1. Privacy Policy

Introduction

The New Zealand Privacy Act 2020 (**the Act**) applies to how companies deal with personal information. Personal information is information about an identifiable individual (a natural person).

This Privacy Policy sets out how Welcome collects, uses, maintains, and discloses personal information we collect and hold about our investors and borrowers (clients), prospective clients, prospective employees etc.

It also covers visitors to our website and other applications including our mobile and social media applications and any other digital property operated by us.

This policy does not limit or exclude any individual's rights under the Act.

Policy Statement

Welcome acquires 'Personal Information' for the purposes of improving and personalising our services to clients, for the purposes of complying with its Reporting Entity obligations under the Anti-Money Laundering and Countering of Financial Terrorism Act 2009, and other regulatory or compliance obligations.

The Privacy Officer will be the Compliance Officer.

All staff, contractors and associated persons must comply with the Act, including the requirements set out in this Policy.

Key Processes

The information that Welcome collects

"Personal Information" refers to all and any information relating to a client, including, the client's name, date of birth, contact numbers, email address, mailing address, copies of identity documents, bank statements, bank deposit slips etc.

In the case of prospective employees, personal information can include (but is not limited to) occupation, employment history and/or details, education and qualifications, testimonials, and feedback.

Welcome may also obtain personal information from publicly available resources such as the Companies Office, LinkedIn, government agencies etc. Where possible, we should collect personal information from the person directly.

Consent to Use of Personal Information

Welcome must obtain the consent of all clients as part of its application process.

If the client is referred by an external party using their own application form (such as a broker), the application form should be checked to ensure that it contains the necessary Privacy consents to enable Welcome to hold, use and share the client information as it is legally required to do in order to provide its services.

How we collect personal information

We will collect personal information:

- Directly when the client provides their details to us; and
- Indirectly through emails, forms, subscription applications, face-to-face meetings, interviews, business cards, telephone conversations and through the use of the services and facilities available through our websites and social media channels.

How we use personal information

Examples of how we may use personal information:

- Review investor eligibility status and to process applications to become an investor.
- To assess a borrowers eligibility for a loan.
- Manage our client records including transfers, deposits, payments, generating reports etc.
- Check a client's identity against governmental databases to complete aml/cft electronic verifications.
- Measure the interest in our products and website.
- Keep clients informed, including inviting clients to attend marketing seminars. Thereafter a client will receive this information unless they ask us not to provide them with this information (opt out).
- Better understand a client's interests and preferences so we can provide them with an improved online experience and to improve our products and website.
- Identify and market the products, promotions, offers or information that we think may be of interest and to measure the effectiveness of and improve the relevance of internet advertising and promotional emails.
- Conduct market, product, or sales research. Data processing and aggregated statistical data analysis, and business improvement analysis.

Disclosing personal information

We may disclose a client's personal information to:

- Another company within our group or a related party or service provider such as TUMU.
- Any business that supports our services and products, including any person that hosts or maintains any underlying IT system or data centre that we use to provide the website or other services and products
- A person who can require us to supply client's personal information (e.g., Supervisor, RBNZ or other regulatory authority)
- Any other person authorised by the Act or another law (e.g., a law enforcement agency)
- Any other person if authorised to do so by the client.

Welcome plans to use cloud based computing products including our loan administration system. This may mean client's personal information is held and processed outside New Zealand.

Protecting personal information

Welcome must take reasonable steps to keep client's personal information safe from loss, unauthorised activity, or other misuse.

This will include taking measures to keep personal data secure on our Website and any associated computer-systems and to prevent acquisition or misuse of personal information by unauthorised persons.

Welcome protects personal information by:

- Limiting physical access to client files by anyone other than approved employees, service providers and third parties.
- Implementing cyber security measures, policies and employee training on privacy and cyber security.
- Ensuring that personal information is destroyed in accordance with our Record Keeping and Destruction Policy.

Accessing and correcting personal information

Subject to certain grounds for refusal set out in the Act, clients have the right to access readily retrievable personal information that we hold and to request a correction to that personal information.

Before a client exercises this right, we will need evidence to confirm that the client is the individual to whom the personal information relates.

In respect of a request for correction, if we think the correction is reasonable and we are reasonably able to change the personal information, we will make the correction. If we do not make the correction, we will note in our records system that the client requested the correction.

Remember that any information noted about the client, particularly a vulnerable client, should not be offensive for the client when they read it. However, it is acceptable to make factual statements such as ways to provide extra assistance to a vulnerable client.

Internet Use

While we will take active steps to maintain secure internet connections, if a client provides us with personal information over the internet, the provision of that information is at their own risk.

If a client follows a link on our website to another site, the owner of that site will have its own privacy policy relating to personal information. We should suggest that clients review that site's privacy policy before providing further personal information.

Website Privacy Information

Our website will contain a Privacy Policy or statement to explain how information collected from the website will be held, used and stored.

Cookies

We may use cookies (an alphanumeric identifier that recognises a client's browser) to monitor use of our website. A client may disable cookies by changing the settings on their browser, although this may mean that a client cannot use all of the features of the website.

Contacting us

If a client has any questions about this privacy policy, our privacy practices, or if a client would like to request access to, or correction of, personal information, they may contact our Privacy Officer. Details of how to contact us will be on our website.

Privacy Breach Notification

What is a privacy breach?

A privacy breach occurs when Welcome either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information.
- Discloses, alters, loses or destroys someone's personal information.
- A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

Reporting the breach

The standard process to investigate, record and report a breach should be followed. See our Material Issues and Breaches Policy.

Under the Act, if Welcome has a privacy breach that either has caused or is likely to cause anyone serious harm, we must notify the Privacy Commissioner and any affected people as soon as we are practically able. The breach notification should be made within 72 hours. The Office of the Privacy Commissioner has a tool to test whether the breach should be reported to them.

Our Supervisor should also be notified of material breaches or near misses.

What is serious harm?

The unwanted sharing, exposure or loss of access to people's personal information may cause individuals or groups serious harm. Some information is more sensitive than others and therefore more likely to cause people serious harm.

Examples of serious harm include:

- Physical harm or intimidation
- Financial fraud including unauthorised credit card transactions or credit fraud
- Family violence
- Psychological, or emotional harm

Controls

Key Controls	How Implemented	Testing
Public statement of our Privacy Policy	Privacy information on the website [www.Welcome.co.nz]	Control testing six monthly.
Request for client data by a third party	To be referred to management for a decision.	
Client request for personal information	Identity to be verified through at least two factors.	
Client request to change personal information	By written communication (email)	

References

Privacy Act 2020	https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html
Office of the Privacy Commissioner	https://www.privacy.org.nz/

Approval

Business Owner:	CEO
Authorised by:	Board
Date:	August 2024
Document Name:	Privacy Policy

Version Control

Version	Date	Author	Description
0.1	28/02/2024	A Douglas with the assistance of RCL	Draft policy
1.0	Aug 2024	Board	Reviewed and subsequent changes made. Approved