Financial Advice Hawkes Bay -Privacy Policy

Introduction

When a client uses our services, they are trusting FAHB with their personal and financial information. We understand that this is a big responsibility and work diligently to protect their information in accordance with the Privacy Act 2020 (the Act).

Policy Statement

A key aspect of our business is obtaining and storing client information and other types of data. If we use service providers who are based overseas (for example, cloud software where servers are based in another country) we need to ensure that the provider meets the New Zealand privacy laws at all times.

We must also ensure that personal client information is held in a safe and secure way and disposed of securely when we have finished with it and/ or are no longer required to hold it.

We follow The Privacy Act's thirteen principles when collecting, using, and storing client's personal information:

Principle 1	Personal information must only be collected when: • The collection is for a lawful purpose, connected with what FAHB does; and • It is necessary to collect the information for that purpose.
Principle 2	Personal information must usually be collected from the person that the information is about. In some instances, however, it will be appropriate to collect information from other people instead. For instance, when: • Getting it from the person concerned would undermine the purpose of the collection • It is necessary for a public sector body to uphold or enforce the law • The person concerned authorises collection from someone else.
Principle 3	When we collect personal information from the person the information is about, we must take reasonable steps to ensure that the person is aware of the following: • Why the information is being collected • Who will get the information • Whether the person has to give the information or whether it is strictly voluntary • What will happen if the information is not provided. Sometimes there are good reasons for not letting a person know about the collection (e.g. if it would undermine the purpose of the collection or it is just not possible to inform the person).
Principle 4	Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.
Principle 5	While it is impossible to stop all mistakes from happening, we must nevertheless ensure that there are reasonable safeguards in place to prevent loss, misuse, or disclosure of personal information.
Principle 6	In general, people have a right to ask for access to personal information that identifies them. However, there are situations where we can refuse to give access to information because doing so would: • Endanger a person's safety • Prevent detection and investigation of criminal offences • Involve an unwarranted breach of someone else's privacy.
Principle 7	People have a right to ask us to correct information about themselves if they think it is incorrect. We are generally not obligated to change the information we hold, but people can request that we include in our records their views about what the correct information is.
Principle 8	Before we use or discloses personal information, we must take reasonable steps to check that the information is accurate, complete, relevant, up to date and not misleading.

Principle 9	We must not keep information for longer than is necessary for the purposes for which the information may be lawfully used.
Principle 10	We must use personal information only for the purpose for which it has been collected. Other uses are occasionally permitted, such as when it is necessary to enforce the law or the use is directly related to the purpose for which the agency obtained the information.
Principle 11	We can only disclose personal information in limited circumstances, such as where another law requires us to disclose the information. We can also disclose information if we reasonably believe that: • Disclosure is one of the purposes for which we got the information • Disclosure is necessary to uphold or enforce the law • Disclosure is necessary for court proceedings • The person concerned authorised the disclosure • The information is going to be used in a form that does not identify the person concerned.
Principle 12	Where disclosure of personal information happens outside of New Zealand (i.e. where the third-party provider is based overseas), we must confirm that the provider meets the New Zealand privacy and data laws *before* entering into a business relationship with them. If they do not meet our criteria, we cannot allow them to hold our data.
Principle 13	FAHB cannot use the unique identifier given to a person by another business. For example, some businesses or agencies give people a 'unique identifier' instead of using their name (e.g. a driver's licence number, a student ID number, an IRD number, etc.). People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up or is directly related to those purposes.

Privacy Officer

FAHB has appointed Michael Gallagher as the company Privacy Officer. The Privacy Officer must have a general understanding of the Act and can deal with privacy issues when they arise. Any breaches or 'near misses' should be reported to the Privacy Officer as soon as possible.

Privacy Breaches

Privacy breaches are a reality for any business that holds personal information. Businesses and organisations can inadvertently release personal information through employee complacency, inadequate security measures, poor procedures or by accident. If a privacy breach happens, it must be carefully managed and resolved.

FAHB must report any serious privacy breaches to the Office of the Privacy Commissioner. A serious breach is one that poses a risk of harm (e.g., leaked personal information is published online or used to facilitate identity theft). Where a serious breach occurs, we must also notify the people whose information was affected.

Breach notifications to the Office of the Privacy Commissioner can be made by email, telephone or by using their online enquiry form: https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/

Key Processes

- We will only collect information that is directly relevant to our business relationship with our clients
- The primary source of information will be from the client directly. Where we use other sources, we must inform the client of those sources before proceeding

- We will not share, sell, or trade personal information to any other company or person. We may contact clients from time to time for relationship management purposes or to advise of other services
- We will use all reasonable endeavours to ensure that personal information is kept secure and confidential
- Only authorised staff will have access to personal information
- Client information is safely disposed of.
- We ensure that our IT network is secure
- If we are considering engaging an overseas-based service provider (e.g., cloud storage services), we must ensure that the provider meets all New Zealand privacy laws.

Breach Process

These are four key steps in dealing with a Privacy Breach:

1. Contain
2. Assess
3. Notify
4. Prevent

Further information can be found at https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/responding-to-privacy-breaches/)

Controls

Key Controls	How Implemented	Responsibility and Frequency
Client Records Security Checks	Client files to be checked to confirm that they have been stored securely and not easily accessed by unauthorised personal.	Compliance Officer - Annually.
Staff training on the Privacy Act 2021	Annual staff training using information from the Privacy Commission website.	Compliance Officer – Annually.
Breach Register	Any breaches or near misses are recorded in the breach register and reported to the Privacy Commissioner if they are serious.	Compliance Officer – as required.
Privacy Statements	We include a privacy statement on our website and in our client documents, so clients know we take their privacy seriously. The privacy statements are periodically reviewed to ensure they are accurate and current.	Compliance Officer – Annually.

Related Policies
IT Systems and Security Policy

References

Privacy Act 2020	http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
Office of the Privacy Commissioner	https://www.privacy.org.nz/
Code of Professional Conduct - Standard 5	Protect Client Information.