PARTNERS SMSF ADVICE

# PRIVACY POLICY

The Licensee, Partners Wealth Group Advice Pty Ltd, has developed a privacy policy and privacy collection statement for this business. The statement must be given to the client at the time the FSG is provided and the policy made available to the client if requested by the client. It is important information and must be treated as such.

## Privacy procedures

The Privacy Act 1988 (Cth), the Australian Privacy Principles protect personal information which belongs to individuals by placing restrictions on how that information may be collected, handled, used and disclosed. Almost all individuals, companies, partnerships, unincorporated associations and trusts who collect and use personal information are bound by the main requirements of the privacy laws, ie the Australian Privacy Principles.

The Licensee has the following Privacy Policy procedures which must be followed when collecting and using information. Consult the Privacy Officer if there are any concerns or questions.

## Personal information

### What is personal information?

**Personal information** is information or an opinion about an identified individual or an individual who is reasonably identifiable. It does not matter whether it is true or whether it is oral or in writing.

In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, employer/place of work, salary and employment details, business activities, investments, and assets and liabilities, or any combination of these.

**Sensitive personal information** is information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, trade or professional association or a trade union, religious or philosophical beliefs or affiliations, sexual preferences, criminal record or health information (including biometric and genetic information).

### Open and transparent management of personal information

**Personal information must be managed in an open and transparent way. This requires businesses to:**

- Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle any enquires or complaints about privacy
- Have a clear and up to date Privacy Policy that documents the way the Licensee manages personal information, including:
  - the kind of information collected

- how this is collected it and for what purpose
- how people can access and correct their information
- how people can make a privacy related complaint
- whether the Licensee or Representative is likely to disclose information to overseas recipients and if so, where they will be located.

# Collection and use of personal information

Personal information must only be collected if it is necessary for the functions and services provided by Representatives and must be collected by lawful and fair means and not in an unreasonably obtrusive way. It should only be collected from the person to whom it relates unless it is unreasonable or impracticable to do so.

**When Representatives collect personal information, the Representative must tell the person from whom they collect it the following things:**

- who they are and how they can be contacted
- why they are collecting the information and to whom they usually provide it
- any law that requires the information to be collected
- what will happen if the information is not provided to them
- the fact that the individual(s) can gain access to the information, correct it or complain about a breach of the Australian Privacy Principles and that the details of how to do this and how the Licensee will deal with the complaint are in the Licensee's Privacy Policy
- whether the information is likely to be disclosed to someone overseas and if so, the countries in which they are likely to be located.

Representatives can do this by telling the person this information or providing them with the FSG which incorporates a Privacy Collection Statement.

- Signed Privacy Consent forms should be obtained from clients during the Fact Find.
- Showing concern for the confidentiality of the client's information is a good way to create trust.
- Reassure clients that they can obtain access to their information at any time if they want to check or update it.
- Do not collect sensitive information from a client unless they have consented to providing this. If in doubt, consult the Privacy Officer.

# Collection from third parties

If the Licensee or Representatives need to collect information from someone other than the person to whom it relates, ensure that the person that the information is about is aware of the above matters and the fact that their information has been collected, when and how this was done, and who provided the information. Do this by providing a copy of the Privacy Policy.

### Sensitive information

Always obtain consent when collecting or disclosing sensitive information. In most cases, this will occur in the usual course of dealings. Consents can be incorporated into on application forms and in other documents used to collect this information.

**Representatives must not collect sensitive information without consent unless:**

- The collection is required by law, or
- It is reasonably necessary for one of more of the Representative's activities.

## Unsolicited information

If Representatives inadvertently receive personal information (ie it wasn't solicited or directly collected), the Representative can only retain it and use it if it is information that they would have been permitted to collect in the first place ie because it was needed the functions and services provided.

Representatives must make an assessment of unsolicited information as soon as possible after it is received. If the Representative determines they would not have collected it or it is not relevant to the services or functions provided, it must be destroyed or de-identified.

If in doubt, consult the Privacy Officer who will provide instructions on what to do with the unsolicited information.

## Use and disclosure of personal information

Personal information should only be used or disclosed for the primary purpose for which it was collected.

**It can be used or disclosed for secondary purposes, ie different purposes than the main purpose for which the information was collected where:**

- The secondary purpose is related to the primary purpose and the individual would reasonably expect the Representative to use or disclose it for the secondary purpose. (If it is sensitive information, the secondary purpose must be directly related to the primary purpose, otherwise an indirect relationship is sufficient), or
- The individual has consented to the use or disclosure, or
- The use or disclosure is required by law or by a court or tribunal order, or
- There is reason to suspect that unlawful activity has, is or may be engaged in and use the information as a necessary part of investigation of the matter or in reporting concerns to the relevant persons or authorities, or
- It is necessary for the establishment, exercise or defence of a legal or equitable claim or the purposes of a confidential alternative dispute resolution process.

**Do not:**

- Trade, rent or sell personal information or
- Provide personal information to anyone other than the organisations to whom the client has expressly or impliedly authorised it to be provided to.

It may be permissible to use or disclose information in some other unusual circumstances. If the Licensee or Representative wants to use or disclose personal information for any reason other than those described above, or are in any doubt about their obligations, legal advice should be obtained.

# Direct marketing

An individual's personal information (eg their name and contact details) can be used for direct marketing if:

- they would reasonably expect this
- their personal information was collected from them
- there is a simple means provided for them to request not to receive any more direct marketing communications.

If a person would not reasonably expect to be sent direct marketing communications, or their personal information was collected from someone other than them, it must not be used for direct marketing unless:

- they consent to receiving direct marketing communications, or it is impracticable to obtain their consent
- there is a simple means provided for them to request not to receive any more direct marketing communications
- each direct marketing communication, if in writing contains a prominent statement, or if by telephone makes them aware that they can request not to receive such communications in the future.

Do not assume that clients expect to be sent direct marketing communications. The test is whether a reasonable person would expect this.

**Consider whether:**

- they have consented, or
- the Privacy Policy explains that this will be done or
- they were notified in the Privacy Collection Statement that one of the purposes of collection of their information was for direct marketing purposes.

**Opting Out** – Include a simple means for clients to opt out of receiving marketing material in all direct marketing communications, ie:

- A clear instruction on what to do
- A quick and simple process that uses the same communication channel used to deliver a direct marketing material (eg by email).

Do not charge clients to opt out and if they have opted out, ensure that their details are not used for direct marketing again.

# Overseas disclosure

If Representatives need to disclose personal information to anyone overseas, they must take reasonable steps to ensure that either they will not breach the Australian Privacy Principles or they are subject to laws which provide similar protection and can be enforced by the individuals whose personal information is being disclosed.

If Representatives disclose personal information to overseas recipients and they breach Australian privacy laws, they may be deemed to have breached the law.

**If Representatives are unsure about the laws that apply to an overseas recipient and they don't have a contractual arrangement under which they can require them to comply with the Australian privacy laws, they are required to:**

- Inform anyone about whom Representatives collect personal information, that they cannot give any assurances about how the information will be used, stored or disclosed if the Licensee discloses it overseas
- Obtain the client's express written consent before it is disclosed overseas.

Disclosure overseas is permitted in other limited circumstances including where it is required by Australian law or an Australian court or tribunal.

# Quality and security of information

**Representatives must take reasonable steps to ensure that the personal information collected, used or disclosed is:**

- Accurate, up-to-date, complete and relevant
- Kept protected from misuse, interference and loss or from unauthorised access, modification or disclosure.
- In dealings with clients, ask clients to confirm that the information held about them is correct and up to date.
- If information has become irrelevant, destroy or de-identify it.

The Privacy Officer will regularly review the Licensee's security measures, including assessing whether information that is no longer used and no longer required to comply with the law can be destroyed.

# Access and correction of personal information

**Access** – In most cases, clients are entitled to access the personal information held about them on request. If a person requests access to their personal information, Representatives must respond within a reasonable period and where possible allow access in the manner asked for (eg by sending copies of records or allowing someone to inspect them onsite).

**On receipt of a request for access:**

- check what particular information the person wants to ensure that **only** this information is provided
- confirm that the person requesting the information is who they claim to be.

**Representatives can provide the information by the most cost-effective method available. This could be:**

- letting the person inspect the information and take notes of its contents
- letting the person view the information and provide an explanation of its contents
- providing a photocopy, fax or email of the information

- providing a printout of information held in electronic form, or
- providing a summary of the information.

**Correction –** If any personal information is incorrect, incomplete, irrelevant, misleading, inaccurate or out of date or if a client requests a correction to their information, update the records to make them accurate, up to date, complete, relevant and not misleading.

If a client asks for any information to be corrected, do so within a reasonable period. Representatives cannot charge for correcting information. If the records are no longer required consider securely destroying them or de-identifying personal information contained in them.

**Timeframes – Acknowledge requests for access or correction within 7 business days. Requests should be fulfilled within a reasonable period:**

- Straightforward requests within 7-14 business days
- Complex requests within 30 business days.

Correction of information should always be actioned within 30 business days of a request. Often this will occur after a person has requested access to their information. If a client that the correction be notified to others who have received personal information (ie other companies dealt with), do so immediately unless it is impracticable or unreasonable to so do.

**Charges for Access** – Representatives must not charge anyone for lodging a request for access or correction. Representatives can, however, charge a reasonable amount for providing information following a request for access. Charges should be based on the actual cost of providing access and could include staff costs of locating and collating information, photocopy charges and the cost of having someone explain information.

**Refusing Access or Correction – Representatives may refuse to provide access to personal information in the following circumstances:**

- the request is frivolous, vexatious, ie trivial, made to pursue an unrelated grievance or is a repeated request for the same information
- provision would unreasonably impact on the privacy of others
- the information relates to existing or anticipated legal proceedings against the Representatives by the person and the information would not be discoverable in those proceedings
- provision would reveal the Representative's intentions in negotiations with the person in such a way as to prejudice the negotiations
- it is unlawful to provide access, the law permits or requires access to be denied or it would prejudice the activities of enforcement bodies.

The Privacy Officer should decide whether access should be refused.

If a Representative does not agree that the information is inaccurate, incomplete or out of date they must provide written reasons for their refusal to make change(s) and tell the client about the complaint. If requested, the Representative must also attach a statement to the information held (eg to the client file) which notes that the client believes it is out of date, incomplete, inaccurate, irrelevant or misleading.

Giving reasons – If a Representative does refuse to allow access or correction, they must explain their reasons for doing so in writing and include information about the privacy complaints process in the communication. The Privacy Officer should approve these before they are communicated to the person requesting access or correction.

# Tax File Numbers and other identifiers

Representatives can only request or collect a Tax File Number (TFN) from clients if it is necessary and relevant for the services provided and/or for a purpose which is authorised by taxation, personal assistance or superannuation law. Financial institutions will often need a client's TFN (particularly if a deposit account is opened) so Representatives may need to collect them from clients.

**When requesting a TFN, inform the client:**

- of the law which authorises it to be requested or collected
- of the purpose for which it is collected
- that declining to provide a TFN is not an offence
- of the consequences of declining to provide a TFN (eg that money will be withheld from interest and investment income).

If Representatives collect TFNs, incorporate this information into the Privacy Collection Statement.

If it is necessary to retain client TFNs, Representatives must ensure they obtain consent in writing from the client, keep the files in lockable secure areas and restrict access to tax file numbers to only the staff who need access to this information.

**Use or Disclosure** - Do not use a client's TFN or other governmental identifier for any purpose other than the legal purpose for which it was obtained. For example, do not use or disclose the number to establish or confirm the identity of a person.

It is possible to disclose identifiers in some circumstances. If Representatives want to do so, check with the Privacy Officer before doing so.

**Storage and Destruction** - If a client's TFN is collected, or incidentally appears on documents relating to an application for a loan, Representatives must:

- protect it from misuse, loss and unauthorised access
- ensure that access to the TFN is restricted to people who need to access it for the legal purpose for which it was collected.

If the Representative does not need the TFN either because they did not request it or it is no longer required by law or for the legal purpose for which it was collected, they must take reasonable steps to securely destroy or permanently de-identify it (eg with permanent white-out, black ink or similar).

Best practice client file security must be employed to protect TFN information.

# Complaints

If a complaint is received about the use of personal information, hand it to the Privacy Officer immediately.

Complaints need not be in writing. They may be presented by any reasonable means, eg letter, telephone, in person or email.

If the Licensee cannot resolve the privacy complaint, the client may escalate the complaint to the Office of the Australian Information Commissioner on www.oaic.gov.au.