ProctorMajor.

PRIVACY POLICY.

This Privacy Policy applies to all personal and sensitive information collected by each of:-

- Proctor Major & Co Pty Ltd, ACN 069 883 165;
- Proctor Major Wealth Pty Ltd, ACN 612 643 348
- Proctor Major Property Solutions Pty Ltd, ACN 155 968 835

(collectively referred to as **Proctor Major**)

1. Introduction

We understand that you want your personal information given confidentiality and to be treated with respect. Protecting your information is an important part of maintaining the trust between you and Proctor Major. By handling your personal information in a secure manner and only making it available as necessary to third parties, we hope to build a strong business relationship with you. Proctor Major is committed to upholding the best standards in privacy compliance possible.

This Privacy Policy explains how we gather, protect, hold and use your personal information so we can provide the products and services you require. It relates to:-

- preparing your statutory accounts;
- preparing and lodging your personal and business income tax returns;
- dealing with relevant government authorities such as:-
  - the Australian Taxation Office
  - the Australian Securities & Investments Commission
  - the State Revenue Office
  - the Australian Prudential Regulation Authority

  and other similar government departments and bodies
- sending your personal and sensitive information between the various entities comprising Proctor Major; and
- providing your data as requested by you.

We are bound by the *Privacy Act* 1988 (Cth) and accordingly, we have adopted and employed the obligations contained in the *Privacy Act* 1988 (Cth), the thirteen Australian Privacy Principles (**APP**) summarised in Paragraph 9, and any registered APP Code applicable to our privacy practices, procedures and systems for handling your personal and sensitive information.

Further, we are required to observe the requirements imposed on accounting and financial planning practices such as Proctor Major with a number of other statutory and other requirements. These are set out in Paragraph 8.

We aim to support and comply with all statutory requirements, the APP and any registered APP Code in relation to collecting, disclosing and protecting your personal and sensitive information.

2. Purpose in Collecting Your Personal Information

You may be considering, or have decided, to enlist the services of Proctor Major to;-

- assist you to prepare your statutory accounts
- prepare and lodge your personal and business income tax returns
- to assist in building your wealth
- to recommend business and investment structures for you or your business
- to assist in procuring a loan, a mortgage or other financial product.
- to help in planning for your retirement
- investment planning
- estate planning
- appropriate insurance cover for you and your business
- to provide an informal or formal business valuation
- to assist with or take over your business negotiations

You may have used our website, have had direct contact with us, or an intermediary or representative (such as your financial planner), with your trustee or administrator of your superannuation fund, your employer or your legal representative(s).

At all times, we try to collect only the information we need for the specific function or activity you have asked us to do. We need to obtain certain items relating to your personal circumstances and your personal details to:-

- provide you with the products and services you require;
- provide you with information about the products and services available to you from Proctor Major;
- provide your details to third party service providers such as legal firms;
- enable your loan applications to be assessed by prospective financial institutions; and
- enable your insurance applications to be assessed by prospective insurance providers.

We are also legally obliged to assist law enforcement or other regulatory authorities where required by the law. Those legal obligations arise under a range of laws including the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (Cth) and other similar laws in other countries. Under these laws, we may be required to collect certain information from you, or about you, to prove your identity and your residency.

3. Collection and Use of Your Personal Information

3.1 Types of Personal Information Collected

Generally, but depending on the products or services you have asked us to provide to you, we ask for your name, address, contact details, date of birth and your gender.

In relation to financial products, we are likely to ask you for your financial details such as your tax file number, bank account details, credit card details, your occupation, income and expenses, your employment information, your residency and citizenship status. We may also ask you for financial information pertaining to your business.

In relation to insurance products, and depending on the type of insurance you wish us to source, we may also need to collect sensitive information which may include your health and medical information, your lifestyle and pastime information, your physical attributes, capacity and activity and your racial or ethnic origin.

3.2 Method of Collecting Personal Information

Your consent is generally required to allow us to collect your personal information unless the law provides otherwise. Before asking for your personal information, we take reasonable measures to provide this Privacy Policy to you. We only collect your personal and sensitive information by

lawful and fair means.

You are able to withdraw your consent at any time of your choice by phoning us, posting a letter to us or sending us an email. Our contact details are shown in Paragraph 7. We only collect and hold sensitive information with your consent, in limited situations which the law allows.

If you refuse to allow us to collect the personal and sensitive information we need to provide you with services you require of us, the appropriateness or adequacy of advice given to you may expose you to higher risks in respect of the recommendations made.

We may collect your personal information when you give it to us by phone, email, online or by post. Your personal information is also captured when you use our services including when you access or use our website or online services.

In some cases, we may also collect your personal information from third parties such as:-

- persons authorised by you, including family members
- lawyers, accountants and other financial advisors
- your employer
- hospitals, medical practitioners and health service providers particularly in relation to insurance products
- public sources of information
- social media and other virtual sources where information is publicly shared.

Unless it is unreasonable or impracticable, we will try to collect your personal information directly from you unless the collection is required by law to be sourced from a third party.

When we have collected your personal information, we will inform you that we have collected it unless:-

- you are aware of its collection; or
- you would expect us to have your personal information; or
- it is not reasonable to do so.

If you have browsed our website, certain anonymous information will be collected relating to your browsing such as your server address, the date and time of your visit, the pages and links accessed and the type of browser you have used. This anonymous information is used for statistical purposes and to improve the content and functionality of our website.

The anonymous information is collected by the use of “cookies”. Cookies by themselves cannot be used to discover the identity of the user. Cookies do not damage your computer and you can set your browser to notify you when you receive a cookie to determine if you wish to accept it. Once you leave the site, the cookie is destroyed and no personal or other information about you is stored.

If you have started an online application but don’t complete and submit it, we may contact you using the contact details you have supplied to offer assistance to complete the form. The information in our online application forms will be kept temporarily then destroyed if the application is not completed within one month.

3.3 Use and Disclosure of Your Personal Information

We may use your personal information to:-

- prepare your statutory accounts
- prepare and lodge your personal and business income tax returns
- to assist in building your wealth
- to recommend business and investment structure for you or your business
- to assist in procuring a loan, a mortgage or other financial product
- to help in planning for your retirement
- investment planning
- estate planning
- appropriate insurance cover for you and your business
- to provide an information or formal business valuation
- to assist with or take over your business negotiations
- give you information about financial products or related services including help and advice
- help you to determine your eligibility for financial products or related services
- help you to prepare an application for financial products or related services
- administer services we provide such as answering requests or dealing with complaints

We may also use your personal information to:-

- notify you about new services and special offers;
- events or articles we think may be of interest to you;
- send you regular updates about business, accounting, taxation, financial or insurance matters.

If you do not wish to receive information of this type, please contact us to arrange for some or all of it to cease.

We may disclose you personal information, with your consent, to:-

- any person authorised by you or acting on your behalf including your accountant, your financial planner, your lawyer, your (superannuation fund) trustee or administrator, your employer, guardian, attorney, agent or platform provider
- affiliated product and service providers including other businesses with whom we have a business or branding arrangement
- regulatory bodies and government agencies, if required or authorised to do so
- financial institutions and credit providers
- insurers and reinsurers;
- co-insured persons, policy or product holders or other persons who are authorised or noted on an insurance policy as having a legal interest where you are the insured person
- hospitals, medical practitioners and health service providers

It is also possible that we may disclose your personal information to third parties which are:-

- undertaking reviews of our systems and operations
- a third party with whom we have an arrangement to provide us with a product or service for you
- involved in providing, managing or administering your product or service such as third party suppliers, posting services, call centres, IT support and our advisers

- involved in maintaining, reviewing and developing our business systems, procedures and infrastructure including testing or upgrading our computer systems
- involved in the payments system including financial institutions, merchants and payment organisations

In all circumstances, these third parties are required to keep your personal information confidential and only use it for the same purposes as we are permitted to do.

Where we hold your personal information in conjunction with that of another individual, we allow each individual access to their own personal information and to common information, but not to the personal information of the other individual or individuals.

3.4 Prohibited Use of Your Personal Information

We are prohibited from using or disclosing your personal information for a purpose other than the purpose for which it was collected, unless you have consented, or it would be reasonable to expect your personal information to be used for the secondary purpose, or another prescribed exception applies.

Such prescribed exceptions generally arise where the disclosure is necessary to protect someone's health or safety or is otherwise in the public interest.

There is a general prohibition on personal information being used for direct marketing purposes unless you reasonably expect it, or have consented to it, and prescribed 'opt out' processes are in place through which you can elect not to receive direct marketing communications (and you have not elected as such).

Finally, there is a prohibition from adopting, using or disclosing a government-related identifier (such as your tax file number, Medicare number, passport number or driver's licence number, etc) unless:-

- required or authorised by law
- necessary to verify your identity and/or
- another prescribed exception applies.

4. Taking Care of Your Personal Information

4.1 Storage and protection

We store your personal information in different ways, including in paper and electronic forms. The security of your personal information is important to us and we take reasonable steps to protect your personal information from unauthorised access, unauthorised disclosure, loss, misuse or interference by implementing a range of electronic, physical and technological safeguards. Some of the ways we do this are:-

- document storage security policies
- security measures for access to our systems
- only giving access to your personal information to a person who is verified to be able to receive that information.

We may store your personal information physically or electronically with third party data storage providers. Where we do this, we use contractual arrangements to ensure those providers take appropriate measures to protect your information and restrict the uses to which they can put that information. Our records are stored on a secured server located in our offices and our website is hosted in Australia. All your personal information is

encrypted when stored electronically.

We have a data breach response plan in place and processes to investigate and, if relevant, to report breaches to impacted individuals and the Office of Australian Information Commissioner (**OAIC**) where there is a likelihood of a real risk of serious harm given the circumstances of the breach.

We require our outsourced service providers who handle your personal and sensitive information to promptly notify us of any privacy and data type breaches and periodically obtain assurances that they have done so.

The actions we take to protect your personal information include:-

- encrypting your personal information when you complete online forms
- educating our staff about the importance of protecting your personal information and requiring them to securely access information on our systems
- using firewalls, intrusion prevention systems and virus scanning tools to protect against unauthorised persons and viruses from entering our systems
- restricting access to your personal information
- physical access controls for our premises and/or
- entering into confidentiality agreements with relevant employees and third parties.

4.2 What Happens to Your Personal Information when it is not Needed

We have processes in place to only retain your personal information for as long as is reasonably required unless we are required or authorised by law to retain it for longer or for prescribed periods.

Where relevant, your personal information that is retained by us is de-identified.

5. Accessing and Changing Your Personal Information

5.1 Accessing Your Personal Information

You are generally entitled to access the personal information we hold about you. If you wish to access your personal information, please send a written request which includes your name and address, the type of information you would like to receive and any relevant details (such as your account number or insurance policy number) sufficient to allow us to identify the information you wish to access.

We will respond to you as soon as possible, with the timing being dependent upon the quantity and complexity of your request. A charge for direct costs, such as photocopying, postage and the like may be imposed. You will not be charged a fee for the time we spend to provide you access to your personal information.

There may be some restrictions on providing access to your personal information if, for example, the provision of that information would pose a serious threat to the life, health or safety of an individual, if there would be an unreasonable impact on the privacy of others, if the information is protected from disclosure by law and the like. Where your personal information cannot be provided to you, and where reasonable, we will provide you with a written notice setting out the reasons for the refusal. That notice will also provide you with advice on making a complaint.

5.2 Changing Your Personal Information

We will correct, amend or delete any personal information that we agree is inaccurate, out-of-date, incomplete, irrelevant or misleading. You will not be charged for any changes which need to be made to your personal information.

If we refuse a request for correction of your personal information, we will provide you with the reasons for the refusal and we may be required to link to your personal information a statement evidencing your view that your personal information held by us is incorrect.

Where we do make a correction to your personal information, we may need to notify third parties to which your personal information, in its incorrect form, was disclosed.

6. Complaints

6.1 Initial action

If you wish to bring our attention to any privacy issues, including the use and/or disclosure of your personal or sensitive information, your first step is to contact us with the details of your complaint. You may make an appointment to see us in our office, or contact us by post, email or phone. Your complaint should be addressed to the Practice Manager.

We will attempt to resolve your complaint immediately but, in any event, we will acknowledge receipt of your complaint within seven days of receiving it regardless of the method of contact you have used. It is possible that one of our team members from our internal complaints division will need to contact you to obtain further details, supporting evidence and the like.

Some complaints require a considerable time to investigate and resolve. If your complaint is of this type, we will keep you informed of progress on a fortnightly basis.

We will do everything in our power to address and resolve your complaint.

6.2 Further action

If you remain unsatisfied with our response to your complaint, you are entitled to take up your complaint with the OAIC (Office of Australian Information Commissioner). That office has the power to investigate privacy complaints from individuals about our business if we are specifically caught by the Privacy Act.

However, before you can lodge a complaint with the OAIC, they will generally need to see that you have firstly lodged your complaint directly with us and given us 30 days to respond to you.

All complaints lodged with the OAIC must be made in writing. Details about the OAIC are set out below:-

Office of Australian Information Commissioner
GPO Box 5218
SYDNEY NSW 2001

Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Website: http://oaic.gov.au

7. Contact Details

Proctor Major Pty Ltd
Level 5 / 1 Como Street
MALVERN VIC 3144

PO Box 455
MALVERN VIC 3144

Phone: (03) 9571 8822
Email: info@proctormajor.com.au
Website: http://www.proctormajor.com.au

8. Statutory and Regulatory Requirements

The following statutes, regulations and bodies require Proctor Major to observe a range of privacy practices. These include:-

- Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- APSES 110 Code of Ethics for Professional Accountants issued by the Accounting Professional and Ethical Standards Board
- Australian Privacy Principles (APP)
- Code of Conduct of the Association of Financial Advisers of Australia
- Code of Practice for CPA Australia
- Code of Practice of the Mortgage and Finance Association of Australia
- Code of Professional Conduct of CPA Australia
- Corporations Act 2001
- National Consumer Credit Protection Act 2009
- Office of the Federal Privacy Commissioner
- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012

9. Australian Privacy Principles

APP 1: Open and transparent management of personal information

APP 1 requires an APP entity to implement privacy practices, procedures and systems:-

- to ensure compliance with the remaining APPs and
- that enable them to deal with inquiries and complaints.

It also requires them to develop and make readily available a policy about its management of personal information.

APP 2: Anonymity and pseudonymity

APP 2 entitles individuals to the option of anonymity or using a pseudonym, when dealing with an APP entity, except where impracticable or another prescribed exception applies.

APP 3: Collection of solicited personal information

APP 3, in summary:-

- permits an APP entity to collect personal information only where reasonably necessary for one or more of its legitimate functions or activities;
- requires personal information to be collected directly from the

individual to whom it relates, unless impracticable or another prescribed exception applies; and

- requires the consent from an individual in order to collect that individual's sensitive information, or another prescribed exception applies.

APP 4: Dealing with unsolicited personal information

APP 4 requires an APP entity that receives unsolicited personal information to determine whether it would otherwise have had grounds on which to collect it (i.e. under APP 3) and:-

- where it does have such grounds, to ensure compliance with the remaining APPs; or
- where it does not have such grounds, to destroy or de-identify the personal information (provided it is lawful and reasonable to do so).

APP 5: Notification of the collection of personal information

APP 5 requires an APP entity to notify an individual (or ensure they are aware), at or before the time of collection, of prescribed matters. Such matters include but are not limited to whether the individual's personal information is collected from any third parties, the purpose(s) of collection, to whom personal information is disclosed and the processes through which an individual can seek access and/or correction to their personal information, or otherwise complain about the way in which it is handled.

Compliance with APP 5 usually requires 'collection statements' to be included on or with forms, or other materials, through which personal information is collected. Such statements should refer and include a link to the APP entity's privacy policy.

APP 6: Use or disclosure of personal information

APP 6 prohibits an APP entity from using or disclosing personal information for a purpose other than the purpose for which it was collected, unless the individual consents, the individual would reasonably expect their personal information to be used for the secondary purpose, or another prescribed exception applies.

Such prescribed exceptions generally arise where the disclosure is necessary to protect someone's health or safety or is otherwise in the public interest.

APP 7: Direct marketing

APP 7 generally prohibits personal information to be used for direct marketing purposes unless the individual reasonably expects it, or consents to it, and prescribed 'opt out' processes are in place through which the individual can elect not to receive direct marketing communications (and the individual has not elected as such).

APP 8: Cross-border disclosure of personal information

If an APP entity is to disclose personal information to an overseas recipient, APP 8 requires it to take reasonable steps to ensure the recipient does not breach the APPs. This usually requires the APP entity to impose contractual obligations on the recipient.

Relevantly, if the overseas recipient does breach the APPs, the Privacy Act

imposes liability on the APP entity that made the overseas disclosure.

There are exceptions to this obligation, including but not limited to where:-

- the APP entity reasonably believes the overseas recipient is bound by a law or scheme that protects personal information in a substantially similar way to that of the APPs or
- the individual consents to the disclosure in the knowledge that such consent will negate the APP entity's obligation to ensure the overseas recipient does not breach the APPs.

APP 9: Adoption, use or disclosure of government related identifiers

APP 9 prohibits an APP entity from adopting, using or disclosing a government-related identifier unless:-

- required or authorised by law
- necessary to verify an individual's identity and/or
- another prescribed exception applies.

Government-related identifiers are identifiers that have been assigned by a government agency including an individual's licence number, Medicare number, passport number and tax file number.

APP 10: Quality of personal information

APP 10 requires an APP entity to take reasonable steps to ensure personal information it collects, uses, discloses and holds is accurate, up-to-date and complete. Additionally, personal information can only be used or disclosed to the extent to which it is relevant to the purpose of the use or disclosure.

APP 11: Security of personal information

APP 11 requires an APP entity to take reasonable steps to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure. An APP entity must also destroy or de-identify personal information it no longer requires (unless otherwise required to retain it by law).

APP 12: Access to personal information

APP 12 requires an APP entity to provide an individual, upon request, with access to their personal information unless a prescribed exception applies.

APP 13: Correction of personal information

APP 13 requires an APP entity to take reasonable steps to correct personal information it holds upon request from an individual for correction or where it is otherwise satisfied, having regard to the purpose for which it holds the personal information, that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If an APP entity refuses a request for correction, it needs to provide the individual with the reasons for the refusal and may be required to associate with the personal information a statement evidencing the individual's view that the information is incorrect.

Where correction does occur, the APP entity may need to notify third parties to which the personal information, in its incorrect form, was disclosed.