Purpose

This Privacy Policy explains how SurePlan Financial Limited ("SurePlan", "we", "us", "our") collects, holds, uses, discloses, stores and protects personal information in connection with our business and services. This Policy is intended to help you understand how we handle your personal information in accordance with the Privacy Act 2020, including the Information Privacy Principles. This Policy should be read together with any privacy collection statement, client engagement document, application form, website notice, or other notice we provide at the time we collect your information.

Who we are

SurePlan Financial Limited provides financial advice and related services. The personal information we collect and hold will depend on the nature of your relationship with us, the services you request, the products you apply for, and any legal or regulatory obligations that apply to us.

How this policy applies

By engaging with us, using our website or communicating with us, you acknowledge that your personal information may be collected, used, stored and disclosed in the ways described in this Privacy Policy and in any specific privacy notice we provide. In some cases, we may ask for your consent to collect, use or disclose personal information for a particular purpose. Where consent is required, we will seek it separately. If you have any questions about this Policy or how your information will be handled, please contact us using the details at the end of this Policy.

Personal Information we collect

Depending on your interactions with us and the services we provide, we may collect personal information such as:

- your name, date of birth and contact details;
- information about your enquiries, communications, preferences and subscriptions;
- details of your financial position, assets, liabilities, income, expenditure, goals, objectives, risk preferences and personal circumstances;
- information relevant to insurance, lending, investment, KiwiSaver or other financial products or services;
- identifiers and verification information required to provide services or comply with legal obligations, such as your IRD number and identity verification information;
- due diligence and source of funds information required under AML/CFT laws;
- records of meetings, advice, recommendations, consents, instructions and transactions;
- information obtained from third-party data providers and publicly available sources (where permitted by law); and
- technical and website usage information as described in the “Online device information (cookies)” section.

We will only collect personal information that is reasonably necessary for our lawful functions and activities or as otherwise permitted or required by law.

How we collect personal information

We usually collect personal information directly from you, including when you:

- contact us by phone, video call, email, post, through our website or via social media;
- complete forms, applications, fact finds, onboarding documents or consent forms;
- meet with us or communicate with our advisers or staff;
- participate in a programme, promotion, seminar or financial wellness service; or
- provide information to us through third-party platforms or file-sharing tools you choose to use.

Where we collect personal information directly from you, we will take reasonable steps to make you aware of matters required by the Privacy Act, including the purpose of collection, who may receive the information, whether the information is required, the consequences of not providing it, and your rights of access and correction.

We take extra care when collecting personal information relating to younger or potentially vulnerable individuals.

Indirect Collection of Personal Information

In some circumstances, we may collect personal information about you from third-party sources rather than directly from you. These sources may include publicly available information, referrers, employers (for workplace programmes), and third-party data providers. We take reasonable steps to ensure third-party data providers collect and supply personal information in accordance with applicable privacy laws.

Where we collect your personal information indirectly, we will take reasonable steps to notify you as soon as practicable. This will include informing you:

- that we have collected your information
- the purpose of collection
- the source of the information
- who we may share it with
- your rights to access and correct that information

We will not use your personal information in a way that is inconsistent with the purpose for which it was collected, unless permitted by law or with your consent.

Marketing Communications

We may contact individuals to inform them about our financial services where we believe the services may be relevant. This may include using information obtained from publicly available sources or reputable business data providers. We only use personal information obtained for marketing purposes for that purpose unless otherwise permitted by law.

You have the right to opt out of receiving marketing communications from us at any time. We will promptly remove your details from future marketing contact if you request this. Where you opt out of marketing, we may retain limited information to ensure we do not contact you again.

We maintain internal suppression lists to ensure individuals who opt out are not contacted again.

Online device information (cookies)

We use cookies and similar technologies to:

- enable core website functionality
- understand how our website is used (analytics)
- improve our communications and services

You can control or disable cookies through your browser settings. Where applicable, you may also manage preferences through our website cookie settings.

Further details are available in our Cookie Notice.

Third-party websites

Our website, emails or social media pages may contain links to third-party websites, applications or services. We are not responsible for the privacy, security or content practices of those third parties. We encourage you to review their privacy policies before providing personal information.

Information shared through third-party platforms

If you choose to share information with us through a third-party file-sharing platform or collaboration tool, you are responsible for managing your own account settings, security credentials and permissions for that platform. You should remove or update our access when it is no longer required. This section does not limit any obligations we may have under the Privacy Act in relation to personal information once we receive it.

Why we collect and use personal information

We collect and use personal information only where it is necessary for our business purposes, to comply with legal obligations, or where otherwise permitted by law.

We collect, use and disclose personal information for purposes connected with our lawful functions and activities, including to:

- identify you and communicate with you;
- assess your needs, objectives and suitability for services or products;
- provide financial advice and related services;
- help arrange, administer or service financial products and related matters;
- respond to enquiries and maintain our relationship with you;
- verify identity and carry out due diligence, fraud prevention and AML/CFT processes (we only collect and retain identity information necessary to meet our legal obligations under

AML/CFT legislation and take reasonable steps to avoid collecting or retaining more information than is required);
- meet legal, regulatory, audit, professional standards, licensing, dispute resolution and compliance obligations;
- maintain records, monitor service quality, train staff and manage our business operations;
- to identify and contact individuals who may benefit from our services where lawful to do so;
- send service-related communications and, where permitted, information about relevant services; and
- obtain professional advice, compliance support, technology support and audit assistance.

We will not use personal information for a purpose that is unrelated to the purpose of collection unless that use is authorised by you, permitted by law, or otherwise allowed under the Privacy Act.

Where permitted by law, we may send you information about our services. You can opt out of marketing communications at any time by clicking 'unsubscribe' or contacting us.

If you do not provide information

If you do not provide personal information we reasonably require, we may be unable to provide some or all of our services, assess suitability, process applications, verify identity, comply with legal obligations, or continue acting for you. Where we collect personal information, we will inform you whether providing the information is voluntary or required and the consequences of not providing it.

Disclosure of personal information

We may disclose personal information where this is reasonably necessary for the purpose for which it was collected, where you have authorised the disclosure, where the disclosure is required or permitted by law, or where otherwise permitted by the Privacy Act.

Depending on the circumstances, we may disclose information to:

- product providers, insurers, lenders, fund managers and other financial service providers;
- identity verification, AML/CFT, technology, messaging, document management, cloud, administrative and IT service providers;
- professional advisers, auditors, compliance consultants and external reviewers;
- regulators, government agencies, courts, tribunals, law enforcement bodies and dispute resolution schemes;
- credit reporting agencies and debt collection agencies where relevant; and
- other persons or organisations authorised by you.

We do not sell personal information.

Unique identifiers

Where we assign a unique identifier to an individual, we will do so only where reasonably necessary for our functions and activities. We will not assign an identifier that is the same as a unique identifier

assigned by another agency unless this is permitted by law or reasonably necessary for our functions. We will take reasonable steps to protect unique identifiers from misuse.

Storage, security and accuracy

We hold personal information in paper files and electronic systems, including cloud-based systems used in the ordinary course of our business.

We take reasonable safeguards to protect personal information against loss, unauthorised access, use, modification, disclosure and other misuse. These safeguards may include physical security, access controls, password protection, staff training, secure configuration, contractual protections with service providers, and policies for handling information.

We also take reasonable steps to ensure that personal information is accurate, up to date, complete, relevant and not misleading before we use or disclose it.

You can help us by letting us know if your personal information changes.

If we provide you with login credentials or passwords, you must keep them secure and notify us promptly if you suspect unauthorised access.

Cloud service providers

We use third-party service providers to help us operate our business and provide services. These may include identity verification providers, CRM providers, document collection tools, cloud storage providers, messaging providers, accounting systems and IT support providers.

Our current providers may include ApplyID, Asana, Microsoft 365 (including OneDrive), NZFSG MyCRM, Sinch MessageMedia, Xero, ActiveCampaign, FileInvite and Support-IT. The providers we use may change from time to time. We take reasonable steps to assess and manage privacy and security risks when using service providers. This may include due diligence, contractual obligations, confidentiality requirements, access controls, and provider oversight. Service providers may access personal information only to the extent reasonably necessary to perform services for us or as otherwise permitted by law.

Overseas transfers

Some of our service providers or related entities may be located outside New Zealand, or may store or process personal information overseas, including in Philippines, Australia, the United States, the United Kingdom and the European Union.

Where we disclose personal information overseas, we will take reasonable steps to ensure that the recipient is required to protect the information in a way that, overall, provides comparable safeguards to those in the New Zealand Privacy Act, or we will otherwise ensure the disclosure is permitted by the Privacy Act. These steps may include contractual protections, due diligence, or reliance on a legal regime recognised as providing comparable safeguards. If comparable safeguards

are not available and another permitted basis does not apply, we will inform you and seek your express authorisation before making the disclosure.

Personal information may be stored or processed in jurisdictions such as Australia, the United States, or the United Kingdom/European Union.

Where information is transferred overseas, we take reasonable steps to ensure that it is protected by safeguards comparable to New Zealand privacy law, including contractual protections with our service providers.

Retention

We retain personal information only for as long as it is reasonably required for the purpose for which it was collected, and for any longer period required or permitted by law.

Different types of information may be retained for different periods, depending on legal, regulatory, audit, complaints, dispute resolution, tax, AML/CFT, limitation, record-keeping and business requirements. As a provider of financial advice and related services, we may retain records needed to demonstrate the services provided, the basis of advice, compliance activity, and related client communications.

We maintain records management and retention practices designed to ensure that information is securely destroyed, deleted or de-identified when it is no longer required.

Your privacy rights

You may request access to personal information we hold about you and request correction of that information. In some circumstances, you may also request that information be deleted or no longer used, for example where the information is no longer required or where correction reasonably requires deletion. However, we may need to retain information to comply with legal, regulatory, contractual, record-keeping or dispute resolution obligations. We may need to verify your identity before responding to your request. We will respond to requests in accordance with the Privacy Act. We generally do not charge for correction requests. If we propose to charge for an access request, any charge will be reasonable and permitted by law, and we will tell you in advance. If we refuse a request, we will explain why unless the law prevents us from doing so, and we will tell you how you can make a complaint.

Privacy breaches

If a privacy breach occurs, we will take steps to contain it, assess it, and respond appropriately.

In assessing whether a breach is likely to cause serious harm, we consider the factors set out in section 113 of the Privacy Act.

Where notification is required, we will notify the Office of the Privacy Commissioner and affected individuals as soon as practicable.

We require relevant service providers to notify us promptly of actual or suspected privacy incidents affecting information they handle for us.

Contact us and complaints

If you have a question, concern, access request, correction request or privacy complaint, please contact us using the details below:

Postal: PO Box 8096, Newmarket, Auckland 1149, New Zealand

Email: info@sureplanfinancial.co.nz

Phone: +64 9 551 9070

We encourage you to contact us first so we can resolve your concerns. If you are not satisfied, you may contact the Office of the Privacy Commissioner.

You may raise a privacy concern or complaint with us by phone, email, post, or through your adviser or another member of our team. We aim to acknowledge privacy complaints within three working days and to investigate and respond as promptly as reasonably practicable. If you are not satisfied with our response, you may make a complaint to the Office of the Privacy Commissioner.

Access and Correction Requests

You may request access to, or correction of, your personal information at any time.

We will respond to your request within 20 working days, in accordance with the Privacy Act.

We may require verification of your identity before actioning your request.

Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements or services. The current version will be available on our website or on request. Where changes are material, we may also notify you directly.