Privacy Policy

Last updated 27 November 2026 · Operated by Synvora Labs LLC · privacy@k00l.app

This policy explains what personal data Kool collects, why, who receives it, how long we keep it, and the rights you have. Kool is operated by Synvora Labs LLC. We collect what we need to run Kool. We **do not sell your data**, we use **no advertising ID** and **no advertising network**, and we **do not track you across other apps or websites**.

What we collect

- **Account.** Your email address (used to sign in and for service emails), username, display name, and optional bio, link, gender and avatar. A phone number only if you add one: we text it a code to verify it, and then keep it with your account.
- **Sign-in and security data.** You can sign in with a one-time code sent by email, a password, a passkey, or your Apple or Google account. We store only a short-lived hash of a one-time code (never the code), a salted one-way hash of a password (never the password), a passkey's public key, and, for Apple or Google, the account identifier and the email address they give us (Google also gives us your name and profile picture, which can become your Kool avatar). We keep hashed session tokens with device info so you can sign devices out, and, if you turn it on, a two-factor secret and hashed recovery codes. We log IP addresses and basic technical data to prevent abuse.
- **Content you create.** Messages, voice messages, photos, videos, files, stories, posts, clips, live streams, comments, notes, and meeting and call details (including any location you type into a meeting or share in a chat). Messages, including voice messages, are kept until they are deleted (for example by disappearing messages) or you close your account. Messages and files you sent stay in the chats of the people you sent them to. Stories delete themselves after 24 hours. Calls are not recorded on our servers, and live captions are made on each device and not stored.
- **Searches.** When you search in Kool, we keep the words you searched, linked to your account, to suggest posts, products and topics you may like. Search history is kept for one year and deleted when you close your account.
- **Ads you see.** A record of the ads and sponsored posts shown to you and the ones you tap or hide, linked to your account (see "Advertising").
- **Purchases and Shop.** Your Kool+ and in-app purchase records, and, when you use the Shop, the delivery addresses you save (name, phone number and address) and your orders (see "Payments").
- **Connected email and calendar (optional).** If you link a mailbox we store its provider, its address and the access tokens the provider gives us. For Gmail we access your mail through Google's API to show and send it inside Kool and, only if you turn on a Pufy routine, daily brief or follow-up that uses your mail, to check it for that feature. We read your Google Calendar to show your next events and, for a Pufy routine that starts before a meeting, to see when it begins. We do not keep a copy of your calendar. When a routine is started by a new email or meeting, we keep its sender, subject and a short preview (or the meeting's title and time) until that routine runs, and then in that run's working record, which is deleted within 8 days. A routine also keeps the IDs of the last 200 messages, threads or events it has already checked, so it never starts twice for the same one, for as long as the routine exists. Kool's use of Google user data complies with the Google API Services User Data Policy, including the Limited Use requirements. We never sell it, use it for ads, or let humans read it.

- **Notifications.** Your device's push token. Notifications travel through Apple Push Notification service or Firebase Cloud Messaging (Google). A chat notification includes the sender's name and a preview of the message, except for sealed and incognito messages.
- **Music tags.** Titles, artwork and 30-second previews come from Apple's public catalog; we store only the tag you attach.
- **Verification and username claims** (from 28 December 2026). When you ask us to verify your account or to claim a username, we process the evidence you send (for example an email address at your organisation's domain, trademark or company documents, or proof of identity) only to decide that request, and delete the evidence file once it is decided. If a username is taken from another account because of your claim, we tell that person their name changed but not who you are.

On your phone

- **Contacts.** To show which of your contacts are on Kool, the app turns their phone numbers and email addresses into SHA-256 hashes on your phone and sends only those hashes, never names. We compare them with the verified numbers and addresses of Kool accounts and discard them when the answer is sent; we do not store your address book. Kool writes to your contacts only when you save a contact yourself (a new contact, or a contact card someone sent you).
- **Calendar.** Kool can show your phone's calendar and add events to it. Those events stay on your phone. The one exception is Pufy (below): on iPhone and iPad, if you ask Pufy about your calendar, the events it reads are sent to answer you.
- **Location.** Used only when you share a location, look up a place, or ask Pufy something that needs it.
- **Camera, microphone and photos.** Used only for what you choose to capture, record, call with or send.

Pufy, the assistant

Pufy is Kool's assistant, part of Kool+. On a child account Pufy only works in a limited help mode, and the guardian can turn it off. Pufy uses **Anthropic (Claude)** to answer. To answer you, Anthropic receives what you ask, your Pufy conversation so far, pictures you add, and what Pufy reads for that answer: for example the chats, emails, meetings, notes, posts, orders or products you ask about, and on iPhone and iPad your phone's contacts, location, calendar, reminders and alarms when the question needs them. If you set up a Pufy routine, goal, daily brief or follow-up, Pufy also runs on its own at the times or events you chose, and Anthropic receives what that run reads, for example the new email or meeting that started it. The working record of each run is deleted within 8 days. What Pufy writes back, which may summarise that email or meeting, is posted to your Pufy conversation, sent to you as a notification, and kept in the routine's history (its last 30 runs) or on the goal, until you delete that routine or goal.

- **Location** read from your phone is rounded to about 1 km before Pufy uses it.
- **Contacts and location** that Pufy reads from your phone are removed from your stored Pufy history once the answer is complete. Pufy's reply itself stays.
- **Places, routes and weather** come from **Google Maps Platform**, which receives the place or route asked for and, when needed, a location.
- **Alarms and reminders** Pufy sets are created on your phone. Their title and time are part of your Pufy conversation.
- **Voice. ElevenLabs** turns Pufy's replies into speech; it receives the text to be spoken. Turning your speech into text runs on Cloudflare.
- **Keeping and deleting.** Your Pufy conversation is kept until you clear it or close your account. Incognito Pufy chats are deleted within 24 hours. Files you give Pufy are deleted after 30 days. Pufy's memory of you can be erased at any time, and is erased 90 days after Kool+ ends.

Anthropic is also used when you mention @Pufy in a chat (Pufy reads that chat's last 12 messages), when Pufy's memory reviews your messages, calls, meetings, calendar and notes as you allow in Pufy's settings, and for automatic translation of messages you send. The iPhone, iPad and Mac app asks for your permission before it first sends your content to Anthropic or ElevenLabs, and uses Cloudflare Workers AI for automatic translation until you allow it. The Android app and the web app do not ask separately: using Pufy or automatic translation there sends what is needed to answer you.

Businesses that use Pufy for Business. When you message a business that uses Pufy for Business, its replies may be written by AI. What you send that business is processed by Anthropic to write the reply.

Anthropic, ElevenLabs and Google Maps Platform act as our service providers under contract, and process this data only to provide the service to us.

Other AI

We use Cloudflare Workers AI, within our infrastructure, for content moderation, translation, captions and speech-to-text. AI dubbing of clips, which a creator turns on for each clip, uses **ElevenLabs** to dub the clip's audio and **Sync.so** to match the lips; we delete ElevenLabs' copy once the dub is done, and a creator can withdraw at any time. We don't sell your content to AI vendors or use your private content to train third-party models. Automated moderation decisions can be appealed in the app.

Advertising

Kool shows its own ads and sponsored (promoted) posts. They are served by Kool itself, not by an ad network, with no advertising SDK, no advertising ID (no IDFA, no Android advertising ID), no cross-app tracking and no App Tracking Transparency prompt.

- **How an ad is chosen.** By your country (from your connection), where in the app it appears, and your own history with ads: how many you have seen recently, which ones you saw in the last few hours, and the ones you hid. Sponsored posts can also be matched to the captions of posts you recently liked.
- **What advertisers see.** People who run ads or promote a post see totals only: views, reach, taps, new followers, and an audience breakdown by country, age range and gender, with groups smaller than five combined. They never receive who you are or any data about you as an individual.
- **Who sees none.** Child accounts and Kool+ subscribers are not shown ads or sponsored posts.

Analytics and crash reports

- **Usage events.** The iPhone, iPad and Mac app sends short usage events to our servers (for example that the app opened, which area you opened, or that a message was sent and of what kind, never its content) and page load times. We keep them on Cloudflare for 90 days. A copy of the usage events goes to **PostHog** for product analytics, without your account ID (replaced by a one-way code PostHog cannot link back to you) and without your IP address. To stop usage events being collected for your account, email privacy@k00l.app.
- **Crash and error reports.** The iPhone, iPad, Mac and Android apps send crash and error reports to **Sentry**: what went wrong in the code, the app version, device model and system version, the app's memory state, recent technical steps before the error, and, for a failed request to our servers, which address was requested and the result. Crash reports contain no message content. The apps are set not to add default personal data such as your email, but the address of a failed request can contain a username or an ID. Our servers also report their own errors to Sentry without any user, IP address or request content.

Payments

We never see or store your card details. **Kool+** and other in-app purchases are processed by Apple (App Store) or, on Android, by Google Play Billing; we keep the purchase record (product, transaction ID, dates and status) to give you what you bought.

Shop and creator payouts, when available, use **Stripe**. Sellers and creators set up payouts on Stripe's own pages, so their identity and bank details go to Stripe, not to us. Buyers pay on Stripe's checkout, and a saved card is stored by Stripe. When a seller ships an order, the buyer's name, delivery address and phone number go to **Shippo** and the carrier to make the shipping label. We keep orders, payments and payout records for 7 years, as tax law requires.

How we protect your data

- **Encryption in transit.** Traffic between your device and Kool uses TLS. Call and live media use the encrypted transport built into WebRTC.
- **Encryption at rest.** Cloudflare encrypts stored data on its platform.
- **Hashed secrets.** Passwords are stored as salted one-way hashes. Sign-in codes, session tokens and recovery codes are stored only as hashes.
- **Account protection.** Two-step verification, passkeys, a list of signed-in devices you can sign out, and rate limits on sign-in.
- **Access control.** Staff access is limited to what a role needs, and sensitive actions in our internal tools need a second factor and are logged.
- **Monitoring.** We log abuse signals and errors to detect and investigate attacks.

Messages on Kool are not end-to-end encrypted. We need to be able to process content to deliver it across your devices, to keep people safe, and to meet our legal duties. No system is perfectly secure, and we cannot guarantee the security of your data; you can help by using two-step verification and by keeping your email account and devices secure.

If a security incident affects your personal data and is likely to put your rights at risk, we will notify the competent authority without undue delay and, where feasible, within 72 hours of becoming aware of it, as the GDPR requires. Where the risk to you is high, we will also tell you directly, by email or in the app, and say what happened, what data was involved and what you can do. Report a vulnerability or a suspected incident to security@k00l.app.

Where it lives and who we share with

Data is stored on Cloudflare (D1 database, R2 storage) and sent over TLS. We share data only with the providers that help run Kool, listed with what each receives on Subprocessors, with other users as you direct, or where required by law. We never sell or rent it.

Your rights

Depending on where you live (GDPR/UK GDPR, CCPA/CPRA and others) you can access, correct, delete, port, or restrict your data, object to certain processing, and withdraw consent. We honour these rights for everyone. In the app, Profile settings → My data downloads a copy of your account, messages, calls, meetings, mail, stories, posts, clips, follows and Pufy profile and memories. For anything else, email privacy@k00l.app. EU/EEA/UK users may also complain to their local data-protection authority. Kool is run from Portugal, so our lead authority in the EU is the Portuguese CNPD.

Retention and deletion

We keep data only as long as needed. Stories expire after 24 hours, usage events after 90 days, Pufy's files after 30 days, and search history after one year. Moderation and safety records and security, audit and abuse logs are kept for 1 year, and purchase, order and payout records for 7 years, as tax law requires. You can close your account at any time in Profile settings → Close account; it is deleted at once and cannot be undone. Everything about closing an account, what is deleted, what is kept and for how long, and how to ask if you cannot sign in, is on Delete your account. Backups are kept for 30 days.

Children

Kool is for 16 and over, with one exception: a **child account**, which a parent or guardian creates inside a Kool family for someone aged 13 to 15. It exists only because that guardian gave permission, and we record who gave it, when, and how, as GDPR Article 8 requires. A guardian can withdraw that permission at any time in Profile → Family, which closes the child's account and deletes its data.

On a child account we collect the same data as any other account, plus the **year of birth** (not a full date: the only question it answers is whether they have turned 16) and a record of **how long they spend in each area of Kool**, which their guardian can see. Guardians can never read anyone's messages, including their child's. When our automated checks **block** a photo or video sent to a child account because it appears to be sexual or violent, or the child taps **Tell my parent**, the guardian receives a **safety alert**: who sent it (name, @username, account ID, account age, and whether a guardian had approved them), where, when, the category and what Kool did. **Never the photo, video or message text**. Other automated signals (criminal or self-harm content) tell the guardian only the topic and the time. Safety records are kept for 90 days, and the child is told in the app that their guardian receives these alerts. If you send something to a child account and it is blocked, that child's guardian sees those details about you, to protect the child. A guardian may also set a **Screen Time schedule** of the times and areas of Kool their child can use. Child accounts are not shown ads or sponsored posts. Content that appears to be child sexual abuse material is reported to NCMEC's CyberTipline as US law requires, preserved for the period the law requires, and never shown to guardians. Guardianship ends automatically the year they turn 16, when the account becomes theirs alone and nothing is deleted.

Synvora Labs LLC is registered with the National Center for Missing & Exploited Children (NCMEC) as an Electronic Service Provider and reports to NCMEC's CyberTipline. If content appears to be child sexual abuse material, US law (18 U.S.C. §2258A) requires us to report it. A report contains the material, the account details of the person involved (such as name, username, email address and IP address with the time it was used) and the context in which the material was found. Our legal bases are our legitimate interest, and that of NCMEC and the authorities, in protecting children from sexual abuse (GDPR Article 6(1)(f)) and, where it applies, the protection of the vital interests of a child (Article 6(1)(d)). For people in the EEA, scanning of private messages for child sexual abuse material is done only as far as Regulation (EU) 2026/1881 allows, with human review before a report is made about material we had not seen before. NCMEC is in the United States and is not one of our subprocessors. We transfer the report with the safeguards GDPR Chapter V requires, which can include standard contractual clauses or, in the individual case, the exceptions in Article 49 for important reasons of public interest or to protect vital interests. The person reported is not told.

Kool is not directed to children under 13 and we do not knowingly collect their data. If you believe a child under 13 has an account, contact privacy@k00l.app and we will delete it.

International transfers

Kool runs on Cloudflare's global network, and some of the providers on Subprocessors process data in the United States; where data crosses borders we rely on appropriate safeguards such as the EU Standard Contractual Clauses (and UK Addendum).

Contact

Privacy: privacy@k00l.app. We have not appointed a Data Protection Officer because the law does not currently require us to.
