Privacy and Data Protection Policy

RC Platform Pty Ltd

ACN 679 306 622

Table of Contents

1. Purpose 3
2. Our Mission and Values 3
3. Scope and Application 3
4. What Personal Information do we collect? 4
   4.1. Personal and Sensitive Information 4
   4.2. High Risk and Emerging Privacy Areas 4
5. How do we collect Personal Information? 5
6. How we use your Personal Information? 5
7. Use of Personal Information for Technology, Marketing and Analytics 6
8. Storage and Security of your Personal Information 6
   8.1. Security of your Personal Information 6
   8.2. Cloud-based Storage 7
   8.3. Overseas Data Disclosure 7
9. CCTV and Security Monitoring 7
10. Access to and Correction of Personal Information 7
11. Access To and Correction of Personal Information 8
12. Data Breaches 8
13. Complaints 8
14. Policy Review 9

1. Purpose

1.1. This Policy outlines how **RC Platform Pty Ltd** ("**Company**", **IPLiving**", "**we**", "**us**") manage personal and sensitive information of residents, employees, contractors, and others who engage with us, in compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Health Records Act 2001 (Vic).

1.2. We are committed to protecting the privacy of individuals and ensuring that their personal information is handled with care and transparency.

2. Our Mission and Values

2.1. Our Privacy Policy is grounded in IPLiving's C.A.R.E.S values and reflects our commitment to respecting and protecting personal information. By safeguarding the privacy of individuals, we create an environment where trust, accountability, and ethical responsibility are central to our operations.

- **C – Customer (Resident) First Mentality-** Respecting the privacy of residents, employees, and stakeholders is essential to maintaining trust. Protecting personal information safeguards their dignity, safety, and wellbeing across all communities**.**
- **A – Act With Integrity and Respect-** We handle personal information lawfully, transparently, and ethically. Integrity underpins our obligations to collect, use, store, and disclose information responsibly.
- **R – Responsible for Long-Term Sustainability-** Strong privacy practices reduce regulatory, operational, and reputational risk. Effective data governance strengthens compliance and supports sustainable, resilient communities**.**
- **E – Embrace Continuous Improvement-** We regularly review and refine our privacy controls in response to feedback, emerging risks, technological changes, and best-practice standards.
- **S – Strive to Be the Preferred Choice-** Demonstrating a commitment to confidentiality and responsible data management ensures IPLiving remains a trusted operator, employer, and partner in the retirement living sector**.**

2.2. Through this Policy, we affirm our mission to provide quality homes in supportive communities by ensuring that all IPL Personnel, residents, and stakeholders can be confident their personal information is protected, respected, and handled responsibly at all times.

3. Scope and Application

3.1. This Policy applies to:

a) All employees (employees and contractors);
b) Volunteers, students, and service providers;
c) Current, prospective, and former residents and their families or representatives;
d) Visitors and individuals engaging with our website or digital platforms.

3.2. "**You**" and "**Your**" in this Policy refer to any individual whose personal information we collect, hold or manage.

4. What Personal Information do we collect?

We collect personal information to provide high-quality care, ensure the effective operation of our community services, and meet our legal obligations under the *Privacy Act 1988 (Cth)*, the *Health Records Act 2001 (Vic)*, and the *Retirement Villages Act 1986 (Vic)*.

4.1. Personal and Sensitive Information

4.1.1. We may collect the following categories of personal information about you:

- Name, address, phone number and email address;
- Date of birth and gender;
- Next of kin or nominated representative;
- Residency or tenancy application information;
- Government-issued identifiers (e.g., Medicare, Centrelink, Pension or DVA numbers); and
- Information about your interactions with our website and digital systems (e.g., IP address, browser details, pages visited).

4.1.2. Sensitive Information, which is a sub-category of personal information under the Privacy Act, includes information or an opinion about your:

- Health condition, medical history, test results or disability status;
- Racial or ethnic origin;
- Religious beliefs or affiliations;
- Sexual orientation;
- Criminal history;
- Genetic or biometric information (if required for safety or identity verification purposes); and
- Financial information (e.g., bank account details).

4.1.3. Due to the nature of services provided in a retirement community setting, we are required to collect sensitive information to assess eligibility, deliver appropriate services to support safety and wellbeing of our residents, and fulfil our obligations under applicable health, and tenancy legislation.

4.1.4. Where reasonably possible, we collect sensitive information with your express consent. Where sensitive information is required for your safety or wellbeing and consent cannot be practically obtained (e.g., in an emergency or due to cognitive impairment), we will act in your best interests and in accordance with applicable privacy laws.

4.2. High Risk and Emerging Privacy Areas

4.2.1. In limited circumstances, we may collect or use sensitive information that presents a higher privacy risk, such as:

- Facial recognition or biometric data (e.g., for employee access or security);
- Geolocation tracking devices used temporarily to assist in locating a resident with cognitive impairment who is at risk of harm during an unexplained absence;

4.2.2. These high-risk activities are only undertaken:

- With your express consent, or
- Where there is a significant health and safety benefit, or
- After a **Privacy Impact Assessment** has been conducted (where applicable).

4.2.3. We prioritise the privacy, dignity and autonomy of all residents in such situations.

5. How do we collect Personal Information?

5.1. We may collect your personal information, including sensitive information, in a variety of ways, including directly from you or from third parties where it is necessary to provide our services, comply with our legal obligations, or carry out our business operations.

5.2. This may include collection from:

- Residents;
- Health practitioners and other healthcare providers or facilities involved in your safety and wellbeing;
- Family members, significant persons, or a responsible person acting on your behalf;
- Legal representatives who act on your instructions or are otherwise authorised; and
- Your interactions with our website, including your online behaviour (e.g., browsing activity, IP address, and cookies).

5.3. We may also collect personal information during the ordinary course of our business. This includes when forming business relationships, entering into service or supplier agreements, or recruiting employees or workers.

5.4. We will generally collect your personal information directly from you unless:

- You have given your consent for us to collect the information from another source;
- We are required or authorised by law to collect it from a third party;
- It is unreasonable or impracticable to collect it directly from you; or
- The collection is fair and reasonably expected as part of our core functions and activities.

5.5. Once you have provided your consent to the collection of your personal or sensitive information, you may withdraw it at any time by contacting us. Please note that if you choose to withdraw your consent, we may be unable to continue providing certain services to you

6. How we use your Personal Information?

6.1. We will only use your personal information in ways that a reasonable person would consider are fair and reasonable for a business of our type. For residents, we may use your personal information:

- Assess eligibility for residency;
- Provide accommodation, services, and support;
- Liaise with family members or nominated representatives;

- Manage safety, security and emergency responses;
- Comply with applicable laws and reporting obligations;
- Conduct internal quality assurance and continuous improvement;
- Coordinate with allied health professionals and medical practitioners;
- Assess an application for employment with us;
- Administer contracts, employee records, or tenancy matters;
- Conduct anonymised research or reporting in the public interest.

7. Use of Personal Information for Technology, Marketing and Analytics

7.1. We acknowledge the growing role of technology, including artificial intelligence (AI), in both business operations and the delivery of health care. We may use such tools to analyse data in order to enhance the quality of care and services we provide. However, we do not use AI or other technologies to make automated decisions that would affect your rights without human involvement.

7.2. We may use your personal information, including information about your interactions with our digital platforms (such as browsing activity), for the following purposes:

- **Direct marketing**, such as email or SMS communications about services we believe may be of interest to you. You may opt out of receiving these communications at any time.
- **Personalised content delivery**, including tailoring the information you see online to your preferences or past behaviour. We believe this enhances the relevance and accessibility of our services.
- **Targeted online advertising** related to our core business activities. We may use your personal information to help us create and deliver advertising that is more relevant to your needs or interests. In doing so, we aim to ensure that the use of your personal information remains fair, proportionate, and beneficial to you.

7.3. We will never sell or trade your personal information to third parties.

8. Storage and Security of your Personal Information

8.1. Security of your Personal Information

8.1.1. We are committed to protecting the privacy and security of your personal information. We take reasonable steps to ensure that all personal information We collect, use, and hold is protected against misuse, interference, loss, and unauthorised access, modification, or disclosure.

8.1.2. Personal information is stored in both physical and electronic formats, including secure databases, cloud-based platforms, and on-premises systems. Access to such information is restricted to authorised personnel who are required to maintain confidentiality.

8.1.3. Non-current personal information is securely archived in accordance with privacy and health record laws.

8.2. Cloud-based Storage

8.2.1. We may utilise secure cloud-based systems to store some of the personal information we collect. Where cloud services are provided by third-party vendors, we take all reasonable steps to ensure these providers comply with applicable Privacy Laws and our internal security standards.

8.3. Overseas Data Disclosure

8.3.1. While we aim to store personal information in Australia wherever possible, certain service providers may operate or store data outside Australia, particularly where cloud-based systems are used.

8.3.2. Where personal information is likely to be disclosed to or accessed by an overseas recipient, we will take reasonable steps to ensure that the overseas recipient protects your personal information in a manner consistent with **Australian Privacy Laws**.

8.3.3. Wherever possible, we seek to work with providers located in countries with privacy protections substantially similar to those under the Australian law.

9. CCTV and Security Monitoring

9.1. We operate CCTV surveillance systems in public and common areas at some of our community facilities and other business premises. The purpose of CCTV surveillance is to support the safety, security and wellbeing of our residents, employees, contractors, visitors, and other individuals on our premises.

9.2. CCTV footage may incidentally capture personal information. Where this occurs, such information is handled in accordance with this Privacy Policy and applicable Privacy Laws. Recorded footage is stored securely and is accessible only to authorised personnel.

9.3. In limited circumstances, CCTV recordings may be disclosed to third parties, such as law enforcement agencies or regulatory authorities, where required or authorised by law, including for the purpose of investigating or managing incidents.

10. Access to and Correction of Personal Information

10.1. You have the right to request access to the personal information we hold about you and to request its correction if you believe it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

10.2. If you make a request, we will:

- provide access to the personal information we hold about you, unless an exception applies under applicable privacy laws;
- identify, where possible, the source of that personal information;
- explain or summarise how your personal information has been used or disclosed;
- consult with you about the preferred format of our response; and
- apply a nominal administrative fee for processing the request, at our discretion (you will be notified of any fees in advance).

10.3. To make a request, you may contact us using the details set out in **Section 12** of this Policy. You may also choose to complete a **Request For Access to Personal Information Form** or a **Request**

For Information – Deceased Person Form, where applicable. we will require acceptable proof of identity before responding to your request.

10.4. If we agree that the information should be corrected, we will take reasonable steps to do so promptly.

10.5. In some cases, you may also request that we delete your personal information. We will consider such requests in line with our legal obligations. Where we are unable to delete information (for example, where retention is required by law), we will explain the reasons for this.

11. Access To and Correction of Personal Information

11.1. You may withdraw consent to the collection or use of your personal or sensitive information by contacting us. We will advise you of any consequences of withdrawing consent, particularly if it affects our ability to provide services

12. Data Breaches

12.1. We are committed to protecting the personal information We hold and ensuring compliance with the Australian Privacy Principles (**APPs**) under the Privacy Act 1988 (Cth).

12.2. Despite our best efforts, if you become aware of any interference with your privacy that you believe originated from us, we encourage you to notify us as soon as possible using the contact details below. The sooner we are informed, the better our ability to assess, contain, and respond to the issue, and to minimise any potential impact on you.

12.3. We maintain a **Data Breach Response Plan** that outlines how we respond to actual or suspected data breaches involving personal information, including lost, stolen, or unauthorised access or disclosure.

12.4. In the event of a data breach that is likely to result in serious harm and meets the threshold of a Notifiable Data Breach (as defined under the Privacy Act), we will:

- promptly assess the breach and take steps to contain it;
- notify our Board and the affected individuals as soon as practicable; and
- notify the **Office of the Australian Information Commissioner (OAIC)** in accordance with our legal obligations.

12.5. We will also take all reasonable steps to mitigate any ongoing risk and will keep a record of the breach in accordance with our obligations.

12.6. If a data breach does not meet the threshold for mandatory notification, we may still take steps to inform affected individuals and support them in reducing any potential harm, where appropriate.

12.7. All data breaches (regardless of the threshold for mandatory reporting) are escalated and reported to our Board.

13. Complaints

13.1. If you have a complaint about a suspected breach of the APPs or other privacy complaint, then you should put your complaint in writing and send it to our Privacy Officer.

Privacy Officer

Address: Suite 105, 9-11 Claremont St, South Yarra VIC 3141
Email: kharman@ipliving.com.au
Telephone: (03) 8825 7600

13.2. We will review and respond to your complaint within a reasonable timeframe in accordance with legislative requirements.

13.3. If you are dissatisfied with the handling or outcome of your complaint or request, you may directly contact the following:

Office of the Australian Information Commissioner.

Post: GPO Box 5218, Sydney NSW 2001

Email: enquiries@oaic.gov.au

Telephone: 1300 363 992

Online: OAIC Web Form

14. Policy Review

14.1. This Policy will be reviewed by the Board at least once **every two years** to ensure it remains effective and meets the best practice, and the Company's needs.

14.2. The Policy will be available on the Company's website within a reasonable time after any such updates or amendments have been approved

Approved by the Board XX on: [Insert Date]

Next Review Date: [Insert Date]

Policy Owner: Group General Counsel