DATA PROTECTION POLICY

Intent

To assure compliance with relevant data protection legislation;
To protect the fundamental right to data protection with respect to the processing of personal, sensitive and health information;
To establish principles of transparency and fairness for the management of personal, health, sensitive or confidential information at **Treysta**.

Scope

This policy covers the management of all personal, sensitive and health information at **Treysta** no matter how this information is collected or stored.
The policy is applicable to all staff within Treysta.

Exclusions

This policy does not apply to personal information or data which has been manifestly made public by the data subject or is legitimately already within the public domain.
This policy does not include information that relates to a corporate, government or business entity.

Objectives

To guide staff in the responsible collection, use, disclosure and handling of information collected and managed by **Treysta**, which relates personally to an individual or their affairs.

Policy Provisions

1. Management of personal, sensitive, health and confidential information

Treysta is committed to the responsible handling, and open and transparent management, of personal, sensitive, health and confidential information and to protecting the right to data protection of individuals whose information it holds.

Treysta must not act or engage in a practice that breaches any relevant data protection legislation in Australia; except where other Australian or international jurisdiction legislation specifically requires or allows the practice.

2. Basic Privacy and confidentiality principles

The following basic privacy principles must be applied in accordance with the relevant supporting instruction.

Treysta and all its operations must:

a. Collect only that information necessary to fulfil **Treysta** functions and activities.

b. Use the information only for the purpose for which it was collected, for related secondary purposes, with consent or as required or permitted by law.

c. Manage all data breaches in accordance with the **Treysta** procedure and always consider, in a non-self-serving manner, notification to impacted individuals.

d. Do not use or disclose personal information for the purpose of direct marketing, unless an exemption applies or unless express consent has been obtained from the individual.

e. Endeavour to ensure that information is accurate, complete and up-to-date.

f. Ensure the security of information and its proper storage, archiving or disposal in accordance with appropriate recordkeeping standards and information technology safeguards.

g. By arrangement, enable individuals to access their data and make appropriate corrections, in accordance with relevant access procedures.

h. Collect and use sensitive information only in accordance with the relevant **Treysta** procedure, or where required or permitted by law.

3. Member's personal information

The principles of Australian privacy law are the base or minimum level of information management and protections for all **Treysta** members and their personal, sensitive and health information.

Access and Correction of Personal Information

Instructions, steps and actions

1. Access to personal information

As a rule, **Treysta** endeavours to let people see their own information in the simplest way possible and correct it where necessary.

Should an individual request to access their own information, **Treysta** will assist in processing this request at no extra charge, though an administrative fee may be charged for providing a copy of the client's personal information.
In order to protect the client's personal information, identification verification may be requested prior to releasing the requested information.

2. Correction of personal information

If **Treysta** holds personal information about an individual and the individual is able to establish to the satisfaction of **Treysta** that the information is not accurate, complete and up to date, **Treysta** will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

Collection of personal information instruction

Instruction Statement

This is a supporting document for the Data Protection Policy and guides information management in accordance with that policy and relevant privacy law.

Instruction steps and action

1. Collection Fundamentals

Collection is a fundamental part of privacy protection and it is essential that it is managed correctly. In simple terms the rules are:

a. Collect only what you need for the advice or research you are conducting.
b. Do it lawfully and fairly.
c. Don't intrude unreasonably
d. Tell people you are doing it.

In practice this means that you should only collect personal information if it is necessary for one or more of **Treysta** functions or activities.

2. Required information

If required information in **Treysta** is not completed and/or provided by an individual, this will impact the ability of the advice/research being completed to a proper degree.
If this missing data is identified, reasonable effort should be made in obtaining this advice from the financial client. Should this not be provided by the client, this in turn may impact on the relevance/appropriateness of the advice and **Treysta** reserves the right to not proceed with any work until properly supplied.

3. Unsolicited personal information

Personal information may be given to **Treysta** that was not requested (unsolicited).
Unsolicited personal information must also be managed in accordance with Treysta's data protection policy and relevant privacy law.
Examples of unsolicited information may be letters or emails to **Treysta** from clients which are not relevant to the advice document or research being conducted.

4. Sensitive and health information

Sensitive information about people – like their ethnic background, religion, political views or affiliations, sexual preference or criminal records – has special protection under law. Such information can only be collected if it is essential for **Treysta** operations, required by law, or with specific and informed consent.
Do not collect it without checking the rules first.
Sensitive and health information have special protections because this kind of information can be used to discriminate against individuals.

It is advised not to collect sensitive or health information about an individual unless certain conditions are met, including:

a. The individual has consented;
b. This information is required to assist with providing financial advice and research about life insurance products.
c. The collection is required under law; and/or
d. The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

There are certain exemptions to the above requirements, such as where:

a. The collection is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services;

b. The information relates to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or education services;

c. There is no reasonably practicable alternative to collecting the information for that purpose; and/or

d. It is impracticable for **Treysta** to seek the individual's consent to the collection.

Management of personal information instruction

Instruction Statement

This is a supporting document for the Privacy and Data Protection Policy and guides information management in accordance with that policy and relevant privacy law.

Instruction steps and actions

1. Management of personal information

The day to day management of personal information is everyone's responsibility.
In brief, rules for managing personal, sensitive and health information are to keep it accurate, complete, up to-date, and secure.
Treysta is available for advice and guidance when needed.

2. Maintaining accuracy and quality of personal information

Staff must take reasonable steps to ensure the information they are working with is accurate.
Personal information that is inaccurate affects the quality of **Treysta** service provision. For example, a wrong birthday may impact on a client's Life insurance premiums which in turn may lead to a misrepresentation of the costs involved.

3. Data security

Security and retention are part of the 'life cycle' of personal information or data. All staff of **Treysta** must take reasonable steps to ensure that:

a. Personal information is protected from misuse, loss, unauthorised access or modification, or improper disclosure.

b. Information has not been changed or tampered with.

c. Hard copy records (if any) containing personal information should be kept in a secure location and away from non-authorized persons.

d. Communications and computing systems have appropriate access security controls and are not disrupted in their normal operations.

e. Authentication processes (for identification) are adhered to, in that a person accessing or providing information are who they claim to be.

If **Treysta** is to ensure the quality and accuracy of personal information, this places an obligation upon an individual, including staff, volunteers and members to provide relevant and accurate information (and where relevant corrections) to **Treysta**.
Treysta takes reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose and in accordance with applicable recordkeeping law and standards.
Recordkeeping standards detail the need for **Treysta** to keep full and accurate.

4. Openness and transparency

Treysta, and its staff must be open about what is done with other people's information. This includes providing the Data Protection Policy to anyone who requests it.
Questions can be referred to the **Treysta** managing director.

Use and disclosure of personal information instruction

Instruction Statement

This is a supporting document for the Data Protection Policy and guides information management in accordance with that policy and relevant privacy law.

Instruction steps and actions

1. Use and disclosure of Treysta's primary purposes

In most cases, use and disclose of an individual's personal information only for the purpose you collected it – this is defined as a primary purpose. For example, client's details are collected to properly provide financial advice and/or research.

Disclosure must always be limited to what is sufficient for the purpose.

2. Use and disclosure of related secondary purposes

There is some allowance to use and disclose personal information for a secondary purpose that is related to the primary purpose and is what someone would reasonably expect. An example of a secondary purpose would be to use a member's email address to provide details of **Treysta** news or events.

Where practicable, prior consent should be obtained before use or disclosure for a secondary purpose.

Impracticality to obtain consent must be assessed in context, but generally is means more than mere inconvenience, incurring some cost or effort, or undesirability of seeking consent.

When use or disclosure of personal information is required for a secondary purpose, without the prior consent of an individual, the following must be considered:

a. The secondary purpose must relate to the primary purpose for collection; and

b. The individual would reasonably expect the use or disclosure of the information for that secondary purpose.

It should be noted that sensitivity of information may affect reasonable expectation.

Please note: If the personal information is sensitive information (e.g. political views, sexual orientation, ethnicity) use and disclosure must be directly related to primary purpose of collection and have consent where that is practicable. If you are considering using or disclosing personal or sensitive information for a secondary purpose, please consult with **Treysta** managing director.

3. Use and disclosure for the prevention of risk to life, health, safety and welfare

Some important interests, such as protecting health and safety, can justify use and disclosure without consent. This kind of lawful use and disclosure can be for purposes unrelated to the primary purpose and must meet the following test:

If **Treysta** reasonably believes that the use or disclosure is necessary to lessen or prevent either:

a. A serious and imminent threat to an individual's life, health, safety or welfare; and/or

b. A serious threat to public health, public safety or public welfare.

In most cases, such a disclosure must be to an appropriate agency or recipient that is able to lessen or prevent the threat. For example, depending on the circumstances, appropriate recipients would be the police, emergency services or health authorities.

4. Use and disclosure to investigate suspected unlawful activity or serious misconduct

If **Treysta** has reason to suspect that unlawful activity has been, is being or may be engaged in, use or disclosure of personal information may be undertaken as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

Misconduct by staff, volunteers and members may also be considered to be unlawful if it contravenes a statutory obligation. Examples of such obligations include misusing information acquired during official duties or breaching the relevant Codes of Conduct. Use and disclosure of personal information at any stage of an investigation into serious misconduct for the purposes of determining whether the suspected activity is taking place is permitted where necessary to the investigation.

Where it is proposed to use or disclose personal information in order to investigate a matter within **Treysta** itself, the following must be taken into consideration:

a. Any suspicion of wrongdoing should be based on reasonable grounds, not just unsubstantiated gossip or rumour;

b. The use or disclosure must be considered necessary after due consideration of alternatives; and

c. The use or disclosure should be as confined as possible throughout the investigation.

5. Use and disclosure required and authorised by law

Personal information may be used or disclosed otherwise than for the primary purpose if such use or disclosure is required or authorised by or under law:

a. Required by law – means that there is a legal obligation to use or disclose personal information in a particular way. It should be noted that, in Australia, other laws take priority over privacy law provisions in
this regard.

b. Authorised by law – means that while the law permits the use or disclosure, it does not make either compulsory. Where doubt exists for this provision, please consult with **Treysta** managing director.

6. Use and disclosure to a law enforcement agency

Use and disclosure of personal information without consent is permitted when **Treysta** reasonably believes that it is necessary for one or more of the following upon request by, or on behalf of, a law enforcement agency:

a. The prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

b. The enforcement of laws relating to the confiscation of the proceeds of crime;

c. The protection of the public revenue;

d. The prevention, detection, investigation or remedying of seriously improper conduct; and/or

e. The preparation for, or conduct of, proceedings before any court or tribunal.

In emergency situations, disclosures of **Treysta** client information to appropriate agencies, such as emergency health services or the Police, can be authorised by the managing director.

A written record must be kept of all such disclosures and circumstances which will be retained by **Treysta**.

Consequences of failing to utilise personal information appropriately

Instruction Statement

This is a supporting document for the Data Protection Policy and guides the consequences if an employee fails to manage information in accordance to the Data Protection Policy.

Instruction steps and actions

1. Confidentiality Agreement

In the course of a staff's employment, and due to the nature of the job scope, an employee will have access to and become privy to the financial background, salary information,

personal/health information, and other confidential information of the Company and/or clients of the Company.

As an employee of **Treysta**, an employee agrees that they will not, at any time and without the prior written consent of the Directors, disclose or make any use whatsoever of such information, except as may be requested by the Directors or otherwise be required by applicable law.

In the event that **Treysta** obtains confidential information as aforementioned from any clients or third party, an employee shall not, without the written consent of the Directors at any time (either during their employment or after the termination of their employment), infringe restrictions on disclosure agreed to by **Treysta**. This has been agreed upon in our letter of employment.

2. Termination for Cause

If the above guidelines and agreements are not adhered to, an employee's employment with **Treysta** can be terminated immediately (without prejudice to and in addition to any other remedy available to us). If this breach of conduct was to a lesser degree, disciplinary action will be pursued in proportion to the severity of the case.