Keystone Underwriting Pty Ltd
Privacy Policy

Commitment

Keystone Underwriting Australia Pty Ltd (Keystone) is committed to providing the highest levels of service. Keystone recognises that client privacy is very important. Privacy Amendment (Enhancing Privacy Protection) Act 2012 sets out a number of Australian Privacy Principles (APPs). Keystone's aim is to both support and ensure that Keystone comply with these principles. Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner at http://www.oaic.gov.au.

This policy discloses the purpose, and how personal information provided by clients and representatives, is collected, used, held, disclosed and disseminated.

Personal Information

Keystone is subject to certain legislative and regulatory requirements under s961B of the *Corporations Act* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* as a financial service provider. These require Keystone to obtain personal information about clients including:

- name, contact details, date of birth, tax file number
- information regarding client dependents and family commitments
- client occupation, and employment history
- client financial needs and objectives;
- client assets, liabilities, income, expenses insurances, and social security entitlements.

Collection of Personal Information

Keystone collects personal information from brokers and sometimes directly from clients or from third parties, once authorisation has been provided by the client. Clients have the right to refuse to authorise Keystone to collect such information from a third party.

Use of Personal Information

Primarily, client personal information is used in order to provide services to clients. Keystone may also use the information for purposes related to the primary purpose where it is reasonable for clients to expect the information to be disclosed.

From time to time, Keystone may provide direct marketing material. If, at any time, a client does not wish to receive this information any further, they may contact Keystone with this request. The client will be given the opportunity to "opt out" from receiving communications from Keystone or from third parties that send communications. The client may "opt out" from receiving these communications, such as newsletters, emails and other marketing and promotional materials, by clicking on an unsubscribe link at the end of an email. Keystone maintain details of the source of clients' personal information used for direct marketing and clients have the right to request these details. Keystone will endeavour to meet any requests within 2 weeks. Keystone maintains a Register for those individuals not wanting direct marketing material.

Disclosing Personal Information

Keystone may disclose personal information to the following organisations in line with modern business practices common to many financial institutions and to meet client specific needs:

- superannuation fund trustees, insurance providers, fund managers and other product providers in order to manage or administer a product or service;
- compliance consultants;
- mailing houses;
- insurance reference bureaus and loss adjusters;
- client professional advisers, including a client's solicitor or accountant as authorised by the client;
- information technology service providers;
- another authorised representative of Keystone if necessary;
- a potential purchaser/organisation involved in the proposed sale of Keystone for the purpose of due diligence, corporate re-organisation and transfer or all or part of the assets of Keystone's

business. 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;
- a new owner of Keystone that will require the transfer of client personal information;
- government and regulatory authorities, as required or authorised by law.

Keystone employees and the outsourcing companies/contractors are obliged to respect the confidentiality of any personal information held by Keystone.

The Corporations Act has provided the Australian Securities and Investments Commission with the authority to inspect certain personal information that is kept on Keystone's files about clients.

Keystone collects information about clients for the purpose of reporting to AUSTRAC under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Some of the recipients to whom Keystone discloses client personal information may be based overseas. It is not practicable to list every country in which such recipients are located, but it will include the United Kingdom.

Storage and Security of Personal Information
Keystone keeps personal information in client files electronically. These files are accessible to authorised personnel only, are appropriately secured, and are subject to confidentiality requirements.

Personal information is treated as confidential information and sensitive information is treated as highly confidential.

It is a legislative requirement that Keystone keep all personal information and records for a minimum period of seven years. Should a client cease to be a Keystone client, personal information of that client will be kept on or off site in a secure manner.

Ensuring Personal Information Is Correct
Keystone takes all reasonable precautions to ensure that the personal information collected, used and disclosed is accurate, complete and up-to-date. Keystone makes the following recommendations to clients to ensure this level of accuracy and completeness can be maintained:
- inform Keystone of any errors in personal information; and
- update Keystone with any changes to personal information as soon as possible.

Keystone may not be able to provide clients with the products or services being sought if clients provide inaccurate or incomplete information.

Unsolicited personal information
Keystone does not collect unsolicited personal information. Keystone will determine whether it would have been permissible to collect personal information if it is received and is unsolicited. Keystone will destroy or de-identify that personal information as soon as practicable if it is decided that collection would not have been permissible by law.

Access to Personal Information
Clients have a right to access personal information subject to certain exceptions allowed by law. Requests for access are required in writing (for security reasons). Access to the requested personal information may include providing the client with:
- copies;
- the opportunity for inspection; or
- a summary.

Keystone will disclose any charges applicable in providing access to clients prior to providing the information.

Some exceptions exist where Keystone will not provide access to client personal information if:
- providing access would pose a serious threat to the life or health of a person;
- providing access would have an unreasonable impact on the privacy of others;
- the request for access is frivolous or vexatious;

- the information is related to existing or anticipated legal proceedings between Keystone and the client and would not be discoverable in those proceedings;
- providing access would reveal Keystone's intentions in relation to negotiations with the client in such a way as to prejudice those negotiations;
- providing access would be unlawful;
- denying access is required or authorised by or under law;
- providing access would be likely to prejudice certain operations by or on behalf of an enforcement body or an enforcement body requests that access not be provided on the grounds of national security.

Keystone will provide the client with a written explanation access to personal information is refused.

Using Government Identifiers
Keystone does not use or disclose government identifiers other than when required or authorised by law or unless the client has voluntarily consented to disclose this information to any third party. There are certain circumstances where Keystone is required to collect government identifiers such as a tax file number, Medicare number or pension card number.

Dealing with Keystone Anonymously or Using a Pseudonym
Clients have the option to deal with Keystone by not identifying themselves or by using a pseudonym where it is lawful and practicable to do so, eg. calling to request Keystone's postal address.

Sensitive Information
Keystone will not collect information about clients without consent that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or affiliations, membership of professional or trade associations, membership of trade unions, details of health, disability, sexual orientation, or criminal record. Keystone will only use or disclose client sensitive information with client consent should direct marketing ever be undertaken. This is subject to some exceptions when:

- collection is required by law; and
- the information is necessary for the establishment, exercise or defence of a legal claim.

Website
The website for Keystone may provide links to third party websites. The use of client information by these third-party sites is not within Keystone's control and responsibility is not accepted for the conduct of these organisations. Other websites are not subject to Keystone's privacy standards. Clients will need to contact or review those websites directly to ascertain their privacy policies.

Clients may register with Keystone to receive newsletters and other information. Client names and email addresses will be collected and stored on Keystone's database by doing so. Keystone takes care to ensure that the personal information given on Keystone's website is protected, eg. the website has electronic security systems in place, including the use of firewalls and data encryption.

Clients need to email requests if they wish to update registration details or do not wish to receive any further information from Keystone. Keystone will endeavour to meet these requests within five working days.

Keystone's website may utilise cookies to provide users with a better experience. Cookies also allow Keystone to identify a client's browser while using the site – they do not identify the user. If a client does not wish to receive cookies, they can instruct their web browsers to refuse them.

Complaints Resolutions
Complaints about any breach or potential breach of client privacy rights need to go to Keystone's Privacy Officer. The Privacy Officer will investigate and determine the steps to be taken to resolve complaints. Keystone will contact complainants if additional information is required and will provide written notification of the determination of Keystone's Privacy Officer. If complainants are not satisfied with the outcome, they are entitled to contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

Privacy Officer
Neil Sheppard
104/266-268 Bay Road, Cheltenham, VIC 3192
T: 0457 762 233 E: neil@ksua.com.au