

Nexus Private Financial Services Pty Ltd abides by the Australian Privacy Principles established under the Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act, 2012. Detailed below, for your information, is our policy on the management of personal information.

APP1 – Open & transparent Management of Personal Information

We are committed to manage any personal information we collect from our clients in an open and transparent way.

We collect personal information from you and about you as part of our advisory role. We do this in a variety of ways, including asking you for data about you and asking others to provide data about you (e.g. a super fund you invest in).

Any personal information we hold about you will be securely stored either in hard copy or on computer hard drive, using computer software and/or data storage facilities provided by third parties over the internet (ie not just on our computers in our offices).

Because we store some of our business data electronically and may back some or all of this data up using so-called “cloud-based” technology there is a chance that some of your personal information may be disclosed to overseas recipients in the sense that its transmission via the internet will mean it is “disclosed” to the party that operates the IT infrastructure where the data is stored. We are unable to say with complete certainty which countries this infrastructure may be located in however if this is of concern to you we are happy to investigate and to advise.

We are also happy to provide you with a copy of this Privacy Policy free of charge upon request.

If you have any call to complaint about our treatment of your personal information you can contact us or the Privacy regulator directly – they are accessible here: www.oaic.gov.au.

APP 2 - Anonymity

Although the Privacy Act makes provision for you to remain anonymous or use pseudonyms this is unlikely to occur in your dealings with Nexus Private Financial Services as we have obligations under the Corporations Act and the Anti-Money Laundering and Counter-Terrorism Financing Act to know and identify our clients before we provide advice to them or transact on their behalf.

APP 3 – Collection of Solicited Personal Information

As an Australian Financial Services Licence holder we are subject to certain legislative and regulatory requirements which necessitate us obtaining and holding detailed information which personally identifies you and/or contains information or an opinion about you (“personal information”).

In addition, our ability to provide you with a comprehensive financial planning and advice service is dependent on us obtaining certain personal information about you, including:

- a) employment details and employment history;
- b) details of your financial needs and objectives;
- c) details of your current financial circumstances, including your assets and liabilities (both actual and potential), income, expenditure, insurance cover and superannuation;
- d) details of your investment preferences and aversion or tolerance to risk;
- e) information about your employment history, employment circumstances, family commitments and social security eligibility;
- f) personal or sensitive information.

Failure to provide the personal information referred to above may expose you to higher risks in respect of the recommendations made to you and may affect the adequacy or appropriateness of advice we give to you.

We are required by the Corporations Act, the Tax Agent Services Act and the rules and standards of various professional to collect sufficient information to ensure appropriate advice can be given in respect of recommendations made to our clients. If you elect not to provide us with the personal information referred to above, we may elect to terminate our retainer with you if we believe we are unable to provide you with a complete service.

APP4 – Dealing with Unsolicited Personal Information

We will not collect any personal information about you except when you have knowingly provided that information to us or authorised a third party to provide that information to us.

If we determine that we have obtained unsolicited personal information from you (i.e. information we don't actually need in order to deliver our services to you) we will contact you and return it or otherwise remove it from our records as soon as is practicable.

APP 5- Notification of the Collection of Personal Information

Generally collection of your personal information will be effected in either face to face interviews, or over the telephone or internet. From time to time additional and/or updated personal information may be collected through one or more of those methods.

Where we collect information about you other than directly from you we will advise you of this fact and provide any other information to you about that collection as is determined relevant in the circumstances and in light of sub-clauses 5.1 and 5.2 of the APPs.

APP 6 – Use or Disclosure of Personal Information

We will not use or disclose Personal Information collected by us for any purpose other than:

- a) the purposes for which it was provided or secondary related purposes in circumstances where you would reasonably expect such use or disclosure as detailed below; or
- b) in the event that we propose to sell our business we may disclose your personal information to potential purchasers for the purpose of them conducting due diligence investigations. Any such disclosure will be made in confidence and it will be a condition of that disclosure that no personal information will be used or disclosed by them. In the event that a sale of our business is effected, we may transfer your personal information to the purchaser of the business. As a client you will be advised of any such transfer; or
- c) where you have consented to such disclosure; or
- d) where the Australian Privacy Principles authorise use or disclosure where required or authorised under law, in circumstances relating to public health and safety and in connection with certain operations by or on behalf of an enforcement body.

We may disclose your Personal Information to superannuation fund trustees, insurance providers, and product issuers for the purpose of giving effect to your financial plan and the recommendations made by us.

We may record and store your Personal Information on computer software and/or data storage facilities provided by third parties over the internet (ie not on our computers in our offices).

In order to ensure that you receive a personal and tailored service, your Personal Information may be transferred to one of our agents or authorised representatives who will be your primary point of contact with the organisation. It is a condition of our agreement with each of our representatives that they adopt and adhere to this privacy policy. You can be assured that your information will be maintained by any agent or representative in accordance with this policy. If you have any concerns in this regard, you should contact us by any of the methods detailed below.

If we disclose your personal information to external contractors we make it a condition of our agreement with each of our external contractors that they adopt and adhere to this privacy policy. You can be assured that your information will be maintained by any contractor to whom it is disclosed in accordance with this policy. If you have any concerns in this regard, you should contact us by any of the methods detailed below.

APP 7 – Direct Marketing

We may use the personal information collected from you for the purpose of providing you with direct marketing material such as articles that may be of interest to you, however you may, by contacting us by any of the methods detailed below, request not to receive such information and we will give effect to that request. Please allow 2 weeks for your request to be actioned.

APP 8 – Cross-Border Disclosure of Personal Information

The only overseas recipient of your personal information we can currently imagine is the party that hosts any IT infrastructure that we back up our business data to – e.g. via the so-called “cloud”. We will seek confirmation from any such service provider that they will treat your data securely and in alignment with the APPs. If we form the view that they are not able to treat client personal information in this way we will seek an alternative service provider.

Although it is highly unlikely, we may transfer personal information about clients to someone (other than ourselves or the client) who is in a foreign country only if:

- a. we reasonably believe that:
 - i. the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
 - ii. there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- b. both of the following apply:
 - i. the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8a will not apply to the disclosure;
 - ii. after being so informed, the individual consents to the disclosure; or
- c. the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- d. a permitted general situation exists in relation to the disclosure of the information by the APP entity; or
- e. the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or
- f. the entity is an agency and both of the following apply:
 - i. the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
 - ii. the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

APP 9 – Adoption, Use or Disclosure of Identifiers

We identify our clients via identifiers created on our electronic database. We do not identify clients using numbers that have been assigned to them by:

- (a) an agency; or
- (b) an agent of an agency acting in its capacity as agent; or
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

It is not our practice to use or disclose an identifier assigned to a client by an agency, or by an agent or contracted service provider, unless:

- a. the use or disclosure is necessary for the us to fulfil our obligations to the agency; or
- b. we reasonably believe that the use or disclosure is necessary to lessen or prevent:
 - (i) a serious and imminent threat to an individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety; or
- c. we have reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- d. the use or disclosure is required or authorised by or under law; or
- e. we reasonably believe that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal
- f. the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.



APP 10 – Quality of Personal Information

We will do all we can to ensure the personal information we collect is accurate, up-to-date and complete.

APP 11 – Security of Personal Information

We will at all times seek to ensure that the personal information collected and held by us is protected from misuse, loss, unauthorised access, modification or disclosure. At all times your personal information is treated as confidential and any sensitive information is treated as highly confidential. All computer based information is protected through the use of access passwords on each computer and screen saver passwords. Data is backed up each evening.

In the event you cease to be a client of this organisation, any personal information which we hold about you will be maintained in a secure off site storage facility for a period of 7 years in order to comply with legislative and professional requirements, following which time the information will be destroyed.

APP 12 – Access to Personal Information

You may at any time, by contacting us by any of the methods detailed below, request access to your personal information and we will (subject to the following exceptions) provide you with access to that information either by providing you with copies of the information requested, allowing you to inspect the information requested or providing you with an accurate summary of the information held. We will, prior to providing access in accordance with this policy, require you to provide evidence of your identity.

We will not provide you access to personal information which would reveal any confidential formulae or the detail of any in house evaluative decision making process, but may instead provide you with the result of the formulae or process or an explanation of that result.

We will not provide you with access to your personal information if:

- a) providing access would pose a serious threat to the life, health or safety of a person, or to public health or public safety; or
- b) providing access would have an unreasonable impact on the privacy of others; or
- c) the request for access is frivolous or vexatious; or
- d) the information related to existing or anticipated legal proceedings between us and would not be discoverable in those proceedings; or
- e) providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations; or
- f) providing access would be unlawful; or
- g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- h) both of the following apply:
 - (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
 - (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- i) providing access would be likely to prejudice certain operations by or on behalf of an enforcement body; or
- j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision making process.

In the event we refuse you access to your personal information, we will provide you with an explanation for that refusal and the mechanisms available to complain about our refusal.

APP 13 – Correction of Personal Information

We will endeavor to ensure that, at all times, the personal information about you which we hold is up to date and accurate. In the event that you become aware, or believe, that any Personal Information which we hold about you is inaccurate, incomplete or outdated, you may contact us by any of the methods detailed below and provide to us evidence of the inaccuracy or incompleteness or outdatedness and we will, if we agree that the information requires correcting, take all reasonable steps to correct the information.

If we do not agree that your personal information requires correcting, we must, if you request, take reasonable steps to ensure that whenever your personal information is accessed or handled in the future, it is apparent that you are not satisfied as to the accuracy or completeness of that information.

We will endeavour to respond to any request for access within 14-30 days depending on the complexity of the information and/or the request. If your request is urgent please indicate this clearly.



Contacting Us

If you wish to complain about any breach or potential breach of this privacy policy or the Australian Privacy Principles, you should contact us by any of the methods detailed below and request that your complaint be directed to the Privacy Officer. Your complaint will be considered within 7 days and responded to. It is our intention to use our best endeavours to resolve any complaint to your satisfaction, however, if you are unhappy with our response, you are entitled to contact the Office of the Privacy Commissioner who may investigate your complaint further.

Contact Details

Privacy Officer: **Matthew Tuton**
Nexus Private Financial Services Pty Ltd
Level 14, 307 Queen Street
Brisbane QLD 4000

Email: financialplanning@exusprivate.com.au

Telephone: 1300 473 347