

# PRIVACY POLICY

**Last updated:** 12 June 2025

## 1. Introduction

This Privacy Policy (**policy**) explains how, we, Bilston Group Pty Ltd (ABN 71 679 894 396) or our associated entities listed at the end (each referred to as **we, our** or **us**), handle your personal information if you use or receive our services, if we contact you, if you visit us or otherwise interact with us online or offline.

This policy applies to our website visitors, platform users, clients, prospective clients, contractors, service providers, collaboration partners, government agencies, members of the public, or others who visit us or interact with us online or offline (each referred to as, **you, your**). This policy applies to you as an individual even if you act as a representative of an organisation (e.g. your employer).

This policy provides information only as required under data privacy laws and it is not intended, and must not be relied on, as a representation, warranty, contract, licence or an acknowledgement of a duty of care.

Our online properties may contain links to third party websites and features. We do not have any control over and are not responsible for those third party assets.

Please read this policy carefully. If you have any questions or if you do not understand anything explained in it, please contact Robert Payne using our [form](mailto:interest@bilstongroup.com.au) or by emailing to [interest@bilstongroup.com.au](mailto:interest@bilstongroup.com.au).

## 2. What is personal information?

**“Personal Information”** means information including an opinion, whether true or not and whether recorded in a material form or not, about an individual who is identified or reasonably identifiable. It does not include de-identified information where you are not reasonably identifiable, as determined in the circumstances.

Please see section 11 for the types of personal information we may collect about you.

## 3. How we collect your personal information

We collect personal information in a variety of ways, including:

<b>From you</b>	We collect personal information provided by you, when you visit us, speak with us, subscribe to our service, create a RAC Pro platform user account, apply to work with us, submit a query through the 'contact us' form on our website, contact us by email or telephone and in other situations.
<b>From third parties</b>	We collect personal information from third parties such as providers of background checks, third party used by you to login into our platform, recruiters, our associated entities, our partners and service providers, shareholders, advisors and other third parties.
<b>From the public domain</b>	Information we obtain from social media, official records and other public sources.
<b>From devices and systems</b>	From CCTV or other security devices when you visit our premises, from logs and records, and from your device or browser when you interact with our online properties and similar information.
<b>From cookies, pixels and similar technologies</b>	When you interact with us online, certain events or your online actions and behaviour online may be tracked by technologies in our online properties or your browser. For example, pixels sit on our website and load each time you visit. This event is recorded on our server and helps us count visitor numbers.

	Cookies are small files that store information on your device and enable us to recognise your device across different websites or browsing sessions, by logging your browsing history under a unique cookie ID assigned to your device.
--	---

We will rely on the information provided by you as accurate, complete and up to date, and we will be grateful if you would inform us of any changes without delay. Providing incorrect information to us could, among other things, prevent us from meaningfully responding to your enquiry or providing our services.

If you provide to us another person's personal information, please only do so if they would reasonably expect it or with their consent.

#### 4. Why we use and hold your personal information

We collect, hold, use and disclose your personal information for the following purposes:

Purpose	Personal information	How collected and held?	Consequences if not collected
<p>To <b>respond to your enquiry</b>, service request, data rights request, complaint or other communication.</p> <p>We may take steps to identify you by asking for your name and other details or checking your public profile, where this is necessary in the handling of your enquiry.</p> <p>We may record, transcribe and analyse our calls and other communications with you for service, compliance, training and development purposes.</p>	<ul style="list-style-type: none"> <li>• Communication records</li> <li>• Details of your enquiry</li> <li>• Identity details</li> <li>• Public data</li> </ul>	<p>From you, our records, our third party communication analysis tools, and from public sources. Information is held in our communication and case management systems.</p>	<p>Unable to efficiently and effectively assist with your enquiry without all necessary information and the use of communication analysis tools. Unable to ensure compliance and service improvement without appropriate records.</p>
<p>To <b>verify your identity</b> where reasonably required for our functions and activities, for example, we verify the identity of our clients, successful job applicants and others, for fraud-prevention, security and compliance reasons (for example, to comply with the AML/CTF Act).<sup>1</sup> Under data privacy laws, we must not use your government related identifiers, such as driver's licence or passport number, for any other purpose. Our third party ID verification solution compares your input data against various Government and private databases to produce a match score. Further, with your consent and upload of relevant data, our third party ID verification solution compares the biometric data derived from a photo or video of your face and the photo on your identity document to produce a match score. We will keep your government related identifiers, biometric data and other background data only until your identity has been sufficiently verified or background check passed, and as required by law.</p>	<ul style="list-style-type: none"> <li>• Background details</li> <li>• Identity details</li> <li>• Public data</li> <li>• Sensitive information (for example, biometric data derived from a photo of your face used for ID verification or your criminal records for background check purposes)</li> </ul>	<p>From you, public sources and from third parties which can verify your identity. Your information is held in our case management systems and third party ID verification and background check platforms.</p>	<p>You do not have provide your identity details or agree with our method of ID verification and we can explore alternative verification methods if you wish. However, any alternative ID verification may involve more time and information required from you. If we are unable to satisfactorily verify your identity or if you fail to pass our background checks, we will be unable to provide our services.</p>
<p>To <b>provide our advisory and review services</b> to our clients, for example, to ascertain relevant facts about you and relevant third parties, take your instructions, provide advice and guidance, manage assets, manage cases, introduce you to relevant third parties, liaise with third parties as</p>	<ul style="list-style-type: none"> <li>• Communication records</li> <li>• Details of your enquiry</li> <li>• Payment details</li> <li>• Sensitive information (for example, if your</li> </ul>	<p>From you, our records, public sources and third parties who provide information about you or provide</p>	<p>Unable to provide our services without all necessary information.</p>

<sup>1</sup> The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Purpose	Personal information	How collected and held?	Consequences if not collected
instructed by you or as anticipated as part of our services, to send you information about our services, seek payment for our services, and similar activities.	<ul style="list-style-type: none"> <li>instructions relate to matters involving health)</li> <li>• Service information</li> </ul>	services. Your information is held in our case management and other systems.	
<p>To <b>provide our digital platform</b> and similar services to our customers and users. Our users use our platform to import, hold and interrogate risk and other platform data, and to create risk assessments, reports, and other outputs.</p> <p>We do not use or access “platform data” except to provide our platform service. Our terms and conditions stipulate that each customer and user is responsible for complying with data privacy compliance obligations in relation to their platform data, including, for example, obtaining consent to handle your sensitive information on our platform or to respond to your data privacy rights requests in relation to your information included in platform data.</p> <p>If we are asked to provide services in relation to platform data with the customer or user’s permission, we will handle such “platform data” as “service information”.</p>	<ul style="list-style-type: none"> <li>• Platform data</li> <li>• Sensitive information (for example, if you use our platform to manage cases involving health, ethnic background, criminal history, etc.)</li> <li>• User details</li> </ul>	User details are inputted by the user when creating a user account and held on our systems. Platform data is uploaded by a user on behalf of the user or customer and held on our platform under the relevant customer/user account. We do not use platform data other than to provide our platform services.	You do not have to create a platform account or provide any information. However, to make the best use of our platform, data input will be required.
To provide our online services to you, such as our <b>website and online content</b> . For example, when you visit our website, your browser will provide certain technical information to enable us to display our content in a compatible manner. Some of our features allow you to input your information, for example, our contact us form.	<ul style="list-style-type: none"> <li>• Details of your enquiry</li> <li>• Device and browser data</li> </ul>	From you, your device and browser, cookies and similar technologies, data generated by our systems and from third parties, such as our technology providers. Your information is held in our internal systems and relevant third party systems.	Our systems automatically collect and provide information necessary to deliver our online services to your device. If you block cookies and similar technologies in your browser, some of our online services may be reduced.
To <b>send you relevant direct marketing communications and display ads</b> about our services, events, services of our associated entities, third-party services, collaborations, by email, text, post, display ads or other channels if we have an existing relationship or with your consent, where required by law. We will use profiling for personalisation and targeting, where appropriate, based on information known, observed or inferred from your activity or information about you provided by our third-party marketing and advertising partners. We use retargeting services which recognise your device or browser and display our ads to you on different websites you visit. We use technologies to track campaign performance.	<ul style="list-style-type: none"> <li>• Contact details</li> <li>• Device and browser data</li> <li>• Preferences and interests</li> <li>• Usage data</li> </ul>	From you, your device and browser, cookies and similar technologies, data generated by our systems and from third parties, such as our technology providers, marketing and advertising partners. Your information is held in our internal systems and on relevant third party partner platforms.	Unable to deliver direct marketing, targeted advertising and personalised communications without all necessary information. If you block cookies and similar technologies in your browser, our direct marketing may be less targeted or personalised.
To carry on <b>recruitment</b> of staff and contractors, for example, to assess your application, interview	<ul style="list-style-type: none"> <li>• Background details</li> </ul>	From you, your recruitment	Unable to identify candidates, make

Purpose	Personal information	How collected and held?	Consequences if not collected
you, assess your qualifications, experience and fitness for a particular role, conduct background checks (as above), make hiring decisions, discuss your terms of engagement and similar activities. We may use automated decision-making tools to eliminate applicants who fail to meet the basic criteria for a role. We use your identifier information only where reasonably necessary to verify your identity as part of recruitment. We will ask for your tax file number (TFN) to set up your “pay as you go” income tax withholding, <sup>2</sup> as appropriate. It is not an offence to choose not to provide your TFN, but this may prevent us from withholding the correct amounts of tax and you may be initially taxed more. We may only use your TFN as authorised under taxation law, personal assistance law or superannuation law.	<ul style="list-style-type: none"> <li>• Communication records</li> <li>• Details of your enquiry</li> <li>• Identity details</li> <li>• Recruitment details</li> <li>• Public data</li> <li>• Sensitive information (for example, where we wish to accommodate your needs on account of disability).</li> </ul>	agent, data generated by our systems, public sources, and third parties, such as persons providing a reference or testimonial about you. Your information is held in our internal systems, systems of third parties such as our service provider or recruitment agents.	hiring or engagement decisions, ensure correct tax deductions and manage our contactors without all necessary information.
To undertake <b>research, analytics, and diversity monitoring</b> , for example, service usage metrics, reviewing your Feedback, improving our services, quality assurance, market research, publishing statistical reports, business development, collaborating with third parties, sharing statistical research outputs, and other research.	<ul style="list-style-type: none"> <li>• Feedback</li> <li>• Usage data</li> <li>• All other de-identified information</li> </ul>	From you, our records, data generated by our systems, and third parties, such as our analytics partners and providers. Your information is held in our internal systems and on relevant third party partner platforms.	Unable to conduct research and development without all necessary data, often based on de-identified personal information.
To <b>administer our organisation</b> , for example, working with our associated entities, contacting and working with our partners, managing our service providers and our professional advisers, maintaining our technology stack, keeping and updating our records, collecting debt, resolving complaints, and similar activities. We may use our record management systems and engagement tools, identifying opportunities and contacting you.	<ul style="list-style-type: none"> <li>• All necessary personal information</li> </ul>	From you, our records, data generated by our systems, and from third parties, such as our service providers. Your information is held in our internal systems and on relevant third party systems.	Unable to perform certain tasks, provide services, administer our organisation, use our group’s corporate resources, and comply with the law without all relevant information and without engaging relevant third parties to handle your personal information on our behalf.
To maintain <b>health, safety and security</b> , for example, to manage incidents, investigations, to make reasonable health and safety adjustments to accommodate your health needs, to prevent imminent risk to health, make enquiries of our visitors where appropriate, deploy physical access control measures, and similar activities.	<ul style="list-style-type: none"> <li>• Details of your enquiry</li> <li>• Identity details</li> <li>• Monitoring data</li> <li>• Public data</li> <li>• Sensitive information (for example, injury details or where we act in a health emergency).</li> </ul>	From you, our records, our security devices, and third parties, such as your health practitioner, ambulance service, our building’s reception and security personnel.	Unable to make relevant risk assessment and take appropriate action without all necessary information. Unable to handle emergencies without using available and necessary information.

<sup>2</sup> Taxation Administration Act 1953 (Cth).

Purpose	Personal information	How collected and held?	Consequences if not collected
To <b>maintain information security</b> of our connected assets and online properties, for example, by monitoring use of our corporate resources, networks and website for suspicious activities, blocking access, isolating suspicious objects, preventing malicious software distribution and implementing other technical and organisational security measures to ensure the confidentiality, integrity and availability of information.	<ul style="list-style-type: none"> <li>Monitoring data</li> <li>Usage data</li> </ul>	From your device and browser, collected and generated by our systems, collected and generated by third party systems.	Unable to ensure information security without monitoring user and network activity and collecting relevant information.
To <b>comply with the law</b> , a binding decision or direction of a regulator, cooperate with a public authority, comply with mandatory disclosure, exercise legal rights and defend legal claims.	<ul style="list-style-type: none"> <li>All necessary personal information</li> </ul>	Collected from you, our records, third parties, and public sources.	Unable to comply with the law, exercise a right or defend a legal claim without the use and disclosure of your personal information.

We will update this policy to include any new purposes from time to time and we will obtain your prior consent for such new purposes where we are required to do so at law. We may not require your prior consent if the secondary purpose is related to our primary purpose and reasonably anticipated by you or otherwise authorised or required by law.

## 5. When we disclose your personal information

We may disclose your personal information on a need-to-know basis where authorised or required by law to:

- our employees, contractors and associated entities;
- your referrer, if you are referred to us by a person or organisation;
- your representative such as your lawyer, accountant, advisor or another third party acting for you or in your interest;
- your principal such as your employer when you engage with us in your professional capacity;
- a person, organisation or agency who can verify information about you or provided by you, where appropriate;
- other users who you collaborate with on our platform;
- where we are asked to provide services in relation to platform data, we may access it with your permission;
- other parties to a communication which you participate in;
- your third parties if they have a proper interest in the disclosure, such as, your colleagues, business partners, investors, etc.
- third party service providers who provide services to us, including IT, communications, office tools, marketing or advertising providers, analytics, payment services, professional advisors and others;
- third parties who provide certain services and information to us and collect and process your data, such as Google Analytics;
- anyone to whom our business or assets (or any part of them) are, or may (in good faith) be, transferred;
- your bank or payment provider, for example, in connection with your payment to us;
- auditors for our annual and ad hoc audits, as required by law or good practice;
- a requestor where it is reasonable in the circumstances to disclose your personal information in complying with a personal information access request;
- a third party in connection with a corporate transaction such as a merger of our organisation or an asset sale of our business as a going concern;
- courts, tribunals and regulatory authorities as required by law or to establish, exercise or defend our legal rights; and

- any other third parties as required or permitted by law, such as where we receive a subpoena.

We take reasonable steps to choose reliable service providers who hold your personal information on our behalf. Other than that, whilst we take reasonable steps to implement appropriate measures to safeguard your personal information in the hands of third parties, we are not responsible for third parties.

## 6. Disclosure of your personal information to overseas recipients

Your personal information may be transferred outside of the country in which you are located, for example, if we use a service provider, collaborate with third parties, seek advice in relation to an asset, or deal with a public authority located overseas, or in similar circumstances. This may include third parties in Australia, Europe, New Zealand, the United Kingdom or the United States.

When we disclose personal information to our recipients overseas, we take reasonable steps to ensure that each recipient will protect your personal information and handle it in accordance with the law. This may include entering into contractual arrangements with the recipient or satisfying ourselves that they are already subject to laws that offer equivalent protection of your personal information that you can enforce.

## 7. Data Retention

We will take such steps as are reasonable in the circumstances to destroy, anonymise or pseudonymise your personal information if no longer needed for our purposes, unless its continued retention is otherwise required by law.

By way of example, we may apply the following data retention periods, except where longer retention is necessary for a lawful purpose or required by law:

Type of information	Retention period
<b>CCTV records</b>	30 days from recording.
<b>Details of your enquiry</b>	6 months from resolution.
<b>Device and browser data</b>	6 months from resolution.
<b>Identifier Information</b>	Copies of ID documents are not retained after identity verification. The fact of ID verification and certain details may be retained on file until 7 years following end of relationship.
<b>Platform data</b>	Kept until the end of the user's or customer's access to our platform, as otherwise agreed in our service terms or deleted earlier as instructed by you.
<b>Recruitment details</b>	One year following unsuccessful application.

While we take reasonable steps to ensure information security, the transmission of information over the Internet is never completely secure, malicious actors constantly improve their attack vectors and human error cannot be completely ruled out. The transmission and exchange of information is carried out at your own risk.

## 8. Information security

We take reasonable steps and implement appropriate technical and organisational measures to protect your personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

While we take reasonable steps to ensure information security, the transmission of information over the Internet is never completely secure, malicious actors constantly improve their attack vectors and human error cannot be completely ruled out. The transmission and exchange of information is carried out at your own risk.

## 9. Your data rights and choices

Subject to certain conditions, exemptions and verification of your identity, as appropriate, you may have the following data privacy rights in respect of your personal information:

- **Right to information** as provided by us in this policy.
- **Right to remain anonymous**, unless this is unreasonable or impracticable in the circumstances.
- **Right to withdraw consent** at any time where our handling of your personal information is based on your consent.
- **Right to access** your personal information we hold about you, except for any platform data.
- **Right to correction** if you believe that any information (except for any platform data) we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading. We will take reasonable steps in the circumstances to ensure your personal information is accurate, up-to-date, complete, relevant and not misleading in the context of each relevant purpose.
- **Right to opt-out from marketing** by using the unsubscribe facility in our communications or by contacting us.
- **Right to know the source of marketing data.**
- **Right to remove your TFN** if you provided it for a purpose not connected with the operation of a taxation law, personal assistance law or superannuation law.
- **Right to complain** in accordance with our complaint's procedure explained below. If you are not satisfied with our response to a complaint, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

We are unable to comply with rights requests in relation to any platform data. You should contact the relevant responsible party in this regard.

Please contact us if you wish to exercise your rights. In most cases, we will be able to respond free of charge. We will take reasonable steps to process your request and respond within one month.

To protect all personal information held by us, we may require you to confirm your identity before resolving your request. If necessary, reasonable costs may be charged to you, where doing so is appropriate and lawful.

We may refuse requests on certain grounds, for example, if they are unreasonably repetitive, disproportionately demanding, impracticable or otherwise exempt or if refusing your request is appropriate and lawful in the circumstances. If we refuse your request, we will explain our lawful reason for doing so.

You can disable cookies and similar technologies through your internet browser. Alternatively, you could prevent some tracking by:

- turning off the automatic download feature in your browser to avoid tracking by pixels;
- applying your browser's do not track (DNT) feature, allowing you to opt out of all tracking, where DNT signals are recognised by our online property or our advertising partners;
- opting out from online interest-based advertising from companies that participate in public opt-out programs;
- enabling privacy controls on your browser to automatically send opt-out signals to sites indicating that you do not wish to share your data for targeted advertising; or
- opting out from Google Analytics or downloading the opt-out add-on and other third party services that deploy cookies and similar technologies.

Please be aware that if you opt-out of certain trackers, some or all of the functionality of our online services may be reduced. If you clear cookies in the browser on your device, the next time you visit our online services, cookies and similar technologies will be deployed again. However, you can prevent this by permanently blocking them in your browser.

## 10. Complaints

If you consider that we have breached your privacy, or you are not happy with the way we have handled your personal information, please contact us.

We will respond to you within a reasonable period of time to acknowledge your complaint and inform you of the next steps we will take in dealing with your complaint. We will endeavour to do so within 7 days of receipt and work with you to resolve your complaint without delay and generally within one month of receipt.

If you are not satisfied with our response, you may complain to the OAIC. If there are other government agencies, we consider you can complain to based on the nature of your complaint, we will inform you of this at the time we respond to your complaint.

## 11. What types of personal information do we collect?

<b>Background details</b>	Background check, references and similar information.
<b>Communication records</b>	A recording of your call or video conference with us, emails and other communications with us.
<b>Details of your enquiry</b>	Information in your enquiry, request for services, complaint, job application, data rights request and similar information.
<b>Device and browser data</b>	Device, browser and network information such as your browser, operating system, language, the domain name of your internet service provider, your IP address and similar information.
<b>Feedback</b>	Your feedback provided by you through online reviews, customer surveys, questionnaires and otherwise.
<b>Identity details</b>	Your name, contact details, including email address, street address and/or telephone number, date of birth, data and documents you provide to us for AML/CTF checks, your passport and other identification documents and government related identifiers and similar information.
<b>Monitoring data</b>	CCTV footage when you visit our premises, access records, usage data relating to your use of our website and other resources, communications metadata, social media activity and similar information.
<b>Payment details</b>	Your credit card, bank account and other payment details.
<b>Preferences and interests</b>	Details of programs or events that are of interest to you, your investment plans, preferences, opinions and similar information.
<b>Platform data</b>	Information held on our platform including data input and documents uploaded by you and outputs generated by our platform based on your input and similar information.
<b>Public data</b>	Information about you from social media, official records (e.g. electoral, postal, court, bankruptcy records, etc.) and similar information.
<b>Recruitment details</b>	Details from your application, employment history, qualifications, visa and/or employment status, tax file number, and any information we need to collect to onboard you, including background checks, information required by law and similar information.
<b>Sensitive information</b>	Information relating to your racial or ethnic origin, political opinions, religion, trade union or other professional associations or memberships, philosophical beliefs, sexual orientation or practices, criminal records, health information, biometric information (for example, if you choose our biometric ID verification comparing a photo of your face against the photo on your official document) and other sensitive information.
<b>Service information</b>	Your instructions, documents and information provided by you and third parties, case details, asset details, platform data which you grant us access to, and similar information.
<b>Usage data</b>	Information about your access and use of our online services collected through internet cookies or otherwise, your communications with our online services, your browser session, geo-location data, statistics on page views and sessions, acquisition sources, search queries, browsing behaviour, information collected from your use of applications, social media platforms and/or accounts that interact with our services and similar information.



<b>User details</b>	Your username, access credentials, use profile details and similar information.
---------------------	---

## **12. Changes to our Privacy Policy**

We may, at any time and at our discretion, vary this policy by publishing the amended policy on our website. We recommend you check our website regularly to ensure you are aware of our current policy.

## **13. Our associated companies**

RC Tech Solutions Pty Ltd ABN 70 687 526 941	Level 3, 175 Collins Street, Melbourne VIC 3000, Australia
---	---