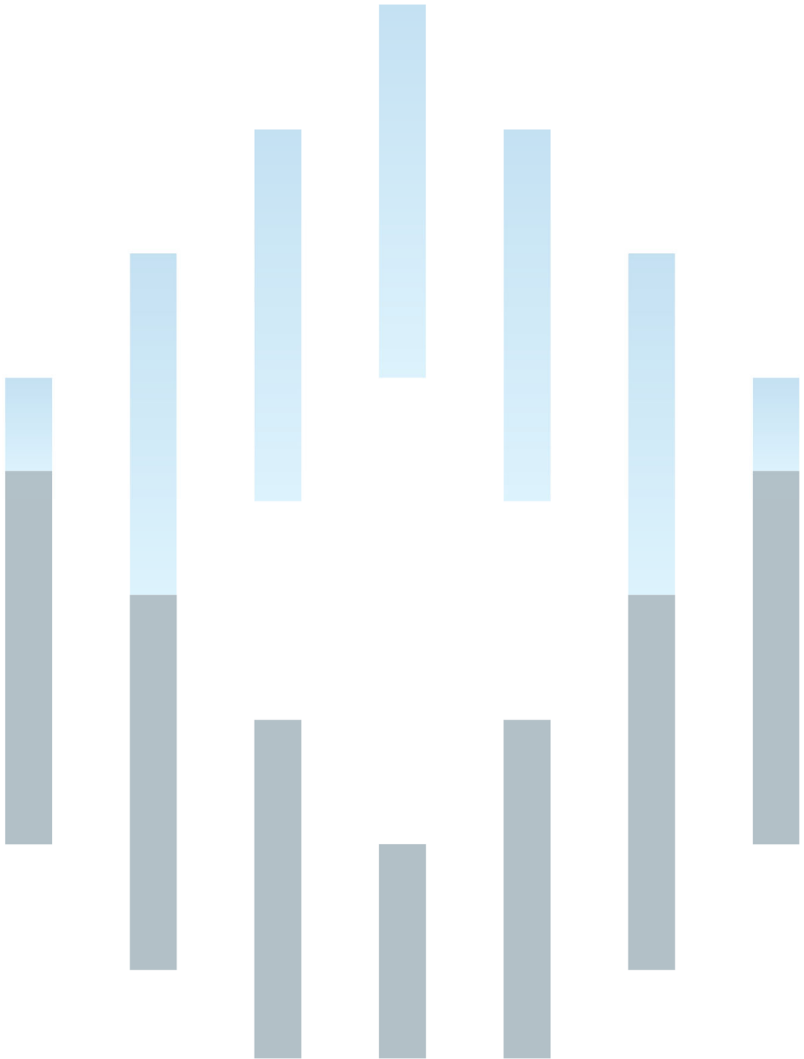
Palisade Investment Partners Limited

Privacy Policy

October 2024



Document Control

Version Control / Revision History

This document has been through the following revisions:

Version	Date of Approval	Remarks/Keys Changes/Reason for update
1		Initial Version
1.2	April 2010	Revision
2	January 2012	Annual Review
2.1	January 2014	Review
3	May 2014	Review
3.1	April 2015	Annual Review
3.2	April 2016	Annual Review
3.3	May 2017	Annual Review
3.4	May 2018	Annual Review
3.5	May 2019	Annual Review
3.6	February 2022	Review
4	October 2024	Captures changes to regulatory requirements since the last review in 2022 as well as inclusion of Privacy Statement (Appendix 1)

Authorisation

This document requires the following approvals:

Authorisation	Name
Initial Version	Palisade Board
Annual Revisions	Managing Director

Scope

This Policy applies to employees of:

- Palisade Investment Partners Limited (Palisade, or the Company) and its subsidiaries; and
- associated companies of Palisade that have adopted this Policy

Reference to the Company in this Policy refers to Palisade, its subsidiaries and each associated company.

Palisade Privacy Policy

Contents

1. Introduction

The Company is committed to complying with the Australian Privacy Principles (**APP**') which form part of the *Privacy Act 1988 (Cth)* (**Privacy Act**).

This Policy presents the framework upon which the Company will handle, hold, access and correct personal information.

2. Application of the Policy

This Policy applies to all employees and service providers engaged by the Company. Information disclosed to any of these individual members in performing their duties of employment for the Company are taken to be disclosed to the Company.

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.

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.

In addition, all employees of the Company are required to complete training on this Policy upon commencement and on an annual basis.

2.1 What personal information does the Company or Service Providers engaged by the Company collect?

Personal information is information relating to an individual, which can be used either alone or with other sources of information to identify that individual.

The types of personal information that we collect depends on our relationship with you, and may include:

- Identification data (full name, title, date of birth, passport number, driver's licence number, tax identifiers, signature);
- Contact data (personal address, telephone number, email address);
- Electronic Monitoring data (to the extent permitted by law, we may record and monitor your electronic communications with us);
- Financial data (bank account number);
- Marketing and Communications data (marketing and communication preferences, tracking data relating to whether you have read marketing communications from us);
- Professional Information data (position/job title, work address, telephone number, email address);
- Profile data (username and password for our online services that you have access to, investments made by you, services requested, marketing communications responded to, survey responses);
- Services data (payment details to and from you, details of services you have provided to us or we have provided to you.

Sensitive personal information includes information relating to race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions or associations, trade union membership or associations, information about health and genetic and biometric data.

In limited circumstances, and where allowed by law, we may collect information about:

- criminal convictions and offences, when legally required;

- sexual orientation if you provide details of your spouse or partner;
- political affiliations for us to determine whether you are a politically exposed person.

2.2 How do we collect Personal Information?

We collect personal information in a number of ways:

- when you or your authorised representatives provide (or update) personal information in connection with a product or service we offer (such as an investment application form or communications with our representatives);
- from organisations or entities that you represent, to whom we provide services;
- through your use of our website (including subscribing for news and insights); and
- from publicly available information.

2.3 Collecting information through our website

Web analytics
We collect data about your interactions with our website. The main purpose of collecting your data is to improve your experience when using our site. We also use this data to understand and report on which content pages and downloads are accessed by visitors.

The types of data we collect with these tools include:

- your device's IP address (collected and stored in an anonymized format);
- search terms and pages visited on our website;
- date and time when pages were accessed;
- downloads, time spent on page, and bounce rate;
- referring domain and out link if applicable;
- device type, operating system and browser information;
- device screen size;
- geographic location (city).

If your web browser has Do Not Track / Incognito enabled, we will not track your visit.

Cookies
Cookies are small data files transferred onto computers or devices by websites for record-keeping purposes and to enhance functionality on the website. Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please set your browser preferences to reject all cookies before accessing our website.

Email lists, registrations and feedback
We will collect information that you provide to us when signing up to mailing lists and registering for our events, or when submitting feedback on your experience with our website.

We use Salesforce Account Engagement to manage our mailing lists. When subscribing to one of our mailing lists, you will be asked to give your express consent that the Pinnacle Group and affiliated investment managers may use your data for analytics purposes. Analytics are performed when you open an email and click on links in the email. They include which emails you open, which links you click, your mail client (e.g. 'Outlook 2016' or 'iPhone'), if your action occurred on 'mobile' or 'desktop'.

We use Cvent to manage event registrations. When registering for an event, you may be required to give Cvent personal information including your name, company telephone number and email address.

Social networking services
We use social networking services such as LinkedIn to communicate with the public. When you communicate with us using these services, we may collect your personal information, but we only use it to help us to communicate with you. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies.

3. Consideration of Personal Information

3.1 Open and Transparent management of personal information

This Policy details the steps taken to ensure the Company complies with the APPs and operates in conjunction with the Company's complaints handling policy.

This Policy is made available upon request as per the Privacy Statement on the Company website.

3.2 Anonymity and Pseudonymity

The Company is subject to certain legislative and regulatory requirements which requires it to obtain and hold detailed information of an individual. For example, due to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**), the Company is obligated to obtain customer identification to whom the Company provides a designated service.

Where the Company is required by a law to deal only with an identified individual, the Company will ensure that the collection does not go beyond the requirements of the law and the requirements are clearly disclosed to the individual.

It is also impracticable for the Company, as a financial services company, to provide ongoing services if the individual does not identify themselves.

3.3 Collection of Personal Information

The Company will only collect personal information which is necessary for its functions as is required by law. The Company will not collect sensitive information about any individual unless the individual has consented to provide the information or authorised for a third party to provide that information.

The Company may collect personal information (other than sensitive information) from a related body corporate and service providers in some circumstances such as for the secondary purpose of marketing.

3.4 Dealing with unsolicited personal information

As a general rule, personal information provided to the Company that is additional to the information that has been requested by the Company will be treated as unsolicited personal information.

Where it is unclear whether the information is solicited or unsolicited personal information, the Company will treat the personal information as unsolicited personal information.

The Company will destroy or de-identify all unsolicited personal information that it determines it could not have collected under the APPs as soon as practicable, if it is lawful and reasonable to do so.

If the Company does not destroy the unsolicited information, it will ensure that:

- a notice of collection is provided, where required;
- the personal information may only be used or disclosed for the primary purpose for which it was collected;
- the security of the information must be protected;
- an individual can request access to the personal information; and
- an individual can request the entity to correct the personal information.

3.5 Notification of the collection of personal information

In general, the Company will notify or ensure awareness of notification of collection of personal information matters as follows:

- if the Company collects personal information directly from an individual who completes a form, clearly and prominently displaying the notification of collection of personal information matters in the form, or providing a readily accessible and prominent link to an APP 5 notice;
- if personal information is collected by telephone, explaining the APP 5 matters to the individual at the commencement of the call. Where this is not practicable, the Company will give the individual information about the notification of collection of personal information matters as soon as possible afterwards, such as in any subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the Company's website;
- if the Company collects personal information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf.

Where it is not reasonable to notify or ensure awareness of the full range of APP 5 matters, the Company will refer the individual to this Privacy Policy and advise the individual to contact the Privacy Officer with any enquiries.

In addition to the conditions of notification of collection of personal information matters, for U.S. clients under Regulation S-P the Company will provide an initial copy of this privacy policy at the time of engagement. The Company will provide U.S. clients with prompt notice of any change to the Company's privacy policy and will give clients sufficient opportunity to opt out of any new disclosure provisions. On an annual basis, the Privacy Officer will review the Company's Privacy Policy and confirm that the Company (i) only shares non-public personal information with non-affiliated third-parties in a manner that does not require an opt-out right be provided to clients and (ii) has not changed its Privacy Policy with regards to disclosing non-public personal information since it last provided a privacy notice to the Company's clients. If the Company cannot confirm these conditions, it will provide a copy of the privacy notice to all U.S. clients describing the Company's privacy policy. The Privacy Officer will retain a copy of the privacy notice sent and will make and retain a record of its distribution.

4. Dealing with personal information

4.1 Use or disclosure of personal information

The Company will only use personal information it collects from individuals for the purpose they have provided and for the purpose disclosed to the individual at the time of collection or otherwise set out in this Policy.

The Company may disclose personal information to third parties on a confidential basis. These parties include, but are not limited to:

- external service providers (such as Pinnacle, registries, administrators, auditors, and providers that host our website servers, manage our IT and human resources information);
- persons authorised by you (such as an adviser or person with power of attorney);
- competent authorities (including any national and/or international regulatory or enforcement body, agency, court or other form of tribunal or tax authority) or their agents where we are required or allowed to do so under applicable law or regulation;
- any person to whom disclosure is allowed or required by applicable law or regulation.

4.2 Direct Marketing

The Company will only use or disclose an individual's personal details for the purpose of direct marketing when:

- the individual has consented to the use or disclosure of their personal information for that purpose;
- the Company has notified the individual that one of the purposes for which it collects the personal information is for the purpose of direct marketing;
- the Company made the individual aware that they could request not to receive direct marketing communications from the Company, and the individual does not make such a request.

Upon request from the individual to identify the source of the personal information that it uses or discloses, the Company will endeavour to provide the information generally within 30 days unless:

- a considerable time has lapsed since the personal information was collected by the organisation;
- for personal information collected before commencement of the APPs, it is possible that the source of the personal information was not recorded.

4.3 Cross-border disclosure of personal information

The Company may transfer personal information about an individual to an overseas recipient only if:

- The recipient of the information is subject to a law, or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to the APPs and mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme;
- The individual consents to the transfer;

- The transfer is required or authorised by law;
- The transfer is in a general permitted situation; or
- The transfer is for an enforcement related activity.

4.4 Adoption, use or disclosure of government related identifiers

The Company has its own identifiers for individuals (clients). It will not adopt other identifiers nor disclose this identifier to external parties unless the disclosure is necessary for the Company to fulfil its obligations to external service providers or government agencies or regulators.

5. Integrity of Personal Information

5.1 Quality of Personal Information

The Company will ensure the quality of personal information it collects at two distinct points in the information handling cycle. The first is at the time the information is collected. The second is at the time the information is used or disclosed, particularly if the collection and disclosure is required by law.

5.2 Security of Personal Information

The Company will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

The Company will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed except where required by law, e.g. AML/CTF Act requires information on client identification be retained.

6. Access to, and correction of, personal information

6.1 Access to Personal Information

The Company must be satisfied that a request for personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf.

Where an individual requests access to their personal information which the Company holds, a reasonable fee may be charged to provide this access.

The Company will endeavour to respond to any legitimate request for access within 30 days depending on the complexity of the information and/or the request. If the client's request is urgent, this needs to be indicated clearly.

Requests regarding the client's personal information could be addressed to the Privacy Officer:

By mail: PO Box R1313
Royal Exchange NSW 1225
By email: Risk.Compliance@pinnacleinvestment.com

6.2 Correction of Personal Information

At all times, the Company will endeavour to ensure that the personal information it holds about an individual is up to date and accurate. If the individual, or authorised person acting on the individual's behalf, after appropriate

identification verification, can confirm the personal information the Company holds is inaccurate, the Company will take all reasonable steps to correct the information.

If the original information was sourced or maintained by another organisation, the Company may advise that organisation of the updated or corrected information unless it is impractical or unlawful to do so.

Request for correction of person information can be made to the Privacy Officer:

By mail: PO Box R1313
Royal Exchange NSW 1225
By email: Risk.Compliance@pinnacleinvestment.com

7. Images and Videos Individuals

Images of individuals in photographs or video (images) are treated as personal information under the Privacy Act where the person's identity is clear or can reasonably be worked out from that image. Images of individuals may also contain sensitive information if, for example, the individual's racial or ethnic origin or religious beliefs is apparent.

The Company may only collect images of identifiable individuals if it is reasonably necessary for one of the Company's functions or activities.

Consent is not required to collect image of identifiable individuals unless the image records sensitive information about the individual. However, the Company must take reasonable steps to make sure the individual is aware of the following:

- who the Company is and how they can contact the Company
- how, when and from where the images are being taken
- if the collection of the images is required or authorised by law
- what the Company is taking their image for
- if there are any consequences for them if the Company does not collect their image
- any other organisations or people with whom the Company usually share personal information
- how they can get access to it later, and
- whether the Company is likely to send the images overseas.

8. Data Breach

A data breach is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, the Company's database containing personal information is hacked or the Company mistakenly provides personal information to the wrong person.

A 'data breach' may also constitute a breach of the Privacy Act, however this will depend on whether the circumstances giving rise to the data breach also constitute a breach of one or more of the APPs.

In the event that any staff of the Company identifies a data breach, it is taken to be a compliance incident and must be reported and managed in accordance with the Incident and Breach Management Policy.

In assessing whether a data breach needs to be notified to the OAIC and affected individuals, the OAIC's resource at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying- eligible-data-breaches should be consulted, as well as the following three questions:

1) Has there been unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that we hold?
2) If yes to (1), is it likely to result in serious harm to one or more individuals?
3) If yes to (1) & (2), have we been able to prevent the likely risk of serious harm with remedial action?
4) If no to (3), does an exception apply? (See: https://www.oaic.gov.au/privacy-law/privacy- act/notifiable-data-breaches-scheme/exceptions-to-notification-obligations)

These questions are incorporated into the Incident and Breach Form to aide assessment as to regulatory reporting requirements.

9. Complaints

If an individual wishes to complain about any breach or potential breach by the Company of this Policy or the APPs, the individual should contact the Privacy Officer:

By mail: PO Box R1313
Royal Exchange NSW 1225
By email: Risk.Compliance@pinnacleinvestment.com

The complaint will be considered and responded to within 30 days and in accordance to the Company's complaints handling policy. The complaint may be handled by an external dispute resolution scheme. Lastly, if the complaint has not been resolved to the complainant's satisfaction, the individual is entitled to contact the OAIC (www.oaic.gov.au).

10. Monitoring and Review of the Policy

The Privacy Officer will ensure compliance with this Policy by the Company and review the contents of this Policy every two years to ensure that it remains current and relevant to the operations of the Company. The Privacy Officer will report any issues related to privacy to the Company Board.

As part of the review, the Privacy Officer will also ensure that any related policies / agreements are reviewed by relevant employees and/or service providers.

Appendix 1 - Privacy Statement

Palisade Investment Partners Limited ("Palisade") understands and appreciates that you, as a visitor to our website, under the domain name www.palisadepartners.com.au ("Website"), are concerned about the confidentiality and security of information that Palisade may collect from you. Palisade is committed to providing you with information on our services within a secure and confidential on-line environment.
This Privacy Statement applies to the Website and forms part of Palisade's Privacy Policy. This Privacy Statement will explain how personal data will be treated as you access and interact with the Website.

WHAT INFORMATION WE COLLECT FROM YOU

We will not collect any information that identifies you as an individual unless you knowingly provide it to us. Any personal information you supply will be used only in accordance with this Privacy Statement and our Privacy Policy.
The personal data about you which the Website may collect includes:

- Information collected when you register or update an online profile, which may include personal data such as your name and contact details;
- Information collected when you submit your resume or application to us for consideration of employment;
- The content of electronic forms you submit via the Website, requesting us to provide services or information, or take actions;
- Information submitted if you participate in an online survey or competition; and
- Any messages or comments you submit to us via the Website, which may include personal data such as name, email address and telephone number.

In common with many commercial websites we may also collect aggregated information which tells us about visitors to the Website but not the identity of those visitors. For example, we may collect information about the date, time and duration of visits and which pages of the Website are most commonly accessed. This information is used by us to help to administer and improve the Website.

USE AND DISCLOSURE OF INFORMATION

In addition to providing our products and services to you, any information we collect about you, may be used by Palisade's associated entities or any entity carrying out functions on behalf of Palisade for:

- The purpose of enabling Palisade to provide services or information to you in accordance with your requests or reasonable expectations;
- The purposes of enabling Palisade to undertake research, planning, product development, risk assessment, risk modelling and marketing; and
- Any other purpose required by or to the extent permitted by law.

We will only disclose personal information to third party entities carrying out functions on behalf of Palisade on a confidential basis.
You should note that information we collect from you may also be disclosed to third parties if that disclosure is required by or to the extent permitted by law.

SECURITY OF YOUR INFORMATION

Palisade regards the security of your personal information as a priority and takes all reasonable steps to protect your information from loss and unauthorised access, destruction, use, modification or disclosure.

The Company has implemented various safeguards to keep your personal information secure, including information and communication technology security, access security, internal training programs and managed detection and response service.

While we take reasonable steps to preserve the security of your personal information, there are inherent risks in transmitting and storing information and we cannot ensure or warrant the security of any information we hold.

The Website may contain links to other websites, and Palisade is not responsible for the privacy practices or the content of those websites.

COOKIES

A cookie is a small data file placed on your computer by Palisade's server. A cookie contains information about your visit to the Website. When you visit the Website again, our server will look for the cookie and structure itself based on the information provided. A cookie identifies your computer to our web server when you visit the Website. We do not use the cookie to store your personal information. Palisade uses browser cookies to improve the speed and reliability of our security system. It is recommended that you turn off any cookie warnings in your browser before using the Website, otherwise you may not be able to enjoy the full functionality of the Website.

ACCEPTANCE AND CHANGES TO THE PRIVACY STATEMENT

You acknowledge and accept that your use of the Website indicates your acceptance of the Website's terms and conditions of use and this Privacy Statement. This Privacy Statement may change from time to time, so please refer to the Website from time to time as the Privacy Statement is subject to change. Any information collected after an amended Privacy Statement has been posted on the Website will be subject to that amended Privacy Statement.

ACCESS AND UPDATE OF INFORMATION

You can access and update your personal information that held by us at any time. To amend personal information that Palisade holds, please contact us at enquiries@palisadepartners.com.au or on (02) 8970 7800.

CONTACT US

If you have any questions or feedback about this Privacy Statement, require a copy of our Privacy Policy or wish to make a complaint about the way in which we have handled your personal information, please contact the Privacy Officer, Pinnacle Investment Management Limited, PO Box R1313 Royal Exchange NSW 1225 at any time in writing or send an e-mail to risk.compliance@pinnacleinvestment.com

Appendix 2 - HR Privacy Statement

The Company collects and uses personal information about employees, or prospective employees to help maintain employment related functions. The Company relies on Pinnacle Investment Management Limited to provide its HR administration and payroll administration functions. As such, the Company adopts Pinnacle's HR Privacy Statement as set out below.

Pinnacle Investment Management Limited ABN 66 109 659 109 ('Pinnacle') is committed to ensuring personal information collected or held are handled in accordance with the Privacy Act 1988 (Cth) and our Privacy Policy.

Collection of Personal Information

How we collect personal information

When you apply for a position, or on commencement of employment at Pinnacle, you are asked to supply information to us to enable processing of your employment and to maintain ongoing employment related functions.

In most instances personal information is collected directly from you, except in special circumstances where information about you may be obtained from third parties (e.g. police checks). In circumstances where Pinnacle is required to collect personal information we will do so only by lawful and fair means. When Pinnacle collects your personal information, we will take reasonable steps to notify you of:

- Why we are collecting the information
- Any third parties to whom we may disclose personal information as required by law

Why we collect personal information

Pinnacle collects personal information as part of our contractual relationship with individuals to allow us to ensure payment for employment services rendered.

How we use your personal information

Personal information collected or held by us or our service providers will be used for managing processes associated with your employment relationship with Pinnacle. Activities may include payroll, human resources management, superannuation, risk management (workers compensation insurance), recruitment and audit.
Personal information may also be used in statistical or aggregated forms for staff planning or for purposes required by Australian government legislation, for example Australian Taxation Office legislation.

Storage and security of personal information

How we store your personal information

Pinnacle store your personal information in a combination of electronic and paper formats. Stringent security procedures in combination with physical and technological systems, provide a robust security environment which restricts access to authorised personnel only. Personal information is disposed of in accordance with the relevant laws, other legal instruments and normal administrative practice. Material is destroyed via a secure service provider.

Disclosure of personal information

When we disclose your personal information

In general, Pinnacle will only disclose your personal information to third parties (including related companies) where required, such as Financial Institutions or Superannuation Funds on the basis that they deal with such information in accordance with their respective privacy policies. These service providers may be located outside of Australia where your personal information may not receive the same level of protection as that afforded under Australian law.
In addition:

- Pinnacle will disclose your personal information when required to do so by law. This could be as a requirement to satisfy warrants, subpoenas, court orders or other commission orders.

- Pinnacle may also disclose personal information to a third party if there are reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of you or another person.

We do not sell, rent or trade your personal information. Personal information is not released outside Pinnacle except in the circumstances described above.
No personal information about staff will be released to the media by Pinnacle without the consent of the individual concerned.

Accessing and Accuracy of Personal Information

How you can access your personal information

You have the right to access personal information held about you by Pinnacle. You are also entitled to request that personal information held about you is accurate and up-to-date, and therefore be amended accordingly. As the accuracy of information held depends largely on the information you provide, we recommend that you:

- advise us immediately if there are any errors in your personal information, and
- keep us up to date with changes to your personal information, such as name and address details.

How to contact us

To access your personal information, contact the Chief Financial Officer on telephone: (07) 3107 2803 or email: risk.compliance@pinnacleinvestment.com.

For a copy of our Privacy Policy, please contact the Privacy Officer (Compliance Manager) via email at Risk.Compliance@pinnacleinvestment.com or telephone (02) 8970 7705.

Complaints
If you believe your privacy has been breached by Pinnacle, you may contact the Compliance Manager.
Telephone: (02) 8970 7705
Email: Risk.Compliance@pinnacleinvestment.com