1. **Privacy Policy**

Introduction

When a client use's our services, they are trusting Financial Services Auckland Ltd (FSA) with their personal and financial information. We understand this is a big responsibility and work hard to protect their information as per the Privacy Act 2020.

Policy Statement

A key aspect of our business is obtaining and storing client information and other types of data. We don't currently use overseas based service providers, but If we were to 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 FSA does, and • it's necessary to collect the information for that purpose.
Principle 2	Personal information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead - for instance, when: • getting it from the person concerned would undermine the purpose of the collection • it's necessary so a public sector body can 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, it must take reasonable steps to make sure that person knows things like: • why the information is being collected • who will get the information? • whether the person has to give the information or whether this is voluntary • what will happen if the information isn't provided. • their rights of access to and correction of information Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it's 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	It's impossible to stop all mistakes. But we must ensure that there are reasonable safeguards in place to prevent loss, misuse, or disclosure of personal information.
Principle 6	People are entitled to receive from FSA upon request • confirmation of whether FSA holds any personal information about them: and • Access to their personal information If a person is given access to personal information, they must be advised that under principle 7 they may request the correction of that information 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. FSA has a legal duty to respond to requests for access to information or correction of information within 20 working days of receiving the request.
Principle 7	People have a right to ask us to correct information about themselves, if they think it is wrong. • FSA must on request take reasonable steps to ensure the information is accurate, up to date, complete and not misleading • When people are requesting the correction of personal information, they are entitled to provide a statement of correction and request it is added to file • FSA must take all reasonable and practical steps to inform every other person that information has been disclosed to that there has been a change
Principle 8	Before we use or discloses personal information, we must take reasonable steps to check that 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 (for example because this is necessary to enforce the law, or the use is directly related to the purpose for which the agency got 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	FSA 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

FSA has appointed the Compliance Officer, Andrea Beuvink, 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.

FSA 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

- FSA collects personal information from,
  - Employees / Prospective Employees
  - Contractors,
  - Authorised bodies
  - Outsource providers
  - Clients and prospective clients
- 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.
- We only keep personal information for as long as it is necessary (refer record Keeping policy)
- Client information is safely disposed of.
- We ensure that our IT network is secure.
- We take all reasonable steps to ensure information is protected when working remotely
- 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.
- Any requests for access to information must be referred to the Privacy / Compliance Officer
- We record breaches on the Breaches register

Breach process

These are four key steps in dealing with a privacy breach:

1. Contain
   - Once you discover a privacy breach, contain it immediately and find out what went wrong
2. Assess
   - Assessing the risks of the privacy breach will help figure out our next steps
3. Notify
   - We will be open and transparent with people about how we are handling their personal information
4. Prevent
   - The most effective way to prevent future breaches is through our security plan for all personal information

Further information about the four steps, follow https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/responding-to-privacy-breaches/)

If we are unsure if a breach is notifiable we can refer to the commissions website https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/