

We Want Your Wheels Privacy Policy

Your privacy is important to us. We are committed to ensuring the confidentiality and security of your personal information.

This Privacy Policy outlines how we collect, use, disclose and protect your personal information, as required by the Privacy Act 1988 (Cth) (Privacy Act). It also outlines how you can access and change your information, ask a question or make a complaint.

It applies to each of the entities within the John Hughes Group (Entities), which include: Rohanna Pty Ltd ATF The Skippers Unit Trust; Sovereign Credit Pty Ltd; SRAC Investments Pty Ltd, and all trading brands.

In this Privacy Policy, unless the context requires otherwise, a reference to 'we', 'us' or 'our' is a reference to the applicable Entity or trading brand you are dealing with from the above list. If we are providing finance or insurance products to you, please ensure that you read the parts of this Privacy Policy relating to credit information or sensitive information as relevant.

If we are providing finance or insurance products to you, please ensure that you read the parts of this Privacy Policy relating to credit information or sensitive information as relevant.

This Privacy Policy does not apply to our handling of personal information relating to employees or job applicants. Please contact us if you would like further details in relation to how we handle information of that nature.

1. Personal Information Policy

1.1 What is personal information?

Personal information is information or an opinion that identifies you as an individual or from which your identity can be reasonably identified (regardless of whether the information or opinion is true or not, or recorded in a material form or not). The types of information that constitutes personal information, and that we may collect, include your name, date of birth, address and other contact information, driver's licence number, employment details and financial information.

In addition, if we are providing finance or insurance products to you, then we may also collect additional types of personal information, as set out in Parts 2 and 3 of this Privacy Policy.

1.2 What is sensitive information?

Sensitive information is personal information that includes health information, racial or ethnic origin, criminal history, political affiliation and biometric information. In limited circumstances, we may collect sensitive information to assist you. For example:

- Health information (where this is relevant to an insurance policy, claim or if you are in financial difficulty and ask for hardship relief due to illness);

- Race or ethnicity (for example we may ask you what language you speak if you request a translator to communicate with us);
- Criminal history and political affiliation (where it is relevant to our regulatory and/or legal obligations); or
- Biometric information (where this information is collected and used for the purpose of automated biometric identification).

We will not collect sensitive information about you unless you consent to the collection and the information is directly related to our activities.

1.3 What is the purpose for collecting personal information?

We only collect personal information that is reasonably necessary for our business functions and activities. This may include using your personal information to process sales or any requests you may have, notify you of important changes to our services, comply with record keeping requirements, advise you of products and services that may interest you (unless you have declined to receive such communications in accordance with section 4 below) or to verify your identity.

We may also keep records of communications containing personal information (including recordings of telephone calls and emails) for the purpose of staff training.

If we do not collect your personal information, we may not be able to provide you with our products or services.

1.4 How do we collect information on our websites?

We can only collect personal information about you by lawful and fair means. We may collect information from you directly, such as when you complete an application form including an online application form, a contract or make an inquiry. We may also collect your personal information indirectly from third parties such as our related companies, introducers, finance and insurance companies or service providers.

We also obtain personal information through the use of website analytics tools, on where, when and how you use our products and services, and to authenticate your access to products and services from us and our service providers and agents.

If we receive personal information about you from someone else without having asked for it (whether from within the Group or from a third party), we will only continue to hold it if it is personal information that we could have collected from you ourselves, in accordance with this Privacy Policy. We will determine whether we could have collected the information ourselves, or if it is necessary for our business functions and activities, within a reasonable period of time after we have received it.

If it is personal information which is not reasonably necessary for our business functions and activities, or that we would not have obtained ourselves in accordance with this Privacy Policy, we will destroy or de-identify it as soon as it is practicable for us to do so.

1.5 Using and disclosing personal information

We only hold, use and disclose personal information about you for the purposes outlined in section 1.2, or for related purposes which might be reasonably expected, including for marketing and promotional purposes, and dealing with any complaints or claims.

To do this, we may disclose your personal information to Entities within the Group or third parties outside the Group who:

1. are service providers to the Group (such as lawyers, accountants and storage providers);
2. are regulatory bodies, government agencies, law enforcement bodies, courts and dispute resolution schemes;
3. introduce you to the Group (such as brokers);
4. are financiers, insurers or warranty providers;
5. are vehicle or parts manufacturers;
6. are your authorised agents, executors, administrators or legal representatives; or
7. are credit reporting bodies (CRBs) who may use this information to provide identity verification services.

We may also hold, use and disclose your personal information in connection with suspected fraud, misconduct and unlawful activity, and as part of acquisitions or potential acquisitions of or by our business.

If we are holding your personal information in connection with suspected fraud, misconduct or unlawful activity, we are not required to give you access to that personal information if we reasonably believe that such access would prejudice the taking of appropriate action in those circumstances.

On some occasions, we may be obliged to disclose your personal information by law, e.g. court order or statutory notices pursuant to any legislation, and to government authorities.

1.6 Government identifiers

If we collect government identifiers, such as your tax file number, we do not use or disclose this information other than as authorised by law. We will never use a government identifier in order to identify you.

1.7 Business without identifying you

In most circumstances it will be necessary for us to identify you in order to successfully do business with you. However, where it is lawful and practicable to do so, we will offer you the opportunity of doing business with us without providing us with your personal information, for example, if you make general inquiries about interest rates or current promotional offers.

2. Credit Information Policy

2.1 What is credit information?

Where we provide finance to you, we collect, hold, use and disclose certain credit information about individuals who are, or apply to be, customers for consumer credit, or guarantors for consumer or commercial credit. We may collect and hold any type of credit information about you as permitted by the Privacy Act and the Privacy (Credit Reporting) Code 2014.

We may collect this information directly from you, or from other third parties such as Credit Reporting Bodies (CRBs). The types of credit information we may collect include:

- identity particulars such as your name, gender, address (and previous addresses), date of birth, name of employer and driver's licence number;
- the fact that credit has been applied for with us and the amount and type of credit;
- details of other credit providers relevant to you;
- details of the start and end dates of credit granted to you and certain terms and conditions of your credit arrangements (such as repayment conditions);
- repayment history information (such as whether you have met payment obligations and the date of payment);
- more specific default information, including information about payments which are more than 60 days overdue, subsequent repayments or if you have entered into a new credit arrangement as a result of a default;
- confirmation of previous information requests to CRBs made by other credit providers, mortgage insurers and trade insurers;
- whether, in our or another credit provider's opinion, you have committed a serious credit infringement (e.g. acted fraudulently);
- the fact that credit provided to you has been paid or otherwise discharged;
- court proceedings information, personal insolvency information and credit-related publicly available information; and
- scores, ratings, summaries, evaluations and other publicly available information relating to credit worthiness, including personal insolvency information, which is derived by us or by CRBs wholly or partly on the basis of the information above and which indicates your eligibility for consumer credit (also called 'credit eligibility information').

Where we collect credit information from a CRB, we may use that information to produce our own assessments and ratings in respect of an individual's credit worthiness.

2.2 What is the purpose for collecting credit information?

We collect your credit information for the purpose of providing you with our credit services. This may include using your credit information to form decisions as to whether to provide you with credit or credit assistance or accept you as a guarantor, to confirm your identity, to manage and review your credit and to participate in the credit reporting system (where credit information is usually exchanged between credit providers and CRBs).

2.3 How do we collect credit information?

We collect credit information in the same way that we collect personal information, as outlined in section 1.3 above.

In addition, we may collect credit information from other credit providers, from CRBs or from the usage and repayment of any account you hold with us. If you are a guarantor, this may include obtaining from a CRB credit reports containing personal information about you and any other information deemed necessary to assess whether to accept you as a guarantor for the credit applied for or given to the applicant.

2.4 Using and disclosing credit information

We only hold, use and disclose your credit information for the purposes outlined in section 2.2, or for related purposes which might reasonably be expected, unless we otherwise obtain your consent. To do this, we may disclose your credit information to Entities within the Group, or third parties outside the Group including those who:

- are considering becoming a guarantor or a person considering offering property as security for the credit in order for them to determine whether to act as guarantor, or to keep that person informed about the guarantee;
- undertake debt collection in relation to the credit;
- are named in an application for credit or guarantee, such as your employer;
- are a transferee from us of the credit;
- are parties involved in loan securitisation arrangements;
- provide credit or other products to you or to whom an application has been made for those products;
- may want to market products to you (unless you have declined to receive such communications in accordance with section 4 below);
- are involved in managing or administering your finance such as third party suppliers, printing and postal services, call centres, trade insurers and CRBs;
- we are legally authorised to do so by law, such as under the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth), government and law enforcement agencies or regulators; or have an interest in your finance or our business.

Further, we may disclose your credit eligibility information to another credit provider in order to assess your credit application or a guarantor application, to help you avoid a default or to tell them of any default you may have had, but only with your consent.

2.5 Disclosure of credit information to CRBs

We may exchange your personal information with CRBs for purposes such as those described in section 2.2 or where the Privacy Act permits us to do so. For example, if you fail to meet your payment obligations in relation to consumer credit provided by us or if you commit a serious credit infringement, we may be entitled to disclose this to CRBs. We may also exchange other information, such as your identification details, what types of loans you have and how much

you have borrowed.

CRBs may include credit information provided by us in the reports given to other credit providers to assist them in assessing your credit worthiness.

We share credit information with the following CRB:

- Equifax Australia Information Services and Solutions Pty Ltd: www.equifax.com.au/contact-us

Additional obligations, privacy consents and notifications may also apply for our credit products. This Credit Reporting Policy is not intended to limit or exclude these provisions.

2.6 Opting out of CRB direct marketing pre-screenings

A CRB may use your credit reporting information to assist us to “pre-screen” you for direct marketing by us. If you do not want any of the CRBs listed above to use your information for the purpose of pre-screening, you have the right under the Privacy Act to contact them and request that they exclude you.

2.7 If you are a victim of fraud (including identity-related fraud)

You are entitled under the Privacy Act to request that a CRB not use or disclose credit reporting information they hold about you in circumstances where you reasonably believe that you have been, or are likely to be, a victim of fraud, including identity-related fraud. For a period of 21 days after the CRB receives your request the CRB is not permitted to use or disclose this information and this period is called a “ban period”. You can make such a request to the CRB listed above at 2.5. Requesting a ban period is free of charge.

3. Direct marketing

From time to time, we may use the personal information collected from you for direct marketing purposes, such as targeted advertising on new vehicles, maintenance, promotions, special offers and other information which we think you may find interesting. If we do contact you in this way, it will only be in relation to matters that customers would reasonably expect us to contact them directly about. We will ensure that our marketing activities comply with applicable laws.

We may contact you by telephone, email or SMS for these purposes.

Your personal information may be disclosed to other Entities within the Group, who may tailor marketing to you by combining personal information about you, which is held by those Entities with personal information we have disclosed.

If you do not wish to receive any direct marketing communications from us, you may at any time decline to receive such information by contacting us. You can also follow the instructions for unsubscribing in our direct marketing communications. We will not charge you for giving effect to your request and will take all reasonable steps to meet your request at the earliest possible opportunity.

We do not sell personal information to third party organisations to allow them to contact you for direct marketing purposes.

4. Disclosure of information overseas

We may disclose your personal information (which may include credit-related information) to overseas entities that provide support functions to us which may also include car manufacturers providing warranties. These are located in China, France, Germany, Japan, Korea, Malaysia and the United States of America. You may obtain more information about these entities by contacting us. When we do this, we make sure appropriate data handling and security arrangements are in place to ensure that the overseas recipient does not breach the Australian Privacy Principles.

5. Keeping personal information secure

5.1 Security

Your personal information (including your credit information and sensitive information) may be held by us in electronic form on our secure servers and may also be held in paper form. We may use cloud storage to store the personal information (including credit information and sensitive information) we hold about you. The security of your information is very important to us and we have security measures to protect any personal, credit or sensitive information that we hold.

Before disclosing personal information to a customer, we confirm the identity of that customer to prevent misuse or unlawful disclosure of the information.

We have security measures to ensure the physical security of personal information held on our premises and systems. When records containing personal information are no longer required, we delete the information or permanently de-identify it.

In relation to data stored or transmitted electronically, we regularly review developments in security and encryption technologies. Unfortunately, no data transmission over the internet can be guaranteed as completely secure. We take all reasonable steps to protect the information in our systems from misuse, interference, loss, and any unauthorised access, modification or disclosure.

We take reasonable steps to preserve the security of cookie and personal information in accordance with this policy. If your browser is suitably configured, it will advise you whether the information you are sending us will be secure (encrypted) or not secure (unencrypted).

5.2 Data breaches

A data breach occurs if personal information that the Group or its Entities hold is subject to unauthorised access or disclosure, or is lost. We will take all reasonable steps to prevent a data breach from occurring.

A data breach will be notified to you and the Australian Privacy Commissioner (Commissioner) if:

- There is unauthorised access to or disclosure of your personal information;
- The unauthorised disclosure is likely to result in serious harm to you; and
- We have been unable to prevent the likely risk of serious harm with remedial action.

We will also conduct an assessment if it is not clear if a suspected data breach meets the above criteria. The assessment will determine whether the data breach is an 'eligible data breach' that triggers notification obligations to you and to the Commissioner.

Once you are notified about a data breach that we have assessed as an eligible data breach, you are encouraged to take steps to reduce your risk of harm, through measures such as changing passwords and being alert to identity fraud or scams.

6. Access and correction of personal information

6.1 Access

You are entitled under the Privacy Act to access the personal information (including credit information and sensitive information) we hold about you and (provided that it is reasonable and practicable) to do so in a manner that you request.

We will need to validate the identity of anyone making an access request, to ensure that we do not provide your information to anyone who does not have the right to that information.

We will provide you access within 30 days if it is reasonable and practicable to do so, but in some circumstances it may take longer (for example, if we need to contact other entities to properly investigate your request).

There may be situations where we may refuse to provide you with access, such as where the information relates to existing or anticipated legal proceedings, if the request is vexatious or if the information is commercially sensitive. If access is refused, we will give you a notice explaining our decision to the extent practicable and your options to make a complaint.

We do not usually charge you for access to your personal information. However, if the request is complex, we may charge you the marginal cost of providing the access, such as staff costs of locating and collating information or copying costs.

6.2 Correction

If you feel that the personal information (including the credit information and sensitive information) we hold about you is incorrect, you are able to contact us at any time to request that we correct that information.

If you would like to do so please contact our Privacy Officer using the contact details in Part 8 below.

If appropriate we will correct the information at the time of the request. Where reasonable, and after our investigation, we will provide you with details about whether we have corrected the personal information. We may need to consult with other entities as a part of our investigation (including other credit providers or CRBs). We will normally try to resolve correction requests

within 30 days of you making a request.

There will be no cost to you if we correct your personal information held by us.

7. Complaints

If you believe that we have not complied with our obligations relating to your personal information (including your credit information and sensitive information), please contact our Privacy Officer as follows:

By phone: (08) 9415 0000 between 9am and 5pm Monday to Friday

By mail:

Privacy Officer

PO Box 273

Victoria Park WA 6979

By email: privacy@johnhughes.com.au

We will investigate your complaint and respond within 30 days with a proposed resolution.

If you feel we have not properly dealt with a complaint, you may contact the Office of the Australian Information Commissioner at enquiries@oaic.gov.au or on 1300 363 992.

8. Updates

We may review and amend this Privacy Policy from time to time to address changes to laws and to reflect our current operations and practices.

You can obtain a copy of the current version on request.

Last updated: July 2023