



## Privacy & Confidentiality Policy

Last updated: June, 2026

At UniLodge Canada, we build inclusive communities for inspired living — and that includes respecting your privacy. This Privacy & Confidentiality Policy explains how UniLodge Holdings (Canada) Inc. ("UniLodge Canada", "we", "us", "our") collects, uses, discloses, safeguards, and retains personal information when you interact with us online and in connection with the student housing services we provide.

### 1. Scope

This Policy applies to personal information we collect from prospective residents/applicants, residents, guarantors or emergency contacts (where applicable), university and college partners, vendors, visitors to our websites and digital platforms, and individuals who contact us or apply to work with us.

"Personal information" means information about an identifiable individual. Business contact information used solely for business communications (for example, a work email address and business phone number) may be treated differently under applicable law.

Student Housing and Residency Operations are commercial activities in the context of applicable privacy legislation.

### 2. What laws does this Policy align with?

We strive to comply with applicable Canadian privacy laws, including:

- The federal Personal Information Protection and Electronic Documents Act (PIPEDA), as applicable.
- Applicable provincial private-sector privacy laws, including in Alberta and British Columbia.
- Canada's Anti-Spam Legislation (CASL) for marketing and commercial electronic messages, where applicable.

While provincial legislation may apply to operations wholly within the relevant province, PIPEDA applies to situations where personal information flows across provincial or international borders. Where laws differ, we aim to meet the most protective standard that reasonably applies to the situation.

### **3. What information do we collect?**

We collect only the personal information we reasonably need for the purposes described in this Policy, or as otherwise permitted or required by law. Depending on your relationship with us, we may collect information as described below.

#### **3.1 Information you provide**

You may be asked to, or required to, provide the following information:

- Contact details (e.g. name, email, phone number, mailing address)
- Application and residency information (e.g. student status, rental history, references, guarantor information where applicable, and information needed to administer your lease and residency)
- Payment and billing information (e.g. payment confirmations and transaction details; we typically rely on payment processors for card handling, where applicable)
- Support and communications (e.g. messages, requests, maintenance issues, incident reports)
- Recruitment information if you apply to work with us (e.g. résumé/CV, education and employment history, screening information where permitted)
- Accessibility and accommodation information which may include sensitive information that you choose to provide or that we require to meet legal obligations and support resident well-being
- Emergency and health-related information you provide in connection with an incident or support request: access is restricted and used only as needed

By providing us with sensitive information relating to accessibility, accommodation, or your health, you consent to our collection and use of such information. You may be asked to select a consent “check box” where applicable. Such sensitive information will only be subject to access or use on a need-to-know basis, subject to additional legal requirements.

### **3.2 Information collected automatically online**

When you use our websites, portals, or apps, we may collect technical and usage information such as:

- Device and browser information (e.g. IP address, device identifiers, operating system, browser type)
- Usage data (e.g. pages viewed, actions taken, timestamps, referring pages)
- Cookie and similar technology data (see Section 7)

### **3.3 Safety and security information at our properties**

To help maintain a safe and secure community, we may collect:

- CCTV footage in common areas and building entrances/exits, where in use and appropriately posted when required. These recordings may capture your image, movements, actions, or other identifiable information about you. Recordings are typically retained for 30 days prior to being overwritten or destroyed.
- Key card/fob access records and related security logs. This information is used solely for ensuring building security, investigating unauthorized access or security incidents, monitoring and managing access to restricted areas, maintaining records for compliance with building safety, and for regulatory compliance. Physical access logs are typically retained for 30 days.
- Incident and security reports, including details relevant to health, safety, or conduct.

The above information is stored in a secure location, and access to such information is limited. The above information may be stored for longer than indicated where required to investigate an incident, for regulatory compliance, or where otherwise required by law.

## **4. How do we collect information?**

We collect personal information in several ways, including:

- Directly from you (e.g. when you contact us, apply for housing, sign a lease, use resident portals, or request support)
- Automatically when you interact with our digital platforms (e.g. cookies, pixels, and log files)

- From third parties when permitted by law and necessary for our services (e.g. identity verification and screening services, payment processors, partner institutions, and references)

Where we use third-party screening or identity verification providers, we will identify the provider and make available its privacy information at or before the time of collection.

## **5. How do we use personal information?**

We use personal information for purposes such as:

- Providing and administering housing services including applications, leases, resident communications, and support.
- Maintaining safety, security, and community standards including access control, incident response, and fraud prevention where applicable.
- Processing payments and managing accounts.
- Communicating with you about your application, residency, services, and requests.
- Operating, evaluating, and improving our services and digital platforms including analytics and service quality.
- Meeting legal, regulatory, and contractual requirements.
- Recruitment and workforce administration for candidates and employees where applicable.
- Sending marketing and promotional communications only where permitted in accordance with CASL and your communication preferences.

We do not use your personal information for unrelated purposes without your consent, unless permitted or required by law.

## **6. Consent and your choices**

Where required by law, we obtain consent for the collection, use, or disclosure of personal information. Consent may be express or implied depending on the context and the sensitivity of the information.

You can withdraw consent in certain circumstances, subject to legal or contractual restrictions and reasonable notice. You can also opt out of marketing emails at any time by using the unsubscribe link in the message or by contacting us.

## **7. Cookies, analytics, and similar technologies**

When you use our websites, portals, or apps, we may collect information you provide to us in addition to certain information automatically collected by those interfaces. This information may include information about your device, browser, usage data, as described in Section 3.2, and cookies.

We use cookies and similar technologies to help our websites and portals work, to remember your preferences, and to understand how our digital platforms are used. We use cookies for site functionality and analytics.

We use Google Analytics ("Google") to collect anonymous traffic data to help us understand website performance and improve user experience. Depending on your jurisdiction, you may be presented with cookie choices or a consent banner. The information stored in the cookie may be transmitted to and stored by Google on servers in the United States. Google may also transmit this information to third parties where required by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. By using our website, you consent to the processing of data about you by Google in the manner and for the purposes set out above. We will not, nor will we enable third parties to, use this analytic information to track or collect any personally identifiable information about you. For further information on the privacy of Google Analytics, please visit <http://policies.google.com/privacy>.

You can manage cookies through your browser settings. If you disable cookies, some website features may not function properly.

## **8. When do we share personal information?**

We do not sell or rent personal information. We may share personal information in limited circumstances, including:

- Service providers who support our operations (e.g. IT hosting, resident portals, payment processing, customer support tools, maintenance systems)
- Partner institutions and property owners where necessary to deliver services and meet contractual requirements (e.g. emergency response, move-in coordination)
- Screening, verification, or collections partners where permitted and relevant to the service
- Professional advisors (e.g. legal, accounting, insurance as needed)
- Authorities or law enforcement where required or permitted by law
- Business transactions (e.g. merger, acquisition, financing subject to appropriate safeguards)

We require service providers to protect personal information, use it only for authorized purposes, and maintain appropriate safeguards. These third parties are subject to contractual agreements requiring the above safeguards, and are subject to confidentiality requirements.

## **9. Where we store and process personal information**

Our core systems are hosted in Canada. We may permit limited access to personal information from outside Canada by trusted service providers or support personnel when necessary to deliver services (e.g., technical support), subject to contractual and security safeguards.

If a service provider outside of Canada collects, uses, discloses, or stores personal information for us or on our behalf, we will make available on request information outlining:

- (a) The countries in which such processing occurs; and
- (b) The purposes for which the service provider has been authorized to process such personal information.

Should your personal information be collected, used, processed, accessed, or stored outside of Canada, it may be subject to the laws of the jurisdiction in which it is processed and may be accessible to Courts, law enforcement, and national security authorities in that jurisdiction.

If you have questions about where your personal information is stored or who may access it, contact us using the information in Section 13.

## **10. Safeguards and retention**

We use reasonable administrative, technical, and physical safeguards to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. Safeguards may include role-based access controls, encryption, logging/monitoring, and training.

We retain personal information only as long as necessary for the purposes described in this Policy and as required by law. When no longer required, we securely destroy, delete, or de-identify the information.

Despite the safeguards that we have put in place, we recognize that there may be breaches of those security safeguards. Breaches may be caused by human error, malicious attack, a technical malfunction, or another reason. A breach is defined as the loss of, unauthorized access to, or unauthorized disclosure of, your personal information.

If a breach occurs, we will conduct a risk assessment to determine if the breach poses a real risk of significant harm to any individual whose information was involved. Significant harm includes bodily harm, humiliation, financial loss, identity theft, negative effects on credit record, and damage to or loss of property. The sensitivity of the information, as well as the probability that the information could be misused, will both be considered.

If we determine that a breach presents a real risk of significant harm, we will report the breach to and notify the relevant privacy regulators as required by law (e.g. the Office of the Privacy Commissioner of Canada under PIPEDA and/or the Alberta/BC Office of the Information and Privacy Commissioner under applicable provincial law). We will notify these regulators, as well as the affected individuals, as soon as feasible and without unreasonable delay. We may also notify other organizations or government institutions that may be able to reduce the risk of harm to affected individuals.

We will keep a record of every breach for a minimum of 24 months after the day we determine a breach has occurred, whether or not we determine that a real risk of significant harm exists.

## **11. Your privacy rights**

Depending on your jurisdiction, you may have rights to:

- Request access to your personal information.
- Request correction of inaccurate or incomplete personal information.
- Request information about how your personal information is used and shared.
- Withdraw consent where applicable.
- File a complaint with the relevant privacy regulator.
- File a complaint with us with respect to the application of the *BC Personal Information Protection Act*

To make a request, contact us as set out in Section 13. We will respond to access and correction requests within applicable legal timelines. We may need to verify your identity before responding.

### **Privacy Complaint – British Columbia**

If you have concerns about how we collect, use, disclose, protect, or correct personal information, you may submit a privacy complaint to our Privacy Officer using the information in Section 13.

To help us respond, please include your name, unit/property, relevant dates, and the type of information requested. We may ask for verification of your identity.

We will acknowledge receipt and investigate. We will respond in writing in a reasonable timeframe or provide an update if more time is required. Typically, we will respond within 30 business days. You may also contact the Office of the Information and Privacy Commissioner for British Columbia if you are not satisfied with our response.

For more details with respect to this British Columbia complaint policy, you can request a copy of the policy from our Privacy Officer.

## **12. Children and minors**

Our services are intended for post-secondary students and related stakeholders. We do not knowingly collect personal information from children without appropriate consent from a parent or guardian where required by law. If you believe a minor has provided us personal information without appropriate consent, please contact us.

## **13. Contact us**

Privacy Officer – UniLodge Canada

Email: [privacy@unilodge.ca](mailto:privacy@unilodge.ca)

Mail: 1400 – 18 King Street East, Toronto, Ontario, M5C 1C4

Please avoid including sensitive information in email where possible.

## **14. Updates to this Policy**

We may update this Policy from time to time. We will post the updated version on our website and revise the “Last updated” date above. If changes are material, we will provide additional notice where required.