

External Privacy Policy

for Milestone Financial

Including: Milestone Financial Services (Southern) Ltd

Milestone Financial Services (Auckland) Ltd

CML Financial Planning Ltd

Policy owner	Milestone JV
Approver	Milestone Financial JV Board
Review time frame	Annually

Contents

Purpose.....	3
Consent to Privacy Policy.....	3
Collection of personal information.....	3
Indirect collection of personal information.....	4
Purpose of collection and use of personal information.....	5
Storage and protection of your personal information.....	6
Disclosure of your personal information	7
Right to access and correct personal information	9
What happens if you do not provide us your information?	9
Changes to this Privacy Policy.....	9
Privacy Policy queries and concerns.....	10

Purpose

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 (i.e. our website, or social media pages) about how we comply with the requirements of the New Zealand Privacy Act 2020 ("the Privacy Act") in managing personal information.

Consent to Privacy Policy

Please note that when you contact us through our website, or social media pages, you are agreeing to this Privacy Policy. If you do not agree with this Privacy Policy, please do not contact us through any of our digital platforms but call our offices using the phone numbers on the [Team Page](#).

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. Where reasonable and practicable, we will collect your personal information directly from you and inform you that we are collecting it, some examples of when we will collect information:

- over the telephone or a video call (such as Microsoft Teams, Google Meet, Zoom) e.g. when you contact our staff;
- through one of our digital platforms like our website or social media pages;
- through one of our online forms;
- when you phone, email, or write to us; 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)
- 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 other people or organisations where this is necessary for the services we provide, for related administration, for legal or regulatory compliance purposes, or for other lawful purposes connected with our business.

These sources may include:

- publicly available sources, such as public registers, websites, and other publicly available information sources;

- your professional advisers, such as your accountant, solicitor, trustee adviser, or other authorised representative;
- product providers, insurers, lenders, custodians, platforms, administrators, and other organisations connected with products or services you hold or apply for;
- identity verification providers, credit reporting agencies, and other compliance or due diligence providers;
- employers or other organisations connected with your financial affairs; and
- any other person or organisation authorised by you, or otherwise permitted or required by law.

Where reasonable and practicable, we will collect personal information directly from you. However, in some circumstances we collect personal information about you from someone else. Where we do so, we will take reasonable steps to ensure you are aware of the collection and the matters required by the Privacy Act, unless an exception applies.

We are not responsible for the privacy or security practices of third parties outside Milestone Financial, and those third parties are not covered by this Privacy Policy.

Indirect collection of personal information

In some circumstances, we collect personal information about you from someone other than you. This is known as indirect collection. We may collect personal information about you indirectly for purposes including:

- providing financial advice and related services;
- assessing eligibility or suitability for products and services;
- implementing recommendations and arranging products or services;
- administering products and services;
- verifying your identity and carrying out compliance checks;
- responding to complaints, disputes, investigations, or claims;
- preventing, detecting, or investigating fraud or other misconduct; and
- maintaining accurate records and meeting our legal and regulatory obligations.

The types of third parties we may collect your personal information from include your professional advisers, product providers, insurers, lenders, custodians, platforms, administrators, employers, identity verification providers, credit reporting agencies, publicly available sources, referrers, and other people or organisations connected with the services we provide to you or your affairs.

Where required by the Privacy Act, we will take reasonable steps to ensure you are aware:

- that we have collected your personal information;
- of the purpose for which the information has been collected;
- of the intended recipients of the information;
- of our name and address as the agency that has collected and holds the information;
- if the collection is authorised or required by law, of that law and the consequences (if any) of not providing the information; and
- that you have rights to request access to, and correction of, your personal information.

In some cases, these matters may be explained through this Privacy Policy, our engagement documents, application forms, authority forms, other privacy notices, or by another organisation notifying you on our behalf. Where another organisation notifies you on our behalf, responsibility for ensuring the notification requirements are met still remains with us as the agency collecting the information indirectly.

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-Milestone website.

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

- the date and time of visits;
- website page(s) 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(s), and the type of web browser used.

We will not ask you to supply personal information publicly over Facebook, LinkedIn, YouTube, or any other 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.

Purpose of collection and use of personal information

Any personal information we collect from you, or about you, may be used to:

- identify you and verify your identity;
- communicate with you and respond to your enquiries;
- assess your eligibility or suitability for products and services;
- provide financial advice and related services to you;
- implement recommendations and arrange, administer, review, or service products and services;
- obtain information relevant to your financial position, objectives, needs, and circumstances;
- undertake legal, regulatory, risk management, and compliance checks;
- respond to complaints, disputes, investigations, or claims;
- protect against, detect, and investigate fraud, misconduct, or other unlawful activity;
- improve our services, systems, and client experience;
- provide you with information you request; and/or
- provide you with further information about our other products and services where permitted by law.

We may also maintain, use, and disclose personal information where this is required or authorised by law, including where information must be provided to regulatory or similar bodies that have a lawful right to receive it.

We also have an obligation to maintain personal information to disclose to regulatory and similar bodies - see 'Disclosure of your personal information' section 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.

Some information we hold about you will be stored in paper files, but most of your information will be stored electronically on physical hard drives and/or on the cloud, by cloud service providers – see 'Cloud-based service providers' section 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 and monitored alarms 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;
- When we send information overseas or use service providers to process or store information, we put arrangements in place to protect your information;
- We regularly 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 policy 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. Between the Milestone Financial offices, we utilise the following cloud-based service providers:

- Microsoft Office suite including OneDrive, SharePoint, and Teams
- Drive, a file hosting service operated by Google
- Dropbox Business, a file hosting service
- Rheel Datacentre in Christchurch, for server back ups
- BasePlate, a Customer Relationship Management tool
- Solve360, a Customer Relationship Management tool
- Jotform, an online form hosting service

- MailChimp, an email marketing platform operated by Rocket Science Group
- iTEASPOON, a Google Workspace Consultant.

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 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 seven (7) years after an account has closed. 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.

We have a records management policy that governs how we manage our information and records to enable us to destroy any information that is outdated, irrelevant or no longer necessary.

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:

- Seek to quickly identify and secure the breach to prevent any further breaches and reduce the harm caused;
- Assess the nature and severity of the breach, including the type of personal information involved and the risk of harm to affected individuals;
- Advise and involve the appropriate authorities where criminal activity is suspected;
- Where appropriate, notify any individuals who are affected by the breach (where possible, directly);
- Where appropriate, put a notice on our website advising our clients of the breach;
- Notify the Privacy Commissioner (if the breach has been deemed to meet the requirements of a reportable breach); and
- Investigate our processes to prevent a breach from occurring in the future.

Disclosure of your personal information

We may disclose your personal information to others outside Milestone Financial 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.

Parties we may disclose your information to

Your personal information may be disclosed, where appropriate, to third parties including:

- product providers, insurers, lenders, custodians, platforms, administrators, and other organisations involved in the provision, arrangement, administration, review, or servicing of products and services;
- outsourced service providers and specialist advisers who assist us to provide advice and related services, including technology providers, document management providers, cloud storage providers, auditors, legal advisers, and external compliance reviewers;
- identity verification providers, credit reporting agencies, debt collecting organisations, and other compliance or due diligence providers;
- your authorised representatives and professional advisers, such as accountants, solicitors, trustees, or attorney representatives;
- our external dispute resolution scheme;
- regulators, courts, tribunals, law enforcement agencies, and other bodies where disclosure is required or authorised by law; and
- any other third party where you have authorised the disclosure or where the disclosure is otherwise permitted under the Privacy Act 2020.

If we do not need to share your personal information with a third party in order to provide advice and services to you, to administer our relationship with you, or to comply with legal obligations, we will not disclose it without your consent unless otherwise permitted or required by law.

Under no circumstances will we sell, rent, or trade your personal information, or receive payment for disclosing it.

Sending your information overseas

We may send your personal information outside New Zealand, including to overseas members of Milestone Financials' related companies and overseas service providers or other third parties who process or store our information, or provide certain services to us.

Where we do this, it does not change any of our commitments to you to safeguard your privacy. We make sure that appropriate security and information handling arrangements are in place and the information remains subject to confidentiality obligations.

All countries have different privacy laws and information protection standards. If we need to send your personal information to a country that has lower standards of information protection than in New Zealand, we will take appropriate measures to protect your personal information. Where it is not possible to ensure that appropriate security and information handling arrangements are in place, we will let you know and gain your consent prior to sending your personal information overseas.

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 the personal information we hold about you and to request correction of that information if you think it is wrong. In some circumstances, and where lawful and appropriate, you may also ask us to delete personal information we hold about you.

You can do so by contacting the office you generally deal with. Contact information can be found on our [Team Page](#). If you do not know which office you belong to, please phone 0508 964 608.

When you contact us with such a request, we will take steps to update or delete 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.

We are only able to delete your personal information to the extent that it is not required to be held by us to satisfy any legal, regulatory, or similar requirements.

There is no fee for requesting that your personal information is corrected or deleted or for us to make corrections or deletions. In processing your request for access to your personal information, a reasonable cost may be charged. This charge covers such things as locating the information and supplying it to you.

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 or delete your personal information, we will let you know our reasons, except if the law prevents us from doing so.

If we do not make a correction you have requested, you may ask us to attach a statement of correction to your personal information noting the correction sought and that you disagree with the accuracy of the information.

If we refuse your request to access, correct or delete 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 reasonably request, we may be unable to verify your identity, assess your circumstances, provide advice and related services, arrange or administer products and services for you, or comply with our legal and regulatory obligations. 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 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 03 964 6082.

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:

Milestone Financial

PO Box 79012, Avonhead, Christchurch 8446

Email: compliance@milestone.co.nz

Phone: 03 964 6082

We endeavour to acknowledge your complaint within three working days of its receipt. We will let you know if we need any further information from you to investigate your complaint.

We aim to resolve complaints as quickly as possible. We strive to resolve complaints within five working days, but some complaints take longer to resolve. If your complaint is taking longer, we will let you know what is happening and a date by which you can reasonably expect a response.

If you are not satisfied with our response to any privacy related concern you may lodge a complaint on the Office of the Privacy Commissioner website [HERE](#) or send a complaint form to the Privacy Commissioner at:

Office of the Privacy Commissioner

PO Box 10 094, Wellington 6140

Phone: 0800 803 909

Website: [Privacy Commissioner - Contact Us](#)