This policy applies to **Knightcorp Holdings Pty Ltd as trustee for WDK Trust trading as Knightcorp Insurance Brokers ("Knightcorp")** and all our representatives. It explains our policy in relation to the collection and management of personal information we collect from individuals. The Privacy Act 1988 requires us to handle personal information in accordance with the Australian Privacy Principles ("APP").

Collection of information – What is collected and why we collect it.

Personal information means information, or an opinion about, an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. We are an Australian Financial Services Licensee ("AFSL"). When we provide you with financial services, we may be required by Corporations Act and regulatory requirements to seek to obtain certain personal information about you, including, but not limited to, your:

Name, date of birth and contact details.
Information required to advise you about your insurance needs and management of your risks.
Information required to organise premium funding arrangements on your behalf.

Sensitive information

We may also need to collect sensitive information if we organise insurance covers for you. Sensitive information includes health information, racial information, genetic information, etc.
We will only collect sensitive information that is reasonably necessary for us to perform our functions or activities in advising you and dealing with you.

How is information collected?

We collect personal and sensitive information in a number of ways, including:

Directly from you such as when you provide the information at meetings, by phone, email, in data collection forms and when you visit our websites.
Our website may use "cookies". Cookies are small data files that are downloaded from our website and stored on your computer when you visit our website. Cookies are used to allow us to see which pages and what information is of most interest to visitors to our website, which in turn enables us to improve our offerings to our customers.
Your computer's web browser will allow you to configure your computer to refuse to accept cookies. You can also delete cookies from your computer's hard drive at any time. However, please note that doing so may hinder your access to valuable areas of information within our site.
Indirectly from insurers and third parties where authorisation has been provided by you or where you have authorised other parties to provide us with this information.

Are you obliged to provide us personal information?

You are not required to provide us the information that we request, or to allow us to collect information from third parties. However, where you choose not to provide us with the information we request, we may not be able to provide you with services that you have requested from us, and we may elect to terminate our arrangement with you.
Importantly, if you provide either inaccurate or incomplete information to us you risk breaching your duty of disclosure, which may result in a reduced payout by the insurer in the event of a claim or the insurer may avoid the contract from its inception.

What happens if we obtain information about you which we have not solicited?

Where we receive unsolicited personal information about you, we will consider if we could have collected the information if we had solicited the information. Where we determine that we could have collected the personal information from you, we will treat your personal information in the same manner as if we have solicited the information directly from you. Where we determine that we could not have collected the personal information, we will destroy the information or ensure that the information is de-identified as soon as practicable.

Use of information

We use your personal information for the primary purpose for which the information was obtained: i.e. for the provision of financial services. As an AFS licensee, that will typically mean for the purpose of:

Providing financial services to you.
Implementing risk management recommendations on your behalf.
Organising premium funding arrangements on your behalf.

We may also use the information for the secondary purpose of:

Attempting to identify other products and services that may be of interest to you.
Conducting any professional quality control review program.
Managing our business operations such as maintaining secure IT systems.

Do we disclose personal information for marketing?

We may use your personal information to offer you products and services that we believe may interest you. We may also disclose your personal information to external associates and service providers who assist us to market our products and services.

If you do not want to receive marketing offers from us, please inform us. Our contact details are included at the end of this policy.

Disclosure of information

We may disclose your personal information to:

Our representatives.
The product issuers of products and services that you have elected to acquire, vary or dispose of using our assistance.
Our external service providers.
Prospective entities interested in acquiring all or part of our business.

For example, information may be disclosed to the following parties:

Insurers for the purpose of giving effect to the recommendations made by us. This may include underwriting agencies and reinsurers.
Premium funders for the purpose of organising a premium funding arrangement on your behalf.
Other parties involved in the administration of your insurance cover (e.g. actuaries, call centers, mail houses, claims assessors, medical advisers, etc).
Our external service providers (e.g. IT providers, professional advisers and contractors).
Government and regulatory authorities and other organisations, as required or authorised by law.
Any person considering acquiring, or acquiring, an interest in our business.

Government related identifiers

We do not collect government related identifiers; e.g. tax file number, Medicare number or pension card number.

Cross-border disclosure of personal information

We may transfer personal information to related bodies corporate or external service providers in locations outside Australia, including, but not limited to, Philippines, India, United States, China, Poland and the United Kingdom in the course of storing that information and when using or disclosing it for one of the purposes referred to above. When transferring personal information to foreign jurisdictions, we will ensure that we satisfy one of the requirements below:

- we will take reasonable steps to ensure the overseas recipient does not breach the APP in relation to the information.
- we form a reasonable belief that the overseas recipient 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 APP protect the information and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- we will seek your informed consent prior to disclosing your personal information overseas.

Storage and security of information

We store personal information in our computer database and hard copy files. We take reasonable steps to ensure the personal information collected and held by us is protected from misuse, interference, loss, unauthorised access, modification or disclosure. Our computer systems are password protected and accessible by our staff only. Our offices have appropriate security.

In the event you cease to be a client of ours, any personal information which we hold about you will be maintained for a period of not less than 7 years in order to comply with legislative and professional requirements.

Notifiable data breaches

We are required to notify you and the Information Commissioner of an eligible data breach. An eligible data breach happens if:

there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by us; and
the access, disclosure or loss is likely to result in serious harm to you.

If you receive a statement of an eligible data breach from us, you should read and implement the recommendations about the steps you should take in response to the eligible data breach.

Access and correction of information

You may request access to the personal information we hold about you, and we will respond within a reasonable period after the request is made. Where we provide you access to such information, we may charge a reasonable fee to cover our costs. We will disclose the amount of such costs to you prior to providing you with the information.

We will take reasonable steps to ensure that the personal information that we collect, use or disclose is accurate, up-to date, complete and relevant. If you become aware, or believe, that any personal information which we hold about you is inaccurate or incomplete, you may contact us to correct the information.

If we disagree about the correction you have supplied, and refuse to correct the personal information, or if we believe that we are unable to comply with your request to access the personal information that you have provided us, we will give you a written notice to that effect. You have a right to make a complaint if you disagree with our decisions in relation to these matters (see below).

Complaints

If you believe that we have breached the APP or disagree with a decision that we have made in relation to our Privacy Policy, you may lodge a complaint with us. To enable us to understand and deal with your complaint in a timely fashion you should set out a brief description of your privacy problem, the reason for your complaint and what action or remedy you are seeking from us. Please address your complaint to our Privacy Officer. Contact details have been included below.

Your complaint will be considered by us through our Internal Complaints Resolution Process. We will acknowledge your complaint in writing and we will respond with a decision within 30 days of you making the complaint. If we need to investigate your complaint and require further time, we will work with you to agree to an appropriate timeframe to investigate. We will provide you with information concerning referring your complaint to the Office of the Australian Information Commissioner (OAIC) if we cannot resolve your complaint.

Policy updates

This policy is subject to change from time to time. The most current version of our Privacy Policy can be obtained from our website (www.knightcorp.insure) or by contacting us.

Contact details

Privacy Officer:	Wayde Knight or Maxine Baker
Address:	Level 7, 5 Mill Street, Perth WA 6000
Postal Address:	PO Box 7195, Cloisters Square PO WA 6850
Telephone:	1300 656 001
E-mail:	insurance@knightcorp.insure