Customer Information and Privacy Policy

Why is this policy important?

Establishing and maintaining a trust-based relationship with our customers is central to our effectiveness as an adviser. Maintaining confidentiality as regards customer information is fundamental to that trust.

Customer information includes all information about the customer that is collected or held by a person who gives Financial Advice. That includes information in work papers and records, and the Financial Advice given to the customer. This includes personal information under the Privacy Act (which is information about an identifiable individual) but is broader as it also includes information relating to entities.

Standard 5 of the Code of Professional Conduct for Financial Advice Services (the Code) sets out clear requirements regarding the handling of customer information. Customer information is broader than personal information under the Privacy Act to the extent that it relates to personal information, however the standard is intended to be applied consistently with obligations under the Privacy Act.

This policy sets out our approach to dealing with customer information. The policy should be read in conjunction with the Information Security Policy.

Our policy

We do this:

- Ensure that customer information is only used, retained, or disclosed:
    - for the purpose of giving Financial Advice to the customer;
    - for another purpose, that is directly related to giving the Financial Advice;
    - if the use, retention, or disclosure is required or permitted by law; and
    - for another purpose, if the Customer has agreed.
- Inform customers how their information will be collected, used, retained, or disclosed by providing a privacy notice.
- Ensure that customer information is retained only for as long as it is required for one or more of the above reasons (consistent with our record-keeping policy).
- Allow customers to access and correct their personal information unless an exception under the Privacy Act applies.
- Ensure that when the customer information is no longer needed, it is returned to the customer or disposed of securely in accordance with our [Data Retention schedule, Record Keeping Policy, and Information Security Policy].
- Appoint a Privacy Officer who understands their responsibilities under the Privacy Act.
- Regularly train our people so they understand what we need to do to ensure compliance with privacy laws, spot, and report privacy breaches, and manage privacy requests and corrections.

- Ensure that physical and electronic security measures and protocols are maintained so that only authorised personnel of our FAP have access to customer information.
- If a privacy breach occurs that is likely to cause harm, we inform the individual and the Office of the Privacy Commissioner as soon as reasonable. If this is a material information security breach, we also notify the FMA.
- Obtain consent from Customers for their information to be provided to regulatory bodies should it be required for supervisory purposes.
- Obtain consent before sending any electronic marketing messages and provide an unsubscribe mechanism.
- When outsourcing and personal information is transferred offshore, we have contractual protections in place to provide the same protections under the NZ Privacy Act.

We don't do this:

- Leave customer documents in an unsecure environment.
- Use customer information for any purpose other than that for which it was provided to us.
- Breach customer confidentiality by disclosing, verbally or in writing, customer information to third parties without Customer consent.
- Breach the information security protocols we have in place restricting who has access to customer information, be it in physical or electronic form.
- Hold customer information for longer than is required for the purposes of the relationship and/or meeting legal requirements.

Implementation

All advisers and employees receive induction and annual retraining on the contents of this policy.

Formal customer consent to provision and use of information on file.

IT security and information access protocols in place.

Secure document storage and destruction facilities in place.

Ensuring compliance

Ongoing monitoring of adviser and employee activity and behaviour.

Yearly adviser and employee attestations to policy adherence.

Review and audit of Customer files annually

Yearly review of IT access protocols.

How to make a complaint

If you wish to make a complaint about a breach of this Privacy Policy or any breach of applicable privacy laws, you can contact us using the contact details below. You will need to provide us with sufficient details regarding your complaint together with any supporting evidence and information. You can also complain to the Privacy Commissioner
(see www.privacy.org.nz).

How to contact us

If you wish to gain access to your personal information, want us to correct or update it, have a complaint about a breach of your privacy or any other query relating to our Privacy Policy, please contact us at privacy@cis.co.nz

Updates of Privacy Policy

We reserve the right to amend our Privacy Policy from time to time to ensure we properly manage and process your personal data.