

PMG PROPERTY FUNDS MANAGEMENT LIMITED

Client Privacy Policy

Document Owner	Approving Party
EA & Governance	Compliance Officer

Version	Amendments	Approved by	Active Date From
1.0	Approval of initial policy	Board of Directors of PMG	2 February 2019
2.0	Review and update	Board of Directors of PMG	1 June 2019
3.0	Updated to reflect Privacy Act 2020	Board of Directors of PMG*	4 February 2021
3.1	Updated for SG comments - reference to regulatory access to records for clarity	^^	April 2021
4.0	Review and update	Compliance Director	28 Feb 2023
5.0	Review and update	Compliance Director	28 Feb 2024
6.0	Review and update	Compliance Officer	6 March 2025
7.0	Review and update	Compliance Officer	26 February 2026
8.0	Update to reflect the recent changes to privacy legislation including the NZ Privacy Amendment Act 2025 to address the IPP 3A notification obligation	Compliance Officer	05 May 2026

Introduction

We know that how we collect, use, disclose and protect your information is important to you, and we value your trust. That's why protecting your information and being clear about what we do with it is a vital part of our relationship with you.

The purpose of this Privacy Policy is to inform our clients and any users of our digital platforms about how we collect, store, use and disclose personal information that we collect from you or that we have obtained about you from a third party. This Privacy Policy sets out various rights that you have in relation to that personal information. It also otherwise explains how we comply with the requirements of the New Zealand Privacy Act 2020 ("the Privacy Act") in managing personal information.

If you do not agree with this Privacy Policy, please do not contact us through any of our digital platforms but call us on (07) 578 3494.

Collection of personal information

Personal Information is defined in the Privacy Act as information about an identifiable individual (a natural person as opposed to a company or other legal entity).

Types of personal information we collect.

The types of personal information we collect will vary depending on the nature of your dealings with us. We only collect personal information that is necessary for the lawful purposes for which we collect the information. Where reasonable and practicable, we will collect your personal information directly from you and inform you that we are collecting it.

We mainly collect personal information directly from you, for example:

- Directly from you, including when you complete an application from for our products or services, or over the telephone or a video call (such as over Microsoft Teams, Zoom or Skype) e.g., when you contact our staff.
- Through one of our digital platforms like our website and social media pages (including through any online chat, or virtual assistant, or bots).
- In the course of conducting customer due diligence, including through our AML service provider FirstAML.
- From third parties acting on your authority or who you authorise us to make contact with about you (e.g., authorised representatives to your account).

- When you email or write to us seeking information about us, our products or services or anything on our website; or
- When you participate in a marketing campaign, competition, or promotion (or a similar event) administered by us or our representatives.

If it is not obvious that we are collecting personal information from you, we will do our best to make it clear to you so that you are always aware when information is being collected.

Generally, the types of personal information we collect, and hold include your:

- Name
- Date of birth
- Contact details (such as your email address, postal address, phone number)
- IRD Number
- Financial information
- Bank account details
- Nominated beneficiaries.
- IP address
- Copies of your verified identification
- Details relating to your use of any product and/or service offered by us.
- Details of your enquiry
- Details of any preferences you tell us about (such as subscription preferences).

We may also collect personal information about you:

- From publicly available sources e.g., via the internet.
- From your professional advisers e.g. (your accountant or solicitor).
- Through the agents and service providers that we may engage to assist us with fulfilling any of the lawful purposes for which we collect your personal information, as outlined below in this policy.

We collect your personal information from the above parties (other than publicly available sources and through our agents and service providers) where we have received your express consent to do so. We are not responsible for the privacy or security practices of the above parties and the parties described above are not covered by this Privacy Policy.

Online device information and cookies

If you are visiting us through our website or social media pages, then we collect information about your use and experience on these by using cookies. Cookies are small pieces of information stored on your hard drive or on your mobile browser. They can record information about your visit to the site, allowing it to remember you the next time you visit and provide a more meaningful experience.

The cookies we send to your computer, mobile phone or other device cannot read your hard drive, obtain any information from your browser, or command your device to perform any action. They are designed so that they cannot be sent to another site or be retrieved by any non-PMG website or social media page.

When you interact with us through our website or social media pages, the information collected through the cookies may include:

- The date and time of visits.
- Website page (or pages) viewed.
- The website from which you accessed the internet and our website or other digital platform.
- How you navigate through the website and interact with pages (including any fields completed in forms and applications completed (where applicable)).
- Information about your location.
- Information about the device used to visit our digital platform; and
- IP address (or addresses), and the type of web browser used.

We will not ask you to supply personal information publicly over any social media platform that we use. Sometimes we may invite

you to send your details to us through a private message, for example, to answer a question. You may also be invited to share your personal information through secure channels to participate in other activities, such as competitions, but we would require your express consent prior to us including you in such activities.

Use of Google Analytics

We use the Google Analytics service, which will issue cookies from its own servers, and which will be able to track visitors throughout our website. For more information on how Google Analytics collects and processes data, you can read Google's Privacy Policy.

Bots

A bot is a piece of software that is programmed to do certain tasks, such as responding to certain phrases with programmed responses. A bot acts in accordance with its instructions, imitating a human user's behaviours, but without a human behind it. PMG may utilise a chatbot function on its website – a software application that conducts an online templated conversation, that stores basic data, so that we may respond to queries. This data is stored confidentially with PMG.

The third-party platform provider (i.e., such as one of our social media pages) may also store your bot conversation. We recommend that you do not share sensitive personal information, such as bank account details, with a bot.

Collection of personal information from third parties

Where we collect personal information about you from someone other than you (for example, from a third party acting on your authority, a service provider, or a publicly available source), we will take reasonable steps, as soon as reasonably practicable, to ensure you are aware that:

- your personal information has been collected;
- the purpose for which it has been collected;
- the name and address of PMG Property Funds Management Limited as the primary agency that collects and holds the information;
- the intended recipients of the information;
- whether the collection is authorised or required by law, and, if so, the relevant law; and
- your rights of access to and correction of that information, unless an exception applies under the Privacy Act 2020.

Purpose of collection and use of personal information.

Any personal information you provide to us may be used to:

- Check whether you are eligible for the product or services offered by us.
- Facilitate those services or provide our services to you.
- Carry out customer due diligence.
- Provide information that you request; and / or
- Provide you with further information about our other products and services.

We also have an obligation to maintain personal information to disclose to regulatory and similar bodies - see "Disclosure of your personal information" below. These bodies have a legal right to such information.

Storage and protection of your personal information

We may electronically record and store personal information which we collect from you. When we do so, we will take all reasonable steps to keep it secure and prevent unauthorised disclosure.

However, we cannot promise that your personal information will not be accessed by an unauthorised person (e.g., a hacker) or that unauthorised disclosures will not occur. If we provide you with any passwords or other security devices, it is important that you keep these confidential and do not allow them to be used by any other person. You should notify us immediately if the

security of your password or security device is breached, this will help prevent the unauthorised disclosure of your personal information.

Your information will be stored electronically on the cloud, by cloud service providers – see “Cloud-based service providers” below.

We use a range of physical and electronic security measures to protect the security of the personal information we hold, including:

- Access to information systems is controlled through identity and access management.
- Our buildings are secured with a combination of locks, monitored alarms and cameras to prevent unauthorised access.
- Employees are bound by internal information security policies and are required to keep information secure.
- Employees are required to complete training about information security and privacy.
- We regularly monitor and review our compliance (and our service providers’ compliance) with internal policies and industry best practice.
- We only keep information for as long as we need it, or as long as the law requires us to. We have a records management process that governs how we manage our information and records to make sure we destroy any information that is outdated, irrelevant or unnecessary.

Cloud-based service providers

We use third party service providers to store and process most of the information we collect. Currently we use AvePoint cloud servers. We ensure that our cloud-based service providers are subject to appropriate security and information handling arrangements and that the information stored or processed by them remains subject to confidentiality obligations.

Timeframes for keeping personal information

We take reasonable steps to destroy or permanently de-identify any personal information as soon as practicable after the date of which the information is no longer required for the purposes which it may lawfully be used (i.e., it has no legal or regulatory purpose, or we have no legitimate business purpose with it).

In the case of information that relates to our advice services or products or services we have provided, we are required by law to hold this information for at least five years. After this time, provided that the personal information is no longer relevant to any service we are providing you, we will take reasonable steps to safely destroy or de-identify any personal information.

If there is a privacy breach

We work hard to keep your personal information safe. However, despite applying strict security measures and following industry standards to protect your personal information, there is still a possibility that our security could be breached. If we experience a privacy breach, where there is a loss or unauthorised access or disclosure of your personal information that is likely to cause you serious harm, we will, as soon as we become aware of the breach:

- **Contain the breach** – Immediately assess and contain the issue to prevent further harm.
- **Assess the risk** – Determine the nature and impact of the breach, considering factors such as:
 - The type of information involved,
 - The extent of unauthorised access,
 - The potential harm to affected individuals.
- **Notify affected individuals and the Privacy Commissioner** – If the breach is likely to cause serious harm, we will:
 - Notify affected individuals as soon as practicable,
 - Report the breach to the **Office of the Privacy Commissioner** via the NotifyUs portal.

- **Take remedial action** – Implement corrective measures to prevent recurrence, such as:
 - Reviewing and updating security measures,
 - Enhancing staff training on data protection.
- **Ongoing Compliance and Review**
 - We will maintain records of all privacy breaches, including our response and corrective actions. Our **Privacy Officer** will review our data protection policies periodically to strengthen compliance.

Disclosure of your personal information

We may disclose your personal information to others outside PMG where:

- It is necessary to enable us to achieve the purpose that we collected the information for.
- We are required or authorised by law or where we have a public duty to do so.
- You have expressly consented to the disclosure, or your consent can be reasonably inferred from the circumstances; or
- We are permitted to disclose the information under the Privacy Act 2020.
- Any regulator that requests the information in the course of performing its regulatory functions.

Parties we may disclose your information to

- Your personal information may be used by us for the purpose of providing advice and services to you and may also be used by agencies such as, but not limited to:
 - Any out-sourced service provider who assists in the services we are required to carry out such as auditors and external compliance reviewers.
 - Our external dispute resolution service.
 - Regulatory bodies.
 - Credit reporting and debt collecting organisations.
 - PMG's related companies.

If we don't need to share your information with a third party in order to provide advice and services to you, we will not pass on your information to them without your consent. Under no circumstances will we sell or receive payment for disclosing your personal information.

Third party websites

Through our website or our other social media pages, you may be able to link to other websites which are not under our control. We are not responsible for the privacy or security practices of those third-party websites and the sites are not covered by this Privacy Policy. Third party websites should have their own privacy and security policies and we encourage you to read them.

In addition, we have no knowledge of (or control over) the nature, content, and availability of those websites. We do not sponsor, recommend, or endorse anything contained on these linked websites. We do not accept any liability of any description for any loss suffered by you by relying on anything contained or not contained on these linked websites.

Right to access and correct personal information.

You have the right to request access to, and correction of your personal information. You can do so by contacting us at:

The Privacy Officer
 PO Box 2034, Seventh Avenue,
 Tauranga 3144
 Or via email at info@pmgfunds.co.nz

When you contact us with such a request, we will take steps to update your personal information, provide you with access to your personal information and/or otherwise address your query within a reasonable period after we receive your request. To protect the security of your personal information, you may be required to provide identification before we update or provide you with access to your personal information.

There is no fee for requesting access to, or correction of, your personal information.

There are some circumstances in which we are not required to give you access to your personal information. If we refuse to give you access or to correct your personal information, we will let you know our reasons, except if the law prevents us from doing so.

If we refuse your request to correct your personal information, you also have the right to request that a statement be associated with your personal information noting that you disagree with its accuracy.

If we refuse your request to access or correct your personal information, we will also provide you with information on how you can complain about the refusal.

What happens if you do not provide us your information?

If you do not provide information we have requested, you may be unable to obtain or access our services for which the information is required. Please ask us if you are unsure what information is important and how this might affect you.

Changes to this Privacy Policy

We review this Privacy Policy periodically (no less than annually) to keep it current and available on our website. If the changes are significant, we may advise you directly. You may also obtain a copy of the latest version by calling us on (07) 578 3494.

Privacy Policy queries and concerns

If you are concerned about how your personal information is being handled or if you feel that we have compromised your privacy in some way, please contact us at:

The Privacy Officer
PO Box 2034, Seventh Avenue, Tauranga 3144 Tel: (07) 578 3494
Email: info@pmgfunfs.co.nz

We will acknowledge your complaint as soon as possible and let you know if we need any further information from you to investigate your complaint.

If you are not satisfied with our response to any privacy related concern you may lodge a complaint on the Privacy Office website (www.privacy.org.nz) or send a complaint form to the Privacy Commissioner at:

Office of the Privacy Commissioner
P O Box 10-094
Wellington 6143, New Zealand Fax: 04- 474 7595
Email: enquiries@privacy.org.nz
Telephone: 0800 803 909 Website: www.privacy.org.nz

