

Privacy Policy

Discovery Asset Management Pty Ltd

ACN: 168 787 353

Corporate Authorised Representative No.: 456684

Date of Issue: April 2014



What you need to know

- Discovery Asset Management Pty Ltd complies with the Australian Privacy Principles (APPs) set out in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*.
- This policy outlines the standards for the collection, disclosure and handling of personal information by Discovery Asset Management Pty Ltd.
- The Privacy Officer must be notified of all queries relating to the privacy of an individual's personal information.
- A breach of this policy will be recorded in Discovery Asset Management Pty Ltd's Breach Register.
- Discovery Asset Management Pty Ltd will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

The Policy was approved by the Board on the above date and replaces any previous versions of the Policy.

Table of Contents

PART A – Privacy Policy	3
1 Commitment to the Policy	3
2 Policy Owner	3
3 Purpose of this Policy	3
4 Who Should Know and Understand the Policy	4
5 Risks of Non-Compliance to the Company	4
6 Legislative and Regulatory Requirements	5
7 Summary of the Australian Privacy Principles (APPs)	5
8 Policy Statement	6
Part B – Operational Procedures	13
9 Review of the Policy	13
10 Record Keeping	13
11 Training on the Policy	13
12 Applying Discretion to the Policy	14
13 Related Policies	14
14 Further Information.....	14
Appendix A – Legislative and Regulatory References	15
Appendix B – Privacy Policy Register Template	16

PART A – Privacy Policy

1 Commitment to the Policy

The Board of Discovery Asset Management Pty Ltd ('Discovery', 'the Company', 'we', 'us' or 'our') is committed to complying with the Australian Privacy Principles ('APPs') of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988* ('the Act').

This Privacy Policy and Procedure ('Policy') has been adopted by the Board and presents the framework upon which the Company will meet its privacy obligations under Act. The APP's prescribes standards for the collection, disclosure and handling of personal information.

Where there is any doubt as to the requirements contained in this Policy, you should have regard to the principle that the Board will always ensure the Company conducts its financial services business in a fair, honest and professional manner in line with the regulatory objective of ensuring the confident and informed participation of consumers in the Australian financial system.

We may vary this Privacy Policy from time to time.

2 Policy Owner

The owner of this Policy is the Privacy Officer ('Policy Owner'). The Policy Owner is responsible for ensuring that the Policy is reviewed annually or when it requires updating (e.g. because of regulatory or operational change).

3 Purpose of this Policy

This Policy relates to the Company in its capacity as a corporate authorised representative of an AFS licensee.

The purpose of this Policy is to identify what the Company must do when collecting, disclosing and handling personal information.

The aim of this Policy is to:

- Outline the process taken for the collection, storage, use and disclosure of personal information collected from the client;
- To protect against the misuse and loss of personal information held by the Company; and
- Promote a culture of compliance.

4 Who Should Know and Understand the Policy

The following people should be aware of the contents of this Policy:

- Directors;
- All employees and representatives who are directly or indirectly involved in providing financial services under the corporate authorised representative agreement;
- Anyone providing services to the Company that the Policy Owner determines should comply with the Policy (e.g. service providers, agents, contractors and temporary staff); and
- Anyone else that the Policy Owner determines should comply with the Policy.

Where functions of the Company are outsourced (e.g. to service providers, agents, contractors and temporary staff), the Company remains responsible and accountable for those actions. The Company may include specific requirements in the outsourcing or other agreements to ensure compliance with this Policy and other regulatory obligations.

Failure by a service provider, agent, contractor or temporary staff member to comply with this Policy or to deliver their contracted services may result in a breach of the agreement and consequently a breach under this Policy. The agreement should provide for actions that either party can take where a breach of the agreement has occurred and/or it may be dealt with according to the Company's Breach Management Policy.

To ensure all officers, employees and agents are aware of the contents of this Policy, it will be made available in a common directory accessible by all relevant staff. An abbreviated form of the policy will also be made available on our website.

5 Risks of Non-Compliance to the Company

The risks to the Company of not complying with this Policy include:

- **Regulatory risk**

The risk that the Company, its officers, employees or agents will be subject to criminal, civil or administrative penalties or sanctions. This could include the termination of our corporate authorised representative agreement, the suspension, cancellation or imposition of additional conditions on the Licensee's AFS licence, or the Licensee being required to provide an enforceable undertaking, being subjected to investigative action, or other remedial actions for non-compliance.
- **Business risk**

The risk that breaches of obligations or failure to resolve breaches may result in poor business outcomes for the Company, with a key risk being termination of the corporate authorised representative agreement and the inability to maintain operations. Compliance with this Policy will enable the Board and delegated staff to appropriately manage this risk by implementing appropriate breach identification, assessment, rectification and procedures.

- **Reputational risk**

The associated damage to the Company's reputation as a result of public reporting of non-compliance with our obligations or by being perceived as non-compliant within the market. This may also have a detrimental affect on the profitability of the Company due to loss of confidence by clients. By approving and implementing a robust Privacy Policy, the Company intends to mitigate our reputational risk.

6 **Legislative and Regulatory Requirements**

Obligations Under the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Privacy Act 1988

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and the *Privacy Act 1988* sets out harmonised privacy principles that regulate the handling of personal information collected by the Company.

The Australian Information Commissioner will also has enhanced powers, including the ability to:

- accept enforceable undertakings
- seek civil penalties in the case of serious or repeated breaches of privacy
- conduct assessments of privacy performance for Australian government agencies and businesses.

7 **Summary of the Australian Privacy Principles (APPs)**

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use of disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

8 Policy Statement

About this Privacy Policy

This Privacy Policy outlines to you all the ways in which the Company aims to protect your personal information and what sort of personal information we hold about you, for what purposes and how it is collected, held, used and disclosed.

Personal information is any information, including an opinion, that can be used to identify an individual or can be linked to an individual.

By continuing to use the products and services provided by the Company, you consent to us dealing with your information in the manner set out in the Privacy Policy.

What information we collect

- Subject to legislative requirements, we will only collect personal information relevant to our business relationship with you. There is some personal information, which is reasonably necessary for us to collect to be able to provide you with a specific product and service, maintain your contact details, consider applications and approaches you make to us, and in order for us to satisfy our obligations under relevant legislation such as the Anti-Money Laundering and Counter Terrorism Financing Act 2006 ("AML-CTF Act"). If you do not provide this personal information we may not be able to provide you with the product or service you have requested.
- Personal information is any information, including an opinion, that can be used to identify an individual or can be linked to an individual.
- Depending upon the products or service you have requested, some examples of the type of information we collect are your name, address, contact details, tax file number, date of birth, and information about your use of our products and services.
- The collection of sensitive personal information is restricted by the provisions of the Privacy Act. This means we will not collect any sensitive information, such as personal information relating to your religious views, ethnicity, political opinion, criminal record, health personal information or sexual preference, unless this is necessary to provide you with a specific product or service and you have consented to that collection.

How we collect your information

- If it is reasonable and practicable to do so, we collect personal information directly from you. How we collect your information will depend upon how you interact with us. We may collect it through application forms, telephone, email and internet contact, from correspondence with you or your adviser and in person.
- There are occasions where we may need to collect personal information from other parties with or without your direct involvement. Depending upon the product or service you have requested, some examples of the persons or organisations from which we may collect personal information, include:
 - ❖ service providers engaged to do something for or on behalf of us
 - ❖ publicly available sources of information (such as telephone directories)
 - ❖ your representative (such as your legal adviser or financial adviser)

Collection information from our website

- We may collect statistical information on website activity, such as the number of users who visit, the date and time of visits, the number of pages viewed and how users navigate through our website. We will be aware of your identity if you log into our web sites. This information is collected through the use of cookies.
- A cookie is a small data file that's automatically placed on your computer's hard disk, and it contains information in relation to your visit to a web site.

- A cookie is created on your hard disk when you log into the secure areas of our web sites. This cookie ensures that accurate information is provided to you while you're transacting online. As soon as you log out of the secure areas, this cookie is deleted.
- Also, another cookie may be stored on your hard disk when you log into our web sites. This cookie lets us analyse our site traffic patterns with the view to continually improving our web sites. This cookie is not deleted once you log out of our secure areas.
- You can configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is sent. Refer to your browser instructions or help screens to learn about these functions. If you reject all cookies, you may not be able to use our website.

Using and disclosing your personal information

- When we collect personal information from you, we will inform you of the purposes for which it is collected. Primarily, this will be to establish and administer the financial products or services we provide to you (such as investments), or to comply with legislative requirements such as the AML-CTF Act.
- We may also use your personal information to:
 - ❖ provide additional services to you, such as market updates and information on products and services available from us. You can notify us at any time if you do not wish to receive any marketing information (see Marketing products and services to you).
 - ❖ carry out our business which includes performing our internal administration and operations including: accounting, risk management, record keeping, archiving, systems development and testing and staff training
 - ❖ develop and establish products and services and conduct market research
 - ❖ undertake planning and statistical analysis
 - ❖ assist you in your queries
 - ❖ prevent fraud and crime in relation to products and services you invest in or we provide; and
 - ❖ fulfil our legal requirements (for example, disclosure to enforcement bodies such as the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO), the Australian Transaction Reports and Analysis Centre ("AUSTRAC") or the courts).
- We may need to disclose your personal information to another person or organisation. However, we will only disclose your personal information where we are allowed to by law and have your express or implied consent, or where we are obliged to by law.
- You can give express consent by, for example, telling or agreeing with us in writing (such as, by signing an application form) or by telling us verbally.

- Implied consent is where we have reasonably assumed you have given consent from your behaviour.
- Where we disclose your personal information to organisations that perform specific essential services for us, for example mailing, we limit this disclosure to the information they need to perform the service.
- Depending upon the products or service you have requested, we may exchange information about you with, for example:
 - ❖ agents, contractors and external service providers of the Company
 - ❖ other financial institutions, including stockbrokers, custodians, and portfolio service providers
 - ❖ payment systems operators
 - ❖ regulatory bodies, government agencies and law enforcement bodies
 - ❖ agents acting on your behalf, including your legal adviser and financial adviser
 - ❖ your executor, administrator, trustee, guardian or attorney
- Those parties which supply services to us, and to which we disclose personal information, have undertaken to comply with our confidentiality requirements under privacy law.
- Sometimes a service provider or your adviser may be located outside Australia. We may transfer your information to a person such as this who is outside Australia only if:
 - ❖ the recipient of the information is subject to law, binding scheme or contract that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles (APPs) protect the information and there are mechanisms that you can access to take action to enforce the protection of the law or binding scheme;
 - ❖ we have your consent to do so; or
 - ❖ the disclosure of the information is required or authorized by or under Australian law or a court/tribunal order.
- The parties with whom we share personal information that operate outside Australia, operate in the following countries (Canada, Hong Kong, Luxembourg, Malaysia, United Kingdom and United States).

Marketing products and services to you

We may use your personal information to offer you other products and services.

We may offer you products and services by various means - including by email, or other electronic means.

From our current relationship with you, we believe that we have your implied consent to do so unless you have told us that you do not wish to receive them.

However, you can notify us at any time if you do not wish the Company to use your details to send these offers. The Company will act promptly on your request which you can make by

Phone:	Client Services on 07 3259 7650
Email:	clientservices@discoveryam.com.au
Mail:	Discovery Asset Management Pty Ltd, Client Services, GPO Box 922, Brisbane QLD 4001

Protecting your information and web site security

- We will take reasonable steps to protect your personal information from misuse, loss and unauthorised access, modification and disclosure.
- Paper documents are protected from unauthorised access or use through the various security systems that we have over our physical premises. We also maintain up-to-date computer and network security systems with appropriate firewalls, encryption technology and passwords to protect electronic copies of personal information.
- To ensure the security of your personal information, we ask that you observe the security requirements that relate to the use of your personal identification number and/or passwords used to access your investments or products or use our services electronically.
- We will take reasonable steps to destroy personal information in a secure manner or remove identifying features from it, if it is no longer required by us. This is subject to any legal obligations we have to retain information for a certain period of time.
- In order to protect your personal information online, we use up-to-date and secure technology methods.
- Stored personal information about you is further protected from unauthorised access through the use of multiple firewalls, secure passwords and sign in processes:
- We cannot guarantee the policies and procedures of any other websites that may be linked from our website. They may or may not comply to the same privacy standards that we do and therefore you should take care to evaluate their particular privacy standards and procedures as needed.

Using government identifiers, such as Tax File Numbers and Medicare numbers

- We do not use Tax File Numbers, Medicare numbers or any other government identifier for the purposes of identifying you with our products or services.
- The only circumstances in which we collect, use or disclose these numbers is where we are required or authorised by law to do so. For example, we may be required by law to disclose your Tax File Number to the Australian Tax Office.

Keeping your information accurate and up-to-date

- We maintain your personal information by taking reasonable steps to make sure that the personal information collected, used and disclosed is accurate, complete and up-to-date.
- So that we can maintain the accuracy of your personal information at all times, we ask that you notify us immediately when you change your contact details such as your telephone number or address, or if you become aware that any personal information we hold about you is incorrect.

Accessing your information

- You can access most of the personal information we hold about you and request corrections.
- Your right of access is subject to some exceptions. For example, you may not be able to obtain access to personal information which:
 - ❖ would reveal personal information about another person
 - ❖ would reveal a commercially sensitive decision making process; or
 - ❖ we are prevented by law from disclosing.
- We will tell you why if we are unable to give you access to your personal information on request.
- You can request access to your personal information by contacting us by phone on (07) 32597650 or by email privacy@discoveryam.com.au;
- This service is free unless the personal information you request requires research or preparation time. Before we act upon requests of this nature, we will provide you with an estimate of how much this service will cost and obtain your agreement before proceeding.

Dealing with us anonymously or under a pseudonym

You can deal with us anonymously or you may use a pseudonym where it is lawful and practical to do so. For example, you may enquire about our products or request a copy of our disclosure documents. However, we regret that we will not be able to offer you the product or services if we cannot identify you.

Changes to the privacy policy

We can make changes to our privacy policy and the processes and systems relating to how we handle your personal information, from time to time, and for any reason. We will update this policy to reflect any changes.

Resolving your privacy issues

Discovery is bound by the Act and the Australian Privacy Principles for the handling of personal information, which are set out in that Act. Our policies, processes and systems have been developed to ensure we comply with all our obligations under the Act.

If you have a privacy concern:

Step 1. Contact our Privacy Officer

Phone:	Privacy Officer on 07 3259 7650
Email:	privacy@discoveryam.com.au

Where possible, your concerns received over the telephone will be resolved at that time and your concerns received via email will be resolved within five working days.

Step2: Contact Office of the Australian Information Commissioner or FOS

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner. The Commissioner can be contacted on the privacy hotline: 1300 363 992.

Part B – Operational Procedures

9 Review of the Policy

The Privacy Officer shall review the contents of this Policy at least annually or as required to ensure it remains current and relevant to the operations of the Company.

As part of the review, the Privacy Officer shall also ensure that any related policies or procedures are reviewed by relevant officers, employees and/or agents. The Privacy Officer will maintain a schedule of reviews to be undertaken as part of the review of this Policy.

The Privacy Officer shall report the findings to the Board once the review has been finalised.

10 Record Keeping

The Privacy Officer is responsible for ensuring that the following information in relation to this Policy is retained for a period of at least 7 years:

- All approved versions of this Policy (including details of their approval);
- Any relevant registers which relate to the Policy;
- Records evidencing compliance or non-compliance with the Policy;
- Details of any reviews undertaken;
- Evidence of induction and ongoing training; and
- Any other documentation relevant to the implementation of and compliance with the Policy.

11 Training on the Policy

As the Board is committed to ensuring the continued compliance with this Policy, a program of regular training sessions will be provided to staff both when they commence and on an ongoing basis.

Training attendance will be recorded in the individual staff member's Training Register and it is the responsibility of the Compliance Officer to review whether relevant personnel have attended appropriate training.

Induction Training

The Privacy Officer and/or the Compliance Officer will provide training on the Privacy Policy and procedure as part of the induction training for all relevant new officers and employees.

Ongoing Training

The Privacy Officer and/or Compliance Officer will also provide refresher training on the Policy and procedure annually to all relevant staff (or as required, where a material change is made to the Policy).

12 Applying Discretion to the Policy

Notwithstanding any requirement contained in this Policy, the Policy Owner may apply, or authorise the application of, reasonable discretion in considering how to apply the requirements of the Policy.

When applying discretion in relation to a particular matter, the Policy Owner shall have regard to the level of risk posed by that matter and relevant regulatory objectives.

Whenever discretion has been exercised in relation to the policy, it should be recorded and reported to the Board.

13 Related Policies

The following policies contain provisions which are directly or indirectly related to the contents of this Policy:

- Compliance Arrangements Policy;
- Complaints Handling and Dispute Resolution Policy;
- Adequacy of Resources Policy;
- Organisational Competence policy;
- Risk management Policy;
- Compensation and Insurance Arrangements Policy;
- Conflicts of Interest Policy; and
- Code of Conduct.

14 Further Information

If you need further information regarding this Policy and how it is implemented you should contact the Policy Owner.

Appendix A – Legislative and Regulatory References

The following sources of information have been used in developing this Policy:

Corporations Act:	Nil
Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Privacy Act 1988:	Australian Privacy Principles (APPs)
Corporations Regulations:	Nil
AFS/Australian Credit licence special licence conditions:	Nil
ASIC policy/guides:	Nil
Australian Standards:	Nil
Commitments made to ASIC:	Nil
Forms:	Nil

Appendix B – Privacy Policy Register Template

No	Date	Version number	Details of change/amendment to the Policy	Person Responsible
1.	April 2014	2014.01	Policy adopted	Channel Capital - David Costello / Jo Hill