

**HR Policy:**                   **Privacy (Client)**

**HR Stream:**               **Inspiring a Committed Workforce**  
**Policy Grouping:**       **Safe, Healthy and Inclusive Environment**  
**Area of Application:** **All Business Units of the Tribe Group**

## **Summary**

It is the policy of the Tribe Group to protect an individual’s right to privacy and to maintain full compliance with our obligations under the Privacy Act (1988), as amended by the Privacy Amendment - Enhancing Privacy Protection Act (2012).

In particular, the Tribe Group will comply with the National Privacy Principles contained in the Act.

The Tribe Group’s values underpinning this policy are ‘respect’ and ‘partnership’.

## **Practical Advice and Processes**

The Tribe Group collects and handles personal information about businesses and individuals (client companies, employees of companies, individuals) during the course of its business operations.

Personal information is defined as any information (solicited or unsolicited) or an opinion (whether true or not) about a person. It may range from sensitive (e.g. medical history or condition) to the everyday (e.g. address or phone number). It also includes the opinions regarding work performance of an individual, work history and experience, investments, financial decisions, illness results, and other information regarding an individual. Personal information includes *sensitive* information.

Sensitive information is considered a special category of personal information. It is information (solicited or unsolicited) or opinion regarding issues such as: racial or ethnic origin; political opinion; professional or political affiliation; sexual preference; health information; religious beliefs; and criminal record.

There are 13 Australian Privacy Principles (APP’s) outlined in the *Privacy Amendment (Enhancing Privacy protection ACT 2012)*. These Principles guide privacy compliance.



These principles are:

**APP 1 - Open and Transparent Management of Personal Information**

Ensure that Tribe Group Manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

**APP 2 - Anonymity and Pseudonymity**

Requires Tribe Group to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

**APP 3 - Collection of solicited (a request where there has been an active step taken) Personal information.**

Outlines when Tribe Group can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information

Tribe group can only collect sensitive information if the individual consents (limited exemption applies)

Tribe group must collect by lawful and fair means

**APP 4 - Dealing with unsolicited personal information**

Tribe Group must (within a reasonable period after receiving the information) determine whether or not the entity could have collected the information under APP 3 if Tribe group had solicited the information.

If not, and the information is not contained in a Commonwealth record, Tribe Group must as soon as practicable to destroy the information or ensure that the information is de-identified.

**APP 5 - Notification of the collection of personal information**

Act or before the timing of (soon as practicable) Tribe Group collects personal information Tribe group must take such steps to

- Notify the individual
- Or otherwise ensure that the individual is aware

**APP 6 - Use or disclosure of personal information**

If Tribe Group holds personal information that was collected for a particular purpose (the primary purpose) Tribe group must not use or disclose the information for another purposes (secondary purpose) unless;

- The individual consents
- The individual would reasonably expect Tribe Group to use or disclose the information for the secondary purpose and the secondary purpose is:- if sensitive – directly related, if no sensitive – related to the primary purpose



- Required by law; permitted general situation exists; permitted health situation exists; Tribe Group reasonably expects information is necessary for enforcement body.
- If none of the above Tribe Group must take steps (reasonable) to de-identify the information.

#### **APP 7 - Direct marketing**

Tribe Group may only use or disclose personal information for direct marketing purposes if certain conditions are met and only if the individual (limited exemption apply).

#### **APP 8 - Cross-border disclosures of Personal information**

Before Tribe group Discloses personal information to an overseas recipient Tribe Group must take reasonable steps to ensure that the overseas recipient does not breach APP in relation to that information.

#### **APP 9 - Adoption, use or disclosure of Government related identifiers.**

Tribe Group may not adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

#### **APP 10- Quality of Personal information**

Tribe Group must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. Tribe Group must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.

#### **APP 11 - Security of Personal information**

Tribe Group must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure.

#### **APP 12 - Access to personal information**

When an individual requests to be given access to personal information Tribe Group is obligated to provide access. This includes a requirement to provide access unless a specific exception applies.

Tribe Group must respond to a request within a reasonable period.

#### **APP 13 - Correction of Personal information**

Tribe Group has an obligation in relation to correcting the personal information it holds about individuals.



During the course of accounting and financial services personal information is collected in a variety of ways. Information may be collected during interviews, through collection of financial data, through the completion of surveys or questionnaires, during training programs, through discussions with accountants, while providing financial advice or through other forms of communications.

If an individual does not disclose information that the Tribe Group is seeking through the course of its business, we may be limited in our ability to complete the work we have undertaken to deliver to the client.

Personal and sensitive information is often analysed by the Tribe Group to fulfill delivery of services to clients. Information is to be used solely for the purpose it was collected. In some circumstances, personal information may, as required, be accessed, transferred or handled by contractors of the Tribe Group. This would only occur if necessary, during the course of completing our business commitments to clients and with your consent.

The Tribe Group is compliant with its legal and ethical obligations of confidentiality, which apply to its clients and employees. It is expressly forbidden to attempt to sell or “rent” any personal information collected by the Tribe Group regarding individuals.

Personal information collected and used by the Tribe Group is usually stored either in hard copy or electronically. The Tribe Group has security procedures in place to ensure the protection of relevant information. If you are unsure about these measures, and their use, please contact to your Team Leader or the Admin Team immediately.

An individual from whom the Tribe Group has collected information has the right to see and have a copy of the information that is held (subject to some exceptions under Australian Privacy Principle 12 – Access to personal information).

If the individual is able to establish that personal information that is held is not accurate, complete and up-to-date, the Tribe Group is obliged to take reasonable steps to correct the information. (Australian Privacy policy 13)

The Tribe Group has a Privacy Officer appointed to handle any concerns, questions and to resolve any privacy related grievances. Please contact the Admin Team for more information and contact details.

### *Role of Managers*

- Managers are responsible for ensuring that all employees are aware of the Privacy Act and the Tribe Group’s obligations to clients and other individuals regarding this Act,
- All managers must actively maintain the security processes in place for personal information.

### *Role of Employees*

- All employees of the Tribe Group must be aware of what constitutes personal and sensitive information as defined in the Privacy Act and explained in this policy
- Employees should actively undertake to utilise security processes in place to protect the privacy of the individual's from whom information has been collected by the Tribe Group

### **More Information**

- Financial Adviser Standards and Ethics Authority Limited (FASEA) Code of Ethics
- Business and Professional Standards
- Tribe Group Values
- Privacy (Employee)
- Code of Conduct for Tax (financial) adviser

### **Policy History**

Date of Issue:

Approved by:

Update History:

<b>Date</b>	<b>Details</b>	<b>Contact Person</b>