KINLOCH BRANDS LTD.

Privacy Policy

Kinloch.med

Version 1.1
Effective date: October 20, 2026
Last updated: November 9, 2026

1. Who we are and what this policy covers

Kinloch Brands Ltd. (“Kinloch,” “we,” “us,” or “our”) operates kinloch.med and the related public website, patient platform, product-discovery experience, clinical-intake tools, account and document services, and order-support services (together, the “Platform”). The Platform supports people seeking medical cannabis authorization from an independent licensed nurse practitioner and, where permitted, the purchase and fulfilment of products in Canada.

This Privacy Policy explains how we collect, use, disclose, store, retain, and protect personal information when you visit or use the Platform, contact us, complete an intake, communicate with a practitioner or support team, or place and manage an order. It applies to patients, prospective patients, website visitors, account holders, responsible adults acting for a patient, and other individuals whose personal information we handle.

We handle personal information in accordance with the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy and health-information laws. Requirements can vary by province and by the role in which information is held. Where another applicable law provides greater protection, we apply that protection.

2. The roles of the parties handling your information

Medical cannabis authorization involves both a clinical relationship and operation of the Platform. The responsible party can therefore depend on the information and purpose involved.

Party	Role	Responsibility for your information
The nurse practitioner or other authorized practitioner who reviews your request	Treating practitioner and, where applicable, health-information custodian	Makes the independent clinical assessment and is responsible for clinical information and records in accordance with professional, regulatory, and applicable health-privacy obligations.
Kinloch Brands Ltd.	Platform operator, licensed seller, and information manager or service provider where applicable	Operates accounts, intake, authorization, registration, order, fulfilment, security, support, and compliance functions. Kinloch also handles information for its own legal and operational responsibilities as described in this Policy.

Party	Role	Responsibility for your information
Ad-Wise Agency Inc.	Contracted technology service provider	Provides software development and related technical services to Kinloch under contractual confidentiality, security, and purpose-limitation obligations.

Service providers may process personal information only for the contracted service and under Kinloch's instructions, unless the law requires otherwise. This Policy does not change a treating practitioner's independent professional duties or determine a legal role differently where applicable law assigns it.

3. The personal information we collect

We limit collection to information reasonably needed for the purposes identified in this Policy. What we collect depends on how you use the Platform.

3.1 Public website, age attestation, and product discovery

We may collect your province or territory, date-of-birth entry used for age attestation, the resulting age-gate status, language, consent version, and limited session, device, security, and request information.

You may manually adjust the Kinloch Wheel before answering a discovery question. In that no-answer mode, your adjustment stays in your browser memory and is not sent to or stored by Kinloch. If you separately consent to product discovery and answer a question, the answers, derived product-attribute settings, filters, and related request receipts may be stored in application-layer-encrypted temporary discovery state. That state is associated with an anonymous session, is kept for no more than 30 days, and is kept separate from your account, cart, clinical intake, and patient record. Withdrawing discovery consent or removing the final answer erases the applicable retained discovery state as described by the on-page controls.

3.2 Account and identity information

We may collect your legal name, date of birth, province or territory, residential and shipping address, email address, telephone number where provided, invitation and verification status, account credentials, session information, language, and authentication records. Patient two-factor authentication is optional unless a particular risk or policy requires an additional verification step; staff accounts use stronger mandatory controls. We store verification evidence and security identifiers rather than plaintext verification codes where the implemented control permits.

3.3 Clinical and authorization information

If you seek clinical review or use an existing medical document, we may collect intake responses, medical history, symptoms, current medications, allergies, contraindication and risk information, identity details needed for assessment, uploaded documents, practitioner information, consultation and clarification records, structured summaries, clinical notes, decisions, signatures, medical authorizations, registration records, amendments, expiry information, and related communications.

Where you give the required consent for a recorded voice interaction, we may collect the recording, transcript, structured clinical information derived from it, provider identifiers, consent evidence, and technical call events. A call that the Platform identifies as not recorded is not converted into an audio record; the practitioner may still create the clinical note required for care.

3.4 Cart, order, checkout, fulfilment, and support information

We may collect cart contents, product and quantity selections, authorization and purchase-limit checks, order history and status, prices, taxes, discounts, shipping details, delivery and carrier events, returns, refunds, replacements, support requests, and communications.

Shopify hosts secure checkout and may process payment, billing, contact, shipping, and order information needed to complete and manage the transaction. Kinloch does not store full payment-card or bank credentials in its own Platform databases. Clinical intake answers, clinical notes, and medical-authorization documents are not included in the checkout handoff. Shopify and its payment providers retain and handle information under their own legal obligations and privacy terms.

3.5 Communications, technical, and security information

We may collect messages, support correspondence, notification preferences and consent records, email and SMS delivery events, IP address, browser and device information, timestamps, request and error identifiers, fraud and security signals, and access or audit records. We design operational logs and audit events to exclude clinical content and other personal information that is not needed for the recorded purpose.

4. Why we collect and use your information

We use personal information to:

- provide age-gated public access and optional product discovery;
- create, verify, secure, and administer accounts;
- enable an independent licensed practitioner to assess an intake, request clarification, make a clinical decision, and issue or decline an authorization;
- receive, verify, maintain, amend, and cancel medical documents and client registrations;
- operate carts and apply current product, inventory, authorization, and legal purchase-limit rules;
- provide hosted checkout, order processing, fulfilment, shipping, returns, refunds, and replacements;
- send requested account, clinical, order, security, and service communications;
- provide customer, technical, and clinical-support coordination;
- prevent, investigate, and respond to fraud, misuse, security events, service failures, and legal claims;
- maintain the integrity, availability, and safety of the Platform;
- meet obligations under the Cannabis Act, Cannabis Regulations, privacy and health-information laws, professional requirements, tax and consumer-protection rules, and other applicable laws; and
- send optional promotional communications only where we have the consent required by law.

We do not use product-discovery answers as clinical intake information, and they do not influence a practitioner's independent clinical decision. We do not use clinical information to advertise products. We will identify a materially new purpose and obtain consent where required before using personal information for that purpose.

5. How we obtain and manage consent

The form of consent depends on the sensitivity of the information, the context, and legal requirements. We use express, purpose-specific consent for sensitive clinical information, recorded interactions, optional discovery answers, and optional promotional communications where required. Age attestation, acceptance of Terms and Conditions, clinical consent, discovery consent, recording consent, and marketing consent are separate decisions.

You may withdraw a consent by using the available Platform controls or contacting us, subject to legal or contractual restrictions and reasonable notice. Withdrawal may prevent us or a practitioner from continuing a service that requires the information. It does not reverse processing already lawfully completed, invalidate a prior clinical decision, or require deletion of a record that must be retained by law or professional obligation. We record the withdrawal and stop the affected optional processing as required.

You can manage retained product-discovery state in the “Manage your privacy choices” section below this Policy. You can manage notification choices in Account & Security and unsubscribe from promotional email or SMS using the message control where available. Service, security, clinical, and order communications may still be sent when necessary to provide the service or meet legal obligations.

6. When and with whom we share your information

We do not sell personal information. We disclose it only for the purposes described in this Policy, with consent where required, or as permitted or required by law.

6.1 Practitioners and care support

We make the information needed for assessment and follow-up available to the licensed practitioner responsible for the case. Where another authorized care professional or coordinator supports the interaction, access is limited to the role and task involved.

6.2 Platform and infrastructure providers

Amazon Web Services supports Canadian-region application hosting, databases, encrypted object storage, caching, encryption-key management, email delivery through Amazon Simple Email Service (SES), and operational services. Where enabled, Amazon Bedrock in the Canada (Central) Region may provide model processing for a permitted Platform function. Kinloch does not send this information to a public model endpoint or authorize model training on it.

Ad-Wise Agency Inc. provides contracted software and technical services. Access to live personal information is limited by role, purpose, environment, and contractual safeguards.

6.3 Checkout, fulfilment, and delivery

Shopify hosts checkout and processes the account contact, billing, shipping, cart, payment, and order information needed for the transaction. Fulfilment partners and carriers receive only the order, identity, address, age-verification, and delivery information needed to prepare and deliver the shipment, manage a return, or respond to a delivery issue. Clinical intake and authorization documents are not shared with Shopify, fulfilment partners, or carriers as part of ordinary checkout or delivery.

6.4 Communications and voice providers

AWS SES delivers account and service email. Where a Kinloch environment is specifically enabled and authorized for a voice or SMS function, Twilio may process telephone numbers, message or call-routing data, and provider events, and ElevenLabs may process the minimum necessary voice interaction and resulting transcript for an authorized intake workflow.

Kinloch-controlled personal health information stores and artifacts use AWS infrastructure in Canada. A limited, owner-controlled AWS development exception may temporarily use real Twilio or ElevenLabs processing outside Canada for active, invited, verified users who have given the required call and recording consents. That exception includes minimum-necessary disclosure, prompt Canadian materialization, provider deletion where supported, and audit evidence. Public telephone networks may also route data outside Canada. This development exception is not production approval. Production use of those providers for personal health information remains disabled unless contractual, privacy, security, residency, and legal requirements are separately cleared.

6.5 Legal, regulatory, safety, and business matters

We may disclose information to Health Canada, privacy or professional regulators, law enforcement, courts, tax authorities, or other parties where legally required or permitted; to protect a person, the public, Kinloch, or the integrity of the Platform; or to investigate fraud or a security incident. A proposed financing, reorganization, merger, or sale may involve limited due-diligence disclosure under confidentiality and applicable legal safeguards. Any transfer remains subject to applicable privacy obligations.

7. Where your information is stored and processed

Kinloch's primary posture is Canadian residency. Kinloch-controlled databases, clinical artifacts, uploaded documents, recordings after Canadian materialization, authorization documents, and audit records are stored in the AWS Canada (Central) Region (ca-central-1) with encryption and role-based access controls. Amazon Bedrock processing, when permitted, is configured for that Canadian region. Public website assets may be delivered through a content-delivery network and are not patient records.

Some providers involved in checkout, carrier delivery, communications, or the limited development voice exception may process information in another jurisdiction. Information in another jurisdiction can be subject to its laws and lawful-access demands. We use purpose limitation, data minimization, contractual controls, secure transfer, access controls, and deletion or return requirements appropriate to the service. We assess a new cross-border use before enabling it and provide additional notice or consent where required.

8. How long we keep your information

We retain personal information only as long as needed for the identified purposes and applicable legal, regulatory, contractual, security, and professional obligations.

- No-answer manual Wheel settings remain in browser memory only and end with the browser state.
- Encrypted post-answer discovery state and related encrypted request receipts expire no later than 30 days after the controlling discovery record and are erased earlier when the applicable withdrawal or final-answer removal flow completes.
- Platform clinical, authorization, registration, order, consequential-action audit, and related protected artifacts use the applicable documented retention class. Where the Cannabis Regulations or the implemented audit catalogue sets a two-year minimum, Kinloch retains the record for at least two years. A practitioner or another applicable law may require a longer clinical-record period.
- Account, security, support, communication, transaction, tax, dispute, and fraud-prevention records are retained for the period reasonably required for their purpose and any legal limitation or record-keeping period.
- Shopify, payment providers, practitioners, carriers, and other independent or separately regulated parties may apply their own legally required retention periods.

At the end of the applicable period, we securely delete, destroy, de-identify, or make the information inaccessible in accordance with the system and legal requirements. Backup and immutable audit copies age out under controlled retention schedules rather than being selectively overwritten.

9. Your privacy rights and choices

Subject to applicable law and lawful exceptions, you may:

- ask whether we hold personal information about you and request access to it;
- ask for inaccurate or incomplete information to be corrected;
- withdraw an optional consent or change communication preferences;

- request deletion of information that is no longer required and is not subject to a legal or professional retention duty;
- ask how information has been used and disclosed;
- challenge our compliance and receive an explanation of a decision affecting your request; and
- make a complaint without retaliation.

Clinical-record requests may need to be coordinated with the treating practitioner or applicable custodian. We will help direct the request. We verify identity before granting access or making a change and respond within the period required by applicable law. Access is generally provided without charge; if a permitted fee applies, we will explain it before proceeding.

10. How we protect your information

We use safeguards proportionate to the sensitivity and volume of the information, including encryption in transit and at rest, managed encryption keys, network and storage restrictions, role-based and least-privilege access, staff multi-factor authentication, optional patient two-factor authentication, secure verification flows, environment separation, monitoring, tested backup and recovery controls, provider contracts, access review, purpose-minimized logging, and append-only audit evidence for consequential actions.

No method of transmission or storage is completely secure. If a breach of security safeguards creates a real risk of significant harm or meets another reporting threshold, we notify affected individuals and regulators as required, keep the prescribed record, and take steps to contain and remediate the incident.

11. Cookies, local storage, analytics, and advertising

The Platform uses cookies and similar browser storage to maintain sessions, remember language and interface preferences, preserve permitted cart or consent state, support security, and operate features. The no-answer Wheel vector remains browser-only. We may use privacy-protective operational measurements to understand service reliability and use, but we do not place clinical intake content in analytics or advertising systems.

On approved public, sign-in, and registration pages, Kinloch counts visits, key steps, and public Shop product interest by SKU on its Canadian servers without storing a visitor identifier, cookie, contact details, or health answers in those measurements. On those approved pages, Google Analytics storage is enabled by default unless this browser has a saved denial, and a limited page-view measurement may be sent before the age check. If you turn off **Allow analytics and ads** before entering, or withdraw that choice later, Kinloch denies analytics and advertising storage, removes known analytics and advertising cookies, and future Google measurements use cookieless requests. A page measurement already sent before you turn the setting off cannot be withdrawn retroactively. Cookieless requests can still expose ordinary network information such as your IP address and browser information.

After a successful age check, Kinloch sends Google the generic site_entered event. Google measurements may include an approved public page path and title, a fixed funnel context, the public origin of a referring site, standard public campaign labels and permitted advertising click identifiers, and generic page, registration, button, outbound-link, download, scroll, form-interaction and video-engagement events where enabled. Public link and download metadata may include the destination, link identifier or styling classes, and public filename or extension. Google’s external-referrer field omits paths and queries. Private handoff or checkout tokens, typed form contents, your date of birth, province or territory, Wheel choices, cart contents, product SKUs, contact details, account identifiers and health answers are excluded from Kinloch-authored browser analytics and advertising events. Advertising click identifiers require advertising permission. Public campaign and referral context may be retained in the current tab only while analytics storage is permitted.

Advertising storage, advertising user-data processing, and advertising personalization remain off unless you enter with **Allow analytics and ads** enabled. When you allow it, Kinloch also uses this browser’s signed anonymous session to

estimate unique browsers in aggregate without retaining the signed session value, and Google, Meta, Pinterest, Reddit, and X may use browser storage and limited site-use data for analytics, attribution, advertising measurement, and personalization. Kinloch does not enable automatic email, phone-number or address matching for this tracking. You can withdraw this choice using the Analytics and ad settings control. These providers may process the permitted technical and site-use information outside Canada under their own service terms.

You can control cookies through your browser. Blocking a required session or security cookie may prevent sign-in or another requested function. Where law requires consent for a non-essential technology, we request it before use.

12. Age and responsible adults

Public cannabis-product content is age-gated according to the province or territory selected. Medical access can involve a patient below the generally applicable age where the Cannabis Regulations permit registration through a responsible adult and a practitioner has issued the required medical document. In that case, we collect and verify the information needed for both the patient and responsible adult, and the adult must have authority to act. We do not knowingly collect information outside an eligible or legally permitted pathway.

13. How to contact us

Kinloch has designated a Privacy Officer accountable for this Policy and for receiving access, correction, withdrawal, and complaint requests.

Contact	Details
Role	Privacy Officer
Organization	Kinloch Brands Ltd.
Email	privacy@kinloch.med
Mailing address	#37 – 5855 Mt. Lehman Road, Abbotsford, BC V4X 2P7
Telephone	Current telephone number available at kinloch.med/contact

Please do not send clinical details by ordinary email. We may ask you to use a secure channel and will verify your identity before discussing or changing an account or record.

14. If you are not satisfied

Contact the Privacy Officer first so we can review and respond to your concern. If you are not satisfied, you may contact the Office of the Privacy Commissioner of Canada at priv.gc.ca. Depending on your province and the nature of the information, you may also contact the applicable provincial privacy, health-information, or professional regulator.

15. Changes to this Policy

We may update this Policy to reflect changes in law, practices, providers, or the Platform. We post the updated version and its effective and last-updated dates. Where a change is material, we provide additional notice and obtain a new consent where required. An updated Policy does not by itself convert a development-only provider exception into production approval or remove an existing legal or professional safeguard.