

PRIVACY POLICY



Policy Name: Privacy Policy
Implementation: Group
Policy Number: 1-004-002-000-21
Date: 23 April 2021

WHO THIS POLICY APPLIES TO: This Policy applies to all directors, officers and employees of Australian Country Choice ("ACC") Group, and all subsidiaries, contractors, secondees, consultants, agents and other individuals or entities that are effectively controlled by ACC Group or act on its behalf, either directly or indirectly ("ACC Personnel").

PURPOSE: ACC Group values the privacy of all its people, customers, suppliers and other parties it does business with, and recognises that the information we collect and hold is often sensitive.

This Policy explains how we collect, use, hold and disclose personal information, as well as ensuring the quality, integrity and security of personal information under applicable Privacy Laws.

1. DEFINITIONS

1.1 What is Personal Information?

"Personal information" includes any information or opinion, about an identified individual or an individual who can be reasonably identified from that information. The information or opinion will still be personal information whether it is true or not and regardless of whether we have kept a record of it.

Some examples of Personal Information may include:

- name, date of birth
- mailing or residential address details
- contact details such as telephone numbers, personal email address
- government issued identifiers such as Tax File Number, Medicare number, Driver's License number, Passport and/or visa/right to work documentation
- bank account details; and
- photograph, video or audio recording

1.2 Sensitive Personal Information

Some types of Personal Information are categorised as **Sensitive Personal Information**, recognising that this type of information is higher risk and needs to be handled with a higher level of confidentiality. ACC collects information from our employees, contractors and other parties such as:

- information relating to your health and well-being for WHS purposes
- biometric data
- criminal history and financial information during recruitment, and
- ethnicity data.

2. WHAT KINDS OF PERSONAL INFORMATION DOES ACC COLLECT AND HOLD?

The Personal Information that ACC collects is required for ACC to meet a range of obligations for employees and for workplace health and safety requirements for any person attending premises and in particular site locations.

If you do not allow ACC to collect all of the Personal Information we reasonably request, ACC may be unable to complete employment offers, or it may prevent you from being permitted entry to ACC business premises.

Throughout the time we are engaged in a business relationship, ACC may also collect and hold additional Personal Information about you. This could include information about insurance claims (workers compensation for example), collecting additional information to assess the claim, health and safety issues, changes to payroll records and/or superannuation records.

ACC's collection of Sensitive Personal Information is restricted to circumstances where ACC has obtained your express consent and to certain other permitted situations.

Generally, ACC only collects this sort of information where it is necessary for employment-related obligations (lawful collection under a State or Commonwealth law), or to enable you access to work premises in order to carry out lawful work instructions (biometric data).

3. HOW DO WE COLLECT PERSONAL INFORMATION?

ACC collects most personal information directly from you whether in person, on the phone or electronically, for example when you interact with ACC to:

- (a) apply for, register your interest in, or enquire about an employment or contract position;
- (b) complete employment information such as completing payroll information;
- (c) provide us with feedback or make a complaint or report under ACC Group policies;
- (d) visit our website; or
- (e) (for external parties) do business with us.

From time-to-time ACC collects Personal Information about you from third parties or organisations. This may arise in circumstances where you have given your consent to do so or where we notify you in our Privacy Notices or Collection Statements, such as when you make an insurance claim or amend payment information. Some examples of where we may collect Personal Information about you are:

- (a) ACC Group companies
- (b) publicly available sources of information, such as public registers
- (c) your representatives (including your legal or other professional advisers),
- (d) Client audit and compliance reviews; and
- (e) your superannuation fund Trustee.

We may disclose information we hold about you:

- to the Trustee of a superannuation fund to help in the management of our superannuation obligations for employees



- our insurers
- government bodies such as taxation, payroll, health and safety, and law enforcement agencies; and
- service providers, such as companies that provide reporting for insurance purposes, health care providers and others relevant to managing your health, safety and welfare.

4. DO WE COLLECT PERSONAL INFORMATION ELECTRONICALLY?

We may collect information from you electronically, for instance through internet browsing on our website.

Each time you visit our website, we may collect information about you which may include personal information (such personal information will be de-identified) and may include the following:

- the date and time of visits
- the pages viewed and your browsing behaviour
- how you navigate through the site and interact with pages (including fields completed in forms)
- general location information
- information about the device used to visit our website (including your tablet or mobile device) such as device IDs; and
- IP addresses. Your IP Address is a number that is automatically assigned to the device that you are using by your Internet Service Provider (ISP).

We collect information using cookies when you use our websites. Cookies are small pieces of information stored on your hard drive or in memory. One of the reasons for using cookies is to offer you increased security. They can also record information about your visit to our website, allowing us to remember you the next time you visit and provide a more meaningful experience.

We may also collect information from third party websites, applications or platforms containing our interactive content or that interface with our own website and applications.

We may collect personal information about you from social media platforms if you publicly comment but we will never ask you to supply personal information publicly over Facebook, Twitter or any other social media platform that we use.

5. PERSONAL INFORMATION ABOUT THIRD PARTIES.

If we receive personal information about you that we do not request directly from you or from another party, we will decide whether we could have collected the information in accordance with this Privacy Policy and applicable Privacy Laws.

If we decide that we could have collected the information in accordance with this Privacy Policy and applicable Privacy Laws, we will keep the information and handle it in accordance with this Privacy Policy and applicable Privacy Laws.



If we decide that we could not have collected the personal information in accordance with this Privacy Policy and applicable Privacy Laws, we will destroy or de-identify the information if it is lawful and reasonable to do so.

6. FOR WHAT PURPOSES DO WE COLLECT, HOLD, USE AND DISCLOSE PERSONAL INFORMATION?

The main reason we collect, use, hold and disclose personal information is to meet our obligations to you (including payroll, taxation and superannuation, WHS and insurance assistance) and to help us run our business.

We may also de-identify your personal information which we have collected for the purposes described in this Privacy Policy. As a result, this Privacy Policy will generally not apply to our use of de-identified information. However, we will continue to safeguard this de-identified information.

Where we use de-identified information together with other information (including personal information) and in doing so, we are able to identify you, that information will be treated as personal information in accordance with this Privacy Policy and applicable Privacy Laws.

We may use or disclose your information to comply with our legislative or regulatory requirements in any jurisdiction and to prevent fraud, criminal or other activity that may cause you, us or others harm including in relation to products or services.

6.1 What laws require or authorise us to collect personal information?

We are required or authorised to collect:

- certain identification information about you by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*;
- your Tax File Number, if you choose to provide it, by the *Income Tax Assessment Act 1936* (Cth);
- employment-related information such as name, date of birth, residential address, bank account information for payroll purposes by the *Fair Work Act 2009* (Cth)
- health and safety information by the *Safe Work Act 2008* (Cth), adopted in QLD on 1 January 2012.

These instruments work in conjunction with the *Privacy Act 1988* (Cth) (“**Privacy Act**”) and applicable Privacy Laws.

6.2 How do we hold and protect your personal information?

Much of the information we hold about you will be stored electronically. We may store some of your information in secure data centres that are located in Australia. We also store information through the data centres of our contracted service providers (including cloud storage providers), and some of these data centres may be located outside Australia. Some information we hold about you will be stored in paper files.

We use a range of physical, electronic and other security measures to protect the security, confidentiality and integrity of the personal information we hold both in Australia and overseas. For example:



- (a) access to our information systems is controlled through identity and access management controls
- (b) employees and our contracted service providers are bound by internal information security policies and are required to keep information secure
- (c) all employees are required to complete training about privacy and information security; and
- (d) we regularly monitor and review our compliance with internal policies and guidance issued by the OAIC on current practice.

Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure you should immediately contact our Privacy Officer.

We take reasonable steps to destroy or permanently de-identify any personal information after we no longer need to hold or use it for any purpose under this Privacy Policy.

6.3 Who do we disclose your personal information to, and why?

We may share your personal information with companies within the ACC Group.

We may also provide personal information about individuals to organisations outside the ACC Group who help deliver or support the provision of services to you. To protect personal information, we enter into contracts with our service providers and other third parties that require them to comply with applicable Privacy Laws and certain ACC Group policies and standards relating to data protection and information security. These contracts, amongst other things, require our service providers to only use the personal information we disclose to them for the specific role we ask them to perform.

Generally, we use contracted service providers to help us in our business activities. For example, they may help us provide you with services, deliver technology or other support for our business systems, or assist us with data analysis. These organisations may include:

- (a) our agents, contractors and contracted service providers (for example, mailing houses, technology service providers and cloud storage providers)
- (b) insurers, re-insurers and health care providers
- (c) payment systems operators
- (d) financial services organisations, including banks, superannuation funds, and contracted service providers
- (e) your representatives (such as your legal adviser or accountant)
- (f) fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct
- (g) external dispute resolution bodies; and
- (h) regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

We may also disclose your personal information to others outside the ACC Group where:

- (a) we are required or authorised by law or where we have a public duty to do so;



- (b) you may have expressly consented to the disclosure or your consent may be reasonably inferred from the circumstances; or
- (c) we are otherwise permitted to disclose the information under applicable Privacy Laws.

6.4 Do we disclose personal information overseas?

We may disclose your personal information to a recipient located outside Australia. This may include our contracted service providers operating overseas and organisations operating overseas with whom we partner to provide goods and services to you.

When we do disclose and/or store personal information overseas, we protect that information using the security measures set out above and require overseas recipients to do the same (see: How do we hold personal information).

6.5 Do we use or disclose personal information for marketing?

No, there is no marketing or other forms of promotional materials that we undertake as a business.

7. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION.

You can request access to the personal information we hold about you. You can also ask for corrections to be made. To do so, please contact the Privacy Officer or Human Resources.

Under Privacy Laws your right to receive access to your personal information, or make corrections to it, is not absolute and exceptions exist. For example, we are not required to give you access to your personal information where giving you access would pose a serious threat to any person's life, health or safety, or to public health or safety, where giving access would be unlawful, where giving access would have an unreasonable impact on other people's privacy or where we reasonably conclude your request is frivolous or vexatious.

If we refuse to give you access to or to correct your personal information, we will give you a notice explaining our reasons except where it would be unreasonable to do so. If we refuse your request to correct your personal information, you also have the right to request that a statement be associated with your personal information noting that you disagree with its accuracy.

If we refuse your request to access or correct your personal information, we will also provide you with information on how you can complain about the refusal.

8. NOTIFIABLE DATA BREACHES.

The Privacy Act includes a Notifiable Data Breaches (**NDB**) scheme which requires us to notify you and the Office of the Australian Information Commissioner (**OAIC**) of certain data breaches and recommend steps you can take to limit the impacts of a breach (for example, a password change).

The NDB scheme requires us to notify about a data breach that is likely to result in serious harm to affected individuals. There are exceptions where notification is not required, such as where we have already taken appropriate remedial action that removes the risk of serious harm to any individuals.

If we believe there has been a data breach that impacts your personal information and creates a likely risk of serious harm, we will notify you and the OAIC as soon as practicable



and keep in close contact with you about the nature of the breach, the steps we are taking and what you can do to reduce the impacts to your privacy.

If you believe that any personal information we hold about you has been impacted by a data breach, please contact the Privacy Officer or Human Resources.

9. RESOLVING YOUR PRIVACY CONCERNS AND COMPLAINTS – YOUR RIGHTS.

If you have a question or complaint about how your personal information is being handled by us, our affiliates or contracted service providers, please contact us first by contacting the Privacy Officer.

We will acknowledge your complaint as soon as we can after receipt of your complaint. We will let you know if we need any further information from you to resolve your complaint.

We aim to resolve complaints as quickly as possible. We strive to resolve complaints within five (5) business days, but some complaints may take longer to resolve. If your complaint is taking longer, we will let you know what is happening and a date by which you can reasonably expect a response.

ACC Group Privacy Officer – Contact Information
C/- ACC Group General Counsel
E: legalcounsel@accbeef.net.au
M: +61 447 772 120

Under the Privacy Act you may complain to the Office of the Australian Information Commissioner (**OAIC**) about the way we handle your personal information. Please note the OAIC requires any complaint must first be made to us (internal complaint process). The Privacy Act also allows 30 days for the respondent organisation to deal with the complaint before a person may make a complaint to the OAIC.

Office of Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Website: www.oaic.gov.au

10. POLICY AMENDMENT

This Policy cannot be amended or otherwise altered without approval of the ACC Board.

It will be reviewed periodically to ensure that it remains effective and meets current legal requirements, industry standards and the needs of ACC Group.

11. RELATED DOCUMENTS

- ACC Group - Surveillance Policy
- ACC Group - IT Security Policy
- ACC Group - Communications and Social Media Policy

(the balance of this page has been intentionally left blank)

PRIVACY POLICY



DOCUMENT CONTROL

Document Owner Group General Counsel

Signed:


Trevor Lee – Director

23 April 2021
Date

Version No.	Issue Date	Reason for Change
2.0	April 2021	New Policy