information?

When we collect personal information directly from an individual, we take reasonable steps at, or before the time of collection to ensure that the individual is aware of certain key matters, such as:

the details of the entity collecting the personal information;

- the purposes for which we are collecting the information (including for example where required by law);
- the organisations (or types of organisations) to which we would normally disclose information of that kind;
- the main consequences if all or some of the personal information is not collected;
- the fact that an individual can access the information and how to contact us to either access or correct their personal information;
- the fact that an individual may complain about the handling of their personal information if they believe it has not been handled in accordance with the Privacy Act, and how the Xplore will deal with the complaint.

We will not collect any personal or sensitive information about you except where you have knowingly provided that information to us or we believe you have authorised a third party to provide that information to us.

We will collect personal information directly from an individual where it is reasonable and practicable to do so. Where we collect information from a third party such as financial advisers, fund manager, or another AFS Licensee, we will still take reasonable steps to ensure that an individual is made aware of same information set out above.

You are not required to give us the information that we request, however if you choose not to provide the information we ask for, or the information you give us is not complete or accurate, this may for

example, prevent or delay the processing of your business, affect your eligibility for specified products, or it may prevent us from contacting you. It may also (in certain circumstances) impact on the taxation treatment of an account with us.

We take reasonable steps to ensure that the personal information that we collect, use and disclose is accurate, complete and up to date. We advise clients to keep their information up to date and provide mechanisms for them to do so.

We take reasonable steps to protect the personal information and sensitive information that we hold from misuse and loss and from unauthorised access, modification or disclosure by using security procedures and up to date technology. Account information is password and security protected and all instructions are verified before they are processed.

Personal information is stored on secured systems, and within our corporate technology infrastructure. Data is backed up regularly and is stored to ensure both the availability and security of the backup information.

Any personal information sent to external locations is secured with encryption.

We may disclose personal information to the following when undertaking our business:

- internally to our staff and related bodies corporate;
- professional advisers nominated by clients;
- financial institutions, where necessary, to allow us to establish accounts or other banking facilities;
- promoters;
- a financial institution;
- any organisations or professional advisers involved in providing, managing or administering our products or services such as auditors, accountants, lawyers, custodians, external dispute resolution services, insurers, investment managers or mail houses, within normal business practices;
- medical practitioners and other relevant professionals, as appropriate;
- your personal representative, or any other person who may be entitled to receive a death benefit, or any person contacted to assist us to process that benefit;
- support services;
- any fund (administrator or Xplore) to which a superannuation benefit is to be transferred or rolled over; and
- where otherwise required or authorised by law.

We will also disclose your personal information if you give us your consent.

If other organisations provide support services to us, they are required to appropriately safeguard the privacy of the personal information provided to them.

Where personal information collected is no longer needed for any purpose that is permitted by the Privacy Act, we can delete, destroy or permanently de-identify the personal information as required.

Use of Commonwealth Government Identifiers

We do not use Commonwealth government identifiers (Identifiers) as our own identifier of individuals or accounts. We will only use or disclose Identifiers in the circumstances permitted by the Privacy Act.

Purposes of collection

We will only collect personal information from an individual or third party which is reasonably necessary to provide our products or services (primary purpose). We collect personal information for the following primary purposes, including:

- processing applications and other transactions for products and services offered by us and our clients;
- providing information and communications to members and other account holders,
- for the operation of products and services offered by us and our clients, or to comply with the requirements of the Corporations Act 2001 (Cth) or any licensing or other regulatory requirements or obligations;
- to record and maintain member and investor details necessary for providing the services offered by us and our clients;
- establishing accounts or other banking facilities on an individual's behalf with third party financial institutions and administering an individual's accounts or other banking facilities;
- communicating with clients, including for the purposes of direct marketing communications (where permitted by law);
- conducting our internal business operations, including meeting any relevant regulatory or legal requirements;
- as agent, collecting information to enable our clients and counterparties to comply with Anti-Money Laundering and Counter-Terrorism Financing Law; and
- assessing applications for employment.

Individuals can request not to receive direct marketing communications by following the opt-out method provided within our communication.

Personal (and/or sensitive) information may also be disclosed where for example it is required by law, or a permitted general or health situation exists in relation to the use or disclosure. This may include for example situations in which the entity reasonably believes that the disclosure of personal information is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or that of the public.

Accessing your personal information or making a complaint

Any individual about whom we hold personal information, can contact us to access and correct their personal information. We may charge a reasonable fee to cover our costs.

We will take all reasonable steps to provide access to or amend any personal information that is incorrect. If we are unable to correct your personal information, or give you access to the information, we will advise you with an explanation in writing.

If you believe that we have not dealt with your personal information in accordance with this Policy or

the APPs, you may make a complaint to us.

You can contact us to either access or correct personal information, or complain about any breach of the APPs by writing to the Privacy Officer at:

The Risk and Compliance Department
PO Box R1197
ROYAL EXCHANGE NSW 1225

We will acknowledge a complaint in writing within 7 days of receipt, and process and respond to your complaint within 30 days. If we cannot resolve your complaint within 30 days of receipt, we will contact you with an explanation and see permission for an extension of time.

If (after 30 days) you are not satisfied with our response, you may raise your concerns with the Office of the Australian Information Commissioner:

Online: www.oaic.gov.au
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Fax: +61 2 9284 9666
Mail: GPO Box 5218, Sydney NSW 2001 or GPO Box 2999, Canberra ACT 2601.

Disclosing personal information

Some of our third party contractors and service providers may perform certain services for Xplore. As a result, personal information collected by us may be disclosed to a third party recipient.

We take reasonable steps to ensure these recipients comply with the APPs by implementing contractual arrangements with Xplore as service providers to ensure the personal information is appropriately safeguarded and to ensure that our service providers comply with the APPs.

Notifiable Data Breaches

We are required to notify individuals at risk of serious harm and the Australian Information Commissioner (the Commissioner) about 'eligible data breaches'.

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that Xplore holds
2. this is likely to result in serious harm to one or more individuals, and
3. Xplore has not been able to prevent the likely risk of serious harm with remedial action.

In circumstances where it is not clear if a suspected data breach meets these criteria we will take all reasonable steps to conduct an assessment within 30 calendar days after the day they became aware of the grounds (or information) that caused it to suspect an eligible data breach.

There are some exceptions to the notification requirements, which relate to:

- eligible data breaches of other entities
- enforcement related activities
- inconsistency with secrecy provisions
- declarations by the Commissioner.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

Xplore's data breach response approach will guide staff on the steps they are required to undertake following a data breach. Firstly, any suspected data breach of any magnitude should be immediately advised to the Head of Risk Management, Compliance and legal and/or the CEO as soon as any breach is suspected [whether or not confirmed] with a view of containing the breach to prevent any further compromise of personal information.

We will then assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm. Where serious harm cannot be mitigated through remedial action, we will notify the individuals at risk of serious harm and provide a statement to the Commissioner as soon as practicable.

The statement and/or notification about an eligible data breach will include:

the identity and contact details of Xplore

- a description of the eligible data breach
- the kind or kinds of information involved in the eligible data breach
- what steps Xplore recommends that individuals take in response to the eligible data breach

If it is not practicable to notify the individuals at risk of serious harm, we must publish a copy of the statement prepared for the Commissioner on our website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

If a single eligible data breach applies to multiple entities, only one entity [Xplore] needs to notify the Commissioner and any individuals at risk of serious harm. It is up to the CEO to decide which entity notifies, however the entity with the most direct relationship with the individuals at risk of serious harm should generally undertake the notification.

Availability of our Privacy Policy

Our Privacy Policy is available free of charge on our public website.

Ends.