Privacy Policy

Clarendon Technologies Inc.

Last updated: February 20th, 2026

---

1. Introduction

Clarendon Technologies Inc. ("Clarendon", "we", "our", or "us") is a Canadian technology company based in London, Ontario. We are committed to protecting your privacy and handling your personal information with care.

This Privacy Policy explains what personal information we collect, how we use and protect it, when we share it, and the rights you have over it. It applies to:

- Visitors to our website;
- Our customers and prospective customers; and
- Individuals who use software platforms we operate on behalf of our clients.

We handle personal information in accordance with the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and applicable provincial privacy laws in Canada.

2. Our Role: When We Are Responsible vs. Acting for a Client

The role we play with respect to your personal information depends on the context:

- **When you interact with Clarendon directly** — for example, through our website, our sales process, or as a customer organization — Clarendon is the organization responsible for your personal information.
- **When you use a platform we operate for a client** — the client is the organization responsible for the personal information collected through that platform. Clarendon acts as a service provider, processing personal information on the client's behalf and under their instructions.

In both cases, we apply the safeguards described in this policy. For privacy questions about information collected on a platform we operate for a client, please contact that client organization in the first instance. Clients may also publish their own privacy notices that apply to their use of our platforms.

3. Information We Collect

3.1 Information you provide

Depending on how you interact with us or with the platforms we operate, we may collect:

- **Contact and account information**, such as your name, email address, telephone number, and mailing address.
- **Authentication information**, such as usernames and password hashes. We do not store passwords in plain text.
- **Membership, program, or transactional information** on platforms we operate for clients, such as profile details, enrollments, and similar records as determined by the client.
- **Financial information** where a platform requires it, such as a void cheque or banking form image used to enroll you in a pre-authorized payment program on a client's behalf. Where this occurs, the banking details themselves are entered into a payment processor; we do not store account or transit numbers as structured data within our platforms.
- **Communications**, such as messages and attachments you send us or submit through our platforms.

3.2 Information we collect automatically

- **Usage data**, such as the pages or features used, actions taken, and the dates and times of activity.
- **Device and technical data**, such as IP address, browser type and version, operating system, and approximate location derived from IP address.
- **Cookies and similar technologies** used to keep you signed in, remember preferences, and understand site usage. You can control cookies through your browser; disabling them may affect some features.

3.3 Information from third parties

We may receive personal information from third parties where you have authorized them to share it (for example, from a client organization enrolling you as a user, or from a payment processor confirming a transaction).

4. How We Use Personal Information

We use personal information for the following purposes:

- **Providing services**, including operating our software platforms and supporting client organizations and their users.
- **Authentication and account management**, including verifying identity and managing access.

- **Processing transactions and enrollments**, including communicating with payment processors where a client platform supports payments.
- **Communications**, such as transactional messages, service notifications, and responses to inquiries.
- **Improvement and analytics**, including diagnosing issues, improving features, and understanding usage patterns.
- **Compliance and protection**, including meeting legal obligations, enforcing our terms, and protecting the security and integrity of our services.

5. Consent

We collect, use, and disclose personal information with your consent, except where the law allows or requires us to do so without consent. Consent may be **express** (for example, when you submit a form) or **implied** (for example, when you continue to use a service after being informed of relevant practices). You may withdraw your consent at any time, subject to legal or contractual restrictions; withdrawal may limit or prevent us from providing some services.

6. Disclosure of Personal Information

We share personal information only as needed and as described below. **We do not sell personal information.**

6.1 With our client organizations

When you use a platform we operate for a client, the personal information collected through that platform is made available to authorized staff of the client organization. The client is responsible for handling that information in accordance with its own privacy practices and applicable law.

6.2 With service providers

We engage trusted service providers to help us operate our services. These providers fall into categories such as:

- **Cloud infrastructure, hosting, and storage providers**;
- **Payment processors**, where a platform supports payments;
- **Email and communications delivery providers**;
- **Analytics, monitoring, and error-tracking providers**; and
- **Development, support, and operational tools** that we use to deliver our services.

We require service providers to handle personal information consistent with this Privacy Policy and to use it only for the purposes for which we engaged them. The specific providers we use evolve over time and vary by service. Where appropriate, additional information about specific providers may be made available to client organizations on request, subject to confidentiality.

6.3 For legal reasons

We may disclose personal information if required by law, in response to a valid legal request, or where necessary to protect our rights, our users' safety, or to investigate fraud or abuse.

6.4 In a corporate transaction

If Clarendon is involved in a merger, acquisition, financing, or sale of assets, personal information may be transferred as part of that transaction, subject to confidentiality protections and applicable law.

7. Where Your Information is Stored

Personal information we process is stored on infrastructure operated by reputable cloud service providers. Where reasonably available and appropriate to the service, we use Canadian-region data centres for storage of personal information related to platforms operated for Canadian clients.

Some of our service providers may process limited information outside of Canada (for example, certain communications, analytics, or support services). Where this occurs, we take steps to ensure comparable protection through contractual safeguards.

8. Retention

We retain personal information only as long as needed to fulfill the purposes for which it was collected, to comply with our legal obligations, to resolve disputes, and to enforce our agreements.

General retention practices include:

- **Uploaded sensitive documents (e.g., financial or health data) on platforms we operate**: deleted by authorized client staff promptly after the enrollment or transaction is processed. As a backstop, an automated lifecycle policy deletes such uploads no later than **[60] days** after upload, regardless of processing status.
- **Account records**: retained for the duration of the user's relationship with the client organization (or with Clarendon), and for a reasonable period afterward to address inquiries, support, audit, and legal needs.
- **System and security logs**: retained for **[12] months** unless a longer period is needed for investigation or compliance.

Specific retention periods for personal information on platforms we operate may be set by our client organizations and may differ from the defaults above.

9. Safeguards

We use a combination of technical, organizational, and physical safeguards to protect personal information, including:

- **Encryption in transit** using HTTPS/TLS for connections between users, our platforms, and our service providers.
- **Encryption at rest** for data stored in our managed databases and object storage.
- **Access controls**, including authenticated, role-based access for both Clarendon staff and client users; least-privilege access internally; and protected administrative interfaces.
- **Network and infrastructure protections**, including managed cloud infrastructure with industry-standard controls, segmented environments, and routine patching.
- **Backups** of databases stored in encrypted form.
- **Operational practices**, including staff confidentiality obligations and limiting access to personal information to those who require it for their role.

No security measure is perfect, and we cannot guarantee that information will be free from unauthorized access. We work to continuously improve our practices.

10. Breach Response and Notification

If we become aware of a breach of security safeguards affecting personal information under our control, we will respond promptly to contain and assess the breach. Where the breach creates a real risk of significant harm, we will, in accordance with PIPEDA:

- Notify affected individuals (or, in the case of platforms operated for clients, notify the client so that they can notify affected individuals);
- Report the breach to the **Office of the Privacy Commissioner of Canada**; and
- Maintain a record of the breach as required by law.

11. Your Rights

Subject to applicable law, you have the right to:

- **Access** the personal information we hold about you;
- **Correct** information that is inaccurate or out of date;
- **Withdraw consent** to our collection, use, or disclosure of your personal information, subject to legal or contractual restrictions;
- **Request deletion** of your personal information, subject to legal or operational limits; and
- **File a complaint** with us or, if you remain unsatisfied, with the **Office of the Privacy Commissioner of Canada** (priv.gc.ca).

To exercise these rights with respect to information you provided directly to Clarendon, contact our Privacy Officer using the details in Section 14. If your request relates to information collected through a platform we operate for a client organization, please contact that client directly — they are the organization responsible for that information, and we will support them as needed.

We may require you to verify your identity before responding to a request.

12. Children

Our services are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13 except on platforms we operate for client organizations where minor accounts are administered by a parent or guardian.

13. Changes to this Policy

We may update this Privacy Policy from time to time. The *"Last updated"* date at the top reflects when the policy was most recently revised. Material changes will be communicated through our website or, where appropriate, by direct notice.

14. Privacy Officer and How to Contact Us

We have designated a Privacy Officer who is accountable for Clarendon's compliance with this Privacy Policy and applicable privacy laws.

Privacy Officer: David MacNeill, President

Email: privacy@clarendontech.com

Mail: Clarendon Technologies Inc., 448 Regent St, London, ON, Canada, N5Y 4H2

For questions about a platform we operate for a client organization, please also contact that organization directly.