PRIVACY POLICY

When does this policy apply?

This policy outlines the principles that TLCo Pty Ltd (**The Living Company**) and its related companies and businesses, including Scape, RTLCo and Aveo (collectively **we**, **us** or **our**) adopt in the conduct of our business to manage and protect your personal information.

Several of our subsidiaries engage in activities under other brands. You can contact The Living Company's Privacy Officer to obtain details of our subsidiaries that this policy also applies to. You can obtain a copy of the most current version of this policy from our website at thelivingcompany.com.au or by contacting our Privacy Officer.

What does this policy deal with?

This policy deals with our collection, use and disclosure of your personal information, including how you can access and correct it, if required.

We are committed to protecting your privacy by maintaining a safe and secure system of handling your personal information. We aim to ensure that your personal information is handled in compliance with the Australian Privacy Principles (**APPs**) which are part of the *Privacy Act 1988* (Cth) (**Privacy Act**) and other relevant laws.

This policy also applies to the collection and processing of your personal information if you are an individual in a country that is a member of the European Economic Area by or on behalf of The Living Company, to the extent the General Data Protection Regulation (EU) 2016/679 (**GDPR**) applies. For information about your rights under the GDPR and how to exercise them, please see the 'Your rights under the GDPR' section below.

What is personal information?

Personal information for the purposes of this policy is information or an opinion (whether true or not and whether recorded in a material form or not) about an individual who is identified or who is reasonably identifiable from the information or opinion.

What personal information do we collect and hold?

We collect personal information to the extent that is reasonably necessary to conduct our business. The personal information that we collect, and hold depends upon the nature of our interaction with you. For example, whether you are a resident, employee, contractor or visitor to one of our properties.

In general, the personal information we may collect can include your:

- personal details (e.g. your name, gender, date of birth, contact details (including email), emergency contacts)
- identification documents, including driver's licence, passport and student identification
- your image, including via our use of CCTV in our communities and workplaces
- Medicare, pension or other concession details, private heath fund details
- employment history and educational qualifications (e.g. for prospective employees), course enrolment and visa status information
- bank account, credit card details and direct debit authorities
- details relevant to your dealings with us and/or the services we provide
- any other information needed to assist us in conducting our business.

For example, when you apply to live in one of our communities, receive services from us, or apply for a role with us, we will collect, hold and use information about you. This may include sensitive information if we are required to collect such information for the purpose of either delivering services to you, employing you or engaging with you as a contractor (as the case may be).

In most cases, the information is collected in a written or electronic application form that we will ask you to complete. Initially we may use your personal information to consider your eligibility to live in one of our communities, or to receive services from us. If you do not provide this information to us, we may not be able to consider your application or we may not be able to provide you with some or all of the services.

We may also:

- collect personal information from you on an ongoing basis for the purpose of providing services to you or for the administration of our buildings
- hold personal information that you provide to us about other individuals (e.g. personal information about your spouse, partner, parent, guardian, friend, referee, emergency contact or someone living with you). We rely on you as our customer to inform those individuals that their personal information is being provided to us, and that they may contact us for further information.

Sensitive Information

To provide you with our services or employ you (as the case may be), we may be required to collect and handle your sensitive information. This can include:

- health information (e.g. medical history, test results, advance care wishes and health assessments) where we provide care services to you
- information about your religion, ethnicity, sexual preferences, gender identity or political opinions
- criminal records or working with children checks (e.g. for employees, contractors and

volunteers).

If we are required to collect sensitive information in respect of you, we will only do so with your consent and ensure that our handling, storage and disclosure of your sensitive information occurs with appropriate controls. Consent will generally be obtained through a written or electronic consent form at the time of collection, or (in care settings) through a verbal consent process documented by our staff. Where a resident lacks capacity to consent, we will seek consent from their authorised representative, guardian, or attorney.

Health and care information – Aveo residents

If you are a resident of an Aveo community, we may collect and hold health and care information about you in order to provide, coordinate, or arrange care and support services. This may include medical history, health assessments, advance care wishes, functional assessments, medication details, and information about your care needs provided by health professionals, family members, or legal representatives.

We handle this information with appropriate care which may include the following protections:

- **Consent**: We only collect health and care information with your consent (which may be express or implied), except where collection is required or authorised by law.
- **Access**: Access to your health and care information is limited to staff and service providers who need it to deliver, enable or coordinate your care.
- **Storage**: Health and care information is stored in systems with controls appropriate to its sensitivity.
- **Correction**: You, or your authorised representative, may request access to or correction of your health and care information by contacting the management team at your community or our Privacy Officer.
- **Your representative**: If you have appointed a family member, guardian, or attorney to act on your behalf, we will work with that person to ensure your privacy rights are respected and your preferences are followed.

If you have questions about how your health or care information is managed at your Aveo community, please contact the Community Manager or our Privacy Officer.

How do we collect personal information?

We generally will collect your personal information directly from you, however it may also be collected via:

- records of our other communications and interactions with you
- our customer survey or market research activities
- the marketing of our products and services
- our websites and Apps (including information you enter in our website and Apps)
- other third parties such as a report provided by a medical professional or an employment reference in respect of prospective employees; and

- publicly available sources.

From time to time, we may also collect information about you from someone that is appointed as your personal representative (such as a family member nominated by you), guardian, attorney or another legal representative. We ask you to keep informed of any nominations or appointments in this respect.

What do we do in a pandemic or emergency response?

We may need to collect personal information from various people (including residents, occupants, employees, contractors and visitors) to prevent or manage a pandemic or other type of emergency response at our communities and our workplaces.

Where relevant and in line with recommended practices by the Australian Government, this may include information needed to identify risk and implement appropriate controls to prevent or manage a pandemic or other emergency. Only the minimum amount of personal information reasonably necessary to prevent or manage a pandemic or other emergency will be collected, used or disclosed.

Our use of cookies

A cookie is a small data file that may be stored on the computer of a web user (usually in the browser software folder) the first time the user accesses a website operating cookies. Cookies are necessary to facilitate online transactions and ensure security.

Cookies do not in themselves identify you as an individual, although they do identify your browser type, the operating system you are using, the web page you visited, your internet service provider and your location. You can configure your internet browser to accept all cookies, reject all cookies or notify you when a cookie is sent.

Our website and Apps include pages that use cookies. This allows our servers to recognise your device when you visit our website or App in the future. If you refuse to use cookies in this way you may not be able to see the full functionality of our website or App that you are using. Please refer to your internet browser's instructions or help screens to learn more about these functions. We use two categories of cookies: (a) strictly necessary cookies, which are required for our websites and Apps to function and cannot be disabled; and (b) analytics and performance cookies, which help us understand how visitors use our sites and may include third-party tools such as Google Analytics. Where required by law, we will seek your consent before placing non-essential cookies on your device. You may withdraw your consent at any time by adjusting your cookie preferences via the cookie settings tool on our website.

Using our website and Apps

We collect the personal information that you enter on our websites and Apps. This may

include personal information about you when you interact with us online or via an App (including when you visit other The Living Company websites or Apps) or when you mention one of our brand names (i.e. Scape or Aveo) or our products via external social media platforms (e.g. Facebook or X (formerly Twitter)). Any personal information that we may collect from social media platforms is determined by the privacy settings of your account within the social media platform (that is, the extent to which your personal information is publicly available on the social media platform) and the content of your post.

Our use of camera surveillance

We may carry out camera surveillance in our buildings, communities or commercial offices to enhance safety, particularly the safety of residents, workers, contractors and visitors.

Camera surveillance will be signed where it is carried out and residents, their visitors, and our workers and contractors will be notified of the installation of surveillance cameras prior to their installation. These surveillance systems may collect personal information, such as your image.

Why do we collect, hold, use and disclose personal information?

We collect, hold, use and disclose your personal information for the primary purposes for which it was collected. The reasons and the parties to whom we might disclose it will be reasonably apparent to you when we collect your information. Generally, primary purposes include:

- conducting our businesses (such as providing accommodation to you), including providing, developing and improving our services
- assessing your application for our services, communicating with you including facilitating responses to your enquiries
- communicating with you via an App
- verifying your identity, address and other details
- contracting with you and processing payments
- conducting debt recovery activities (including through a debt collection agency)
- conducting customer surveys
- gathering and aggregating information for statistical and modelling purposes, including customer segmentation processes
- managing performance and compliance with our contractual and regulatory obligations and assessing that compliance through independent audits
- maintaining and updating our records
- contacting you to obtain your feedback or comments on our products and services
- facilitating acquisitions and potential acquisitions of our businesses.

If you are a resident and reasonable efforts to recover outstanding amounts owed by you have been unsuccessful, we may disclose information regarding your rental default to residential

tenancy databases (if relevant) and/or debt collection agencies.

We also use your personal information to provide you with information on products and services that we or third parties offer, as well as offers, competitions and other marketing information that we consider may be relevant to you or that you might be interested in, even after you cease acquiring products or services from us. If you use an App owned or operated by us, this may include push notifications to tell you about offers, events, updates and our products and services that may be of interest to you. You can tell us if you do not want to receive such information by contacting our Privacy Officer. Subject to the configuration options available on your device, you may also decline marketing messaging sent by push notifications by refusing the relevant permissions in your device settings, however this may also prevent you from receiving updates via push notifications on the Scape App.

We may use and disclose your personal information for other purposes which you consent to or which are required, permitted or authorised by or under law.

How do we hold and keep secure personal information?

We will hold your personal information we collect by a combination of physical records and electronic storage, which may be through third party service providers. Images recorded by camera surveillance are stored as digital files within the camera surveillance software for a limited period after which they usually will be deleted unless required in certain circumstances (e.g. in respect of an investigation).

We take steps in accordance with law to protect the personal information we hold about you from misuse, loss, interference, theft and from unauthorised access, modification or disclosure both physically and through computer security methods. We will keep your personal information for no longer than is reasonably necessary for the purpose for which it was collected, or as required or permitted by law. Retention periods vary depending on the type of information and our relationship with you. A summary of our standard retention periods is available on request from our Privacy Officer. We will take reasonable steps to destroy or permanently de-identify the information if it is no longer needed for any purpose and we are not required by law to retain the information.

In what situations might we disclose personal information?

We may disclose personal information (including, in certain circumstances, sensitive information) to third parties that help us provide services to you as our resident or for us to employee or otherwise engage with you. Third parties that we may disclose your personal information to include:

- your authorised representative, guardian or lawfully appointed attorney under a power of attorney you have provided to us
- businesses involved in providing, managing or administering our services or providing services to us at our communities (including for example, our software and IT providers,

suppliers, contractors and agents)

- If relevant to our services to you, medical and health professionals, hospitals and aged care operators
- financial institutions for payment processing and billing activities, credit providers and
- our related entities, including subsidiaries and partners, including third party operators of residential tenancy databases and debt collection agencies).
- Government agencies, regulatory authorities or enforcement bodies (e.g. Australian Federal Police) where required or authorised by law (for example bond authorities)
- our insurers and professional advisers, including independent auditors, accountants, lawyers and asset managers
- any person or organisation to which you have consented, or we are required, permitted or authorised by or under law to disclose.

If we do provide third parties with your personal information, we will only do so on the basis that the third party is contractually bound to comply with this policy, the Australian privacy laws in respect of the handling and processing of your personal information.

Transferring and storing your personal information outside Australia

Where it is practicable or we are otherwise legally required to do so, we hold personal information we collect on electronic databases located in Australia.

Where we are legally permitted to do so, we may disclose personal information to our international network of companies under the Living Company name (**Members Companies**) and other entities overseas where it is reasonably necessary to help us fulfil the purpose for which the personal information was collected, or for a related or ancillary purpose or otherwise in accordance with the Privacy Act and, where relevant, the GDPR. The countries to which such disclosures are made, and types of personal information disclosed, depend on the specific circumstances of the engagement.

Where we can do so by law, we may also store, process or back-up your personal information on secure servers that are located overseas (including through third party service providers, as legally permitted). These servers are located in the United Kingdom, United States, Japan, the Philippines, New Zealand and Singapore.

Where we transfer personal information between countries, we will only do so with reasonable protections in place, to ensure your personal information is protected in accordance with applicable laws and this policy. At a minimum, we will take reasonable steps to ensure any third parties who process your personal information overseas are contractually bound to comply with this policy and the Australian privacy laws (including the Australian Privacy Principles).

Our use of artificial intelligence and automated decision-making

We may use artificial intelligence (**AI**) tools and automated systems in a number of ways

across our business. Where these tools involve processing your personal information, we take reasonable steps to ensure that use is consistent with the purpose for which your information was collected and compliant with applicable privacy laws.

Current uses of AI and automated decision-making that may involve your personal information include:

- Resident and customer service: We use AI-assisted tools (including chatbots and virtual assistants) to respond to enquiries, process service requests, and personalise your experience. Where you interact with an AI tool, we will take reasonable steps to make this clear to you at the start of the interaction.
- Recruitment: We may use AI-assisted tools to process employment applications, including screening resumes and assessing candidate information. Where a significant decision about your application is made using automated processing, you may request that a human review that decision. To make such a request, contact our Privacy Officer.
- Analytics and business operations: We use data analytics tools – which may incorporate AI – to analyse usage patterns, assess service performance, and support business planning. Where possible, this analysis is performed on aggregated or de-identified data.

Where AI processing involves sub-processors located overseas (including in the United States), we will take reasonable steps to ensure those processors are contractually bound to handle your personal information in accordance with Australian privacy laws and, where applicable, the GDPR.

Regardless of where you are located, if you believe a significant decision has been made about you based solely on automated processing and you wish to request human review, please contact our Privacy Officer. To the extent we are subject to the GDPR, you may have additional rights under Article 22 in relation to automated decision-making.

Marketing

We may use or disclose your personal information to send you about our products and services which may be of interest to you (except if sensitive information, we will only do so with your consent), but we respect your right to ask us not to do this.

If you no longer wish to receive those sorts of communications from us, you should click the unsubscribe link in any marketing email, send a message through the contact feature on our website or by contacting our Privacy Officer and we will ensure that this is corrected. If we undertake direct marketing, we acknowledge that we are bound by the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

How can you access and correct your personal information?

Under the Privacy Act, you may seek access to or correct your personal information that we hold about you. These rights are subject to certain exceptions. You can ask for access or correction by contacting our Privacy Officer or, if you are a resident, you can contact your

management team at your relevant community in which you reside.

You may be asked to submit your request in writing. We must give you access to, and take reasonable steps to correct, your personal information if it is incorrect, unless an exception in the Privacy Act or other applicable law applies. We will require you to verify your identity (and provide us with evidence of your authority, if applicable) before we provide access or correct your personal information. We may charge a reasonable fee for providing access. We will advise you in writing if a correction request is refused and will include in this advice the information required by the Australian Privacy Principles or any other applicable law.

We may not be able to provide you with the services you are seeking if you provide incomplete or inaccurate personal information. If you believe the personal information we hold about you is inaccurate, incomplete or outdated, please contact us using the details listed above so that we can correct it.

Your rights under the GDPR

This policy applies to individuals in European Economic Area (**EEA**) countries to the extent the General Data Protection Regulation (**EU**) 2016/679 (**GDPR**) applies.

For the purposes of the GDPR, The Living Company is a 'data controller' responsible for, and in control of, the processing of your personal information. If you are in the EEA, you may have the following rights in relation to your personal information, subject to applicable conditions and exemptions under the GDPR:

- **Access**: You may request a copy of the personal information we hold about you.
- **Rectification**: You may ask us to correct inaccurate or incomplete personal information we hold about you.
- **Erasure**: You may ask us to delete your personal information in certain circumstances (for example, where it is no longer necessary for the purposes for which it was collected). We will notify you within a reasonable timeframe whether we agree to delete your personal information or provide reasons for declining. If we decline, you may have the right to complain to a supervisory authority.
- **Restriction of processing**: You may ask us to restrict processing of your personal information in certain circumstances, for example while we verify the accuracy of information you have disputed.
- **Data portability**: You may request that we provide you with, or transfer to a third party, a structured, commonly used, machine-readable copy of personal information you have provided to us, where our processing is based on your consent or performance of a contract.
- **Object to processing**: You may object to our processing of your personal information

where we rely on legitimate interests as our legal basis, unless we can demonstrate compelling legitimate grounds that override your interests.

- **Automated decision-making**: You have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects. Where such a decision has been made about you, please contact our Privacy Officer to request human review.

To exercise any of these rights, please contact our Privacy Officer. We may ask you to verify your identity before responding to your request. We will aim to respond within 30 days of receipt. If you are not satisfied with our response, you may have the right to lodge a complaint with the data protection supervisory authority in your country.

Links to third party services and websites

Should you decide to stay at one of our communities or use any of our Apps, you will be offered services from third party providers who may collect personal information from you. These services are not operated by us and if you use these services, you should review the providers' privacy policy, terms and conditions, and other policies. We are not responsible for the policies and practices of third parties. Any information you submit to those third parties is subject to their privacy policy, terms and conditions, and other policies.

What happens if there is a data breach?

We are subject to the *Notifiable Data Breaches* (**NDB**) scheme under the Privacy Act. If we become aware of a data breach that is likely to result in serious harm to any individual whose personal information is involved, we will:

- take reasonable steps to contain the breach and assess its likely impact;
- notify the Office of the Australian Information Commissioner (**OAIC**) in accordance with our obligations under the NDB scheme; and
- notify affected individuals directly, where required to do so under the NDB scheme.

If you believe your personal information held by us may have been compromised, please contact our Privacy Officer immediately.

For further information on the NDB scheme, visit www.oaic.gov.au.

Privacy Officer Details

Should you have a query about this policy, request for access or correction or complaint, please contact us on any of the methods below:

Attention: Privacy Officer

Postal Address: The Living Company, Level 14, 275 George Street, Sydney NSW 2000

Email: privacy@thelivingcompany.com.au

Phone: (02) 9098 8800

How can you make a complaint?

If you have a complaint about a suspected breach of our privacy obligations, then you should put your complaint in writing and send it to the Privacy Officer. We will review and respond to your complaint within 30 days of receipt. There may be times when we need a bit longer to investigate the complaint and respond to you but we will contact you within five business days to give you an update and let you know when we think we'll find the answer or solution. We will also confirm how frequently you would like to be updated moving forward.

If you are not satisfied with our response to your complaint, there is a process for complaints to be made with the OAIC. For more information about making a complaint to OAIC, visit Privacy complaints | OAIC.

Additional information on Privacy

For further information on Australian Privacy laws, please visit the Australian Federal Privacy Commissioner's website at www.privacy.gov.au.

Review of and updates to this policy

We will review and update this policy on a periodic basis to reflect our current practices and obligations, and the current version will be made available on our website at TheLivingCompany.com.au. Each published version of this policy will display a version number and effective date on the face of the document to assist you in identifying the most current version.

Version 1.0 – Effective: 14 May 2026