

PRIVACY POLICY – Corporate

Definitions

| | |
|----------------------------------|--|
| “ <i>Personal Information</i> ” | has the meaning given under the Privacy Act but, in short, means information or an opinion relating to an individual that can be used to identify that individual. |
| “ <i>Privacy Act</i> ” | means the Privacy Act 1988 (Cth) including the Australian Privacy Principles (as amended from time to time). |
| “ <i>Sensitive Information</i> ” | has the same meaning as under the Privacy Act. |
| “ <i>Services</i> ” | means the consultancy services of a commercial nature that we provide. |
| “ <i>Website</i> ” | means www.adelaideunicare.com.au and other websites and forms of social media where you post comments or we interact with you. |

The meaning of any general language is not restricted by any accompanying example and the words 'includes', 'including', 'such as', 'for example' or similar words are not words of limitation.

What Personal Information do we collect and why do we require it?

To provide you with our Services, we need to collect Personal Information. If any of the Personal Information you provide is incomplete or inaccurate, we may be unable to provide Services to you or the quality of those Services and the accuracy of the advice we provide may be compromised.

The nature of the relationship we have with you, the Services you require and the particulars of any matter in which we act will determine the personal and other information we collect. The personal information may include:

- your name, email address, telephone numbers and address;
- Personal Information (including Sensitive Information) which is provided to us in the course of a Consultancy Project by you or a third party;
- bank details, credit card details and expiry dates;
- information contained in a CV if you apply for a position with us; and
- information relating to the Services for which you have engaged us.

How do we collect Personal Information?

We aim to collect Personal Information directly from you, for example, when you send us information, during interviews and meetings with you, from business cards and during telephone calls.

We may also collect Personal Information:

- from parties to whom we refer you – e.g. other third party experts or professional advisors;
- from credit reporting and fraud checking agencies;
- from debt collection agencies if you default in a payment to us;
- through our Website and by other electronic communication channels (e.g. when you send us an email or post a comment on one of our blogs);
- from third parties, for example in the course of performing the Services for which you have engaged us;
- from publicly available sources of information; and
- when we are permitted or required to do so by law (including the Privacy Act).

How do we use your Personal Information?

We use the Personal Information we collect for the purpose of providing our Services.

We may also use the Personal Information:

- to comply with our contractual and other legal obligations;
- for insurance purposes;
- subject to you advising us otherwise (see Marketing below), to advise you of additional services or information which may be of interest to you; and
- otherwise as permitted under the Privacy Act.

If you default in a payment to us, we may use your Personal Information to recover that debt.

Marketing

We do not provide your personal information to any other person for marketing purposes.

From time to time, we may use your personal information to provide you with information about ourselves or to invite you to briefings or events we are holding. We do not, however, use Sensitive Information for this purpose.

If at any time you do not wish to receive any additional material from us, contact our Risk & Compliance Manager and we will remove your details from our marketing database.

Disclosing personal information

We may disclose your Personal Information to third parties in certain circumstances including:

- if you agree to the disclosure;
- when we use it for the purpose for which it was collected, e.g. to provide you with Services;
- in circumstances where you would reasonably expect information of that kind to be passed to a third party (e.g. where we are engaging with your approval & on your behalf a third party to assist in the provision of the Services for which you have engaged us);
- where disclosure is required or permitted by law (including under the Privacy Act), by court order, or is required to investigate suspected fraud or other unlawful activity; or
- if disclosure will prevent or lessen a serious or imminent threat to someone's life or health.

Disclosing personal information off-shore

We do not store personal information on off-shore servers or by way of cloud services.

In some matters, we may however be required to disclose personal information off-shore, for example, where the Services for which you have engaged us involves a transaction in another country or specialist advice is required from an overseas expert. In these circumstances you will be advised as part of the Services when and to whom personal information will be disclosed.

If information has to be disclosed overseas, the overseas recipient may not be subject to privacy obligations or to any principles similar to the rules of legal professional privilege or the Australian Privacy Principles.

An overseas recipient may also be subject to a foreign law that could compel disclosure of personal information to a third party, for example, an overseas government or regulatory authority.

If you consent to the disclosure in circumstances where we have informed you that we will not take any steps to ensure that the overseas recipient deals with your Personal Information in accordance with the Australian Privacy Principles and the overseas recipient handles the information in breach of the Australian Privacy Principles, you will not be able to seek redress under the Privacy Act, may not be able to seek redress in the overseas jurisdiction and we will not be accountable under the Privacy Act.

| | | | | |
|---------------|---|-----------------|------------|-------------|
| Document | Privacy Policy | Effective Date: | 06 07 2018 | Version 1.1 |
| Authorised by | Chief Executive Officer | Review Date: | 30 11 2020 | Page 2 of 4 |
| Warning | This process is uncontrolled when printed. The current version of this document is available on Adelaide Unicare website. | | | |

Considerations when you send information to us electronically

If you send an email to us, the information in your email (including any Personal Information) may be retained on our systems in accordance with applicable email retention policies and procedures.

While we do all we reasonably can to protect your Personal Information from misuse, loss, unauthorised access, modification or disclosure, including investing in security software, no data transfer over the Internet is 100% secure.

If you access another website from our website, you do so and provide personal information in accordance with the terms and conditions under which the provider of that website operates.

The open nature of the Internet is such that information exchanged via the internet may be accessed and used by people other than those for whom the data is intended. If you send us any information, including (without limitation) Personal Information, it is sent through the Internet or other electronic means at your own risk.

While we are not in a position to give you advice on internet security, if you provide Personal Information to us electronically, there are some things you can do which may help maintain the privacy of your information, including:

- always closing your browser when you have finished your session; and
- never providing Personal Information when using a public computer.

You should contact us immediately if you believe:

- someone has gained access to Personal Information you have provided to us;
- we have breached our privacy obligations or your privacy rights in any way; or
- you would like to discuss any issues about our privacy policy.

How we act to protect and retain your personal information

We endeavour to keep our information systems and files secured from unauthorised access. Those who work with us are aware of the legal obligations in respect to confidentiality and the importance we place on protecting your privacy.

Our procedures to securely store Personal Information include electronic and physical security measures, staff training and use of password protection software.

We retain our files for at least seven years after the matter has been completed and the file is closed. However, information filed in our electronic files may be retained indefinitely.

Personal Information may also be retained if we consider it necessary to do so or to comply with any applicable law or our insurance, governance obligations in our IT back-up records, for the collection of any monies owed and to resolve disputes.

Personal Information of Job Applicants

If you apply for a job with us, we will collect Personal Information about you. This will include contact information as well as information in your CV. Depending on the position applied for, we may also collect Sensitive Information about you including any previous criminal convictions.

We will collect Personal Information from you directly and may also collect Personal Information from third parties (for example referees or employment agencies) or from publicly available sources (such as social media sites). We will not collect Personal Information about you from someone else or from a publicly available source unless you have consented or we are legally permitted to do so.

We will only use or disclosure your Personal Information for the purpose of:

- considering your job application;
- creating an employment relationship with you (if your application is successful); or

| | | | | |
|---------------|---|-----------------|------------|-------------|
| Document | Privacy Policy | Effective Date: | 06 07 2018 | Version 1.1 |
| Authorised by | Chief Executive Officer | Review Date: | 30 11 2020 | Page 3 of 4 |
| Warning | This process is uncontrolled when printed. The current version of this document is available on Adelaide Unicare website. | | | |

- otherwise as permitted by law (including under the Privacy Act).

How you can update or correct your Personal Information

You may request access to your Personal Information or correct any inaccurate or out of date information by contacting our Risk & Compliance Officer using the details below. For security purposes, before we provide you with personal information, we may ask you to provide evidence of your identity.

You may request the source of any information we collect from a third party. We will provide this at no cost, unless under the Privacy Act or other law there is a reason for this information being withheld.

If there is a reason under the Privacy Act or other law for us not to provide you with information, we will give you a written notice of refusal setting out the reasons for the refusal except to the extent it would be unreasonable to do so and the mechanisms available to you to complain about the refusal.

How to complain if you believe we have breached the Australian Privacy Principles

If you believe that we have dealt with your personal information in a way that is inconsistent with the Australian Privacy Principles, you should contact our Risk & Compliance Manager in the first instance using the details below. If we are unable to resolve your complaint, you may contact the Office of the Australian Information Commissioner (contact details are below).

Changes to Privacy Policy

From time to time, it may be necessary for us to review and revise our Privacy Policy. We reserve the right to change our Privacy Policy at any time. Any changes to our policies will be notified to interested parties by posting an updated version of the policy document on our website.

Contact details

If you would like further information on our Privacy Policy or if you have any concerns over the protection of the information you have given to us or that we have collected from others, please contact our Risk & Compliance Manager and Privacy Officer at privacy@adelaideunicare.com.au.

More information about your rights and our obligations in respect to privacy and information on making a privacy complaint are available from the Office of the Australian Information Commissioner at:

Phone 1300 363 992
 Website www.oaic.gov.au
 Email enquiries@oaic.gov.au
 Write GPO Box 5218, Sydney NSW 2001

| | | | | |
|---------------|---|-----------------|------------|-------------|
| Document | Privacy Policy | Effective Date: | 06 07 2018 | Version 1.1 |
| Authorised by | Chief Executive Officer | Review Date: | 30 11 2020 | Page 4 of 4 |
| Warning | This process is uncontrolled when printed. The current version of this document is available on Adelaide Unicare website. | | | |