DROP APPLICATION

Privacy Policy

Effective Date: October 29, 2026 | Last Updated: October 29, 2026

Drop Application LLC (“Drop,” “we,” “our,” or “us”) operates the Drop website, mobile and installable applications, and associated services (the “Service”). This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information. Our Terms of Service and Community Guidelines separately govern use of the Service.

Important location notice. With your device permission, Drop collects and processes location information while you use the Service and, where background location access is enabled, while the application is not actively open. This allows Drop to identify Drops near your location and send nearby-Drop notifications. Drop does not display your live device location to other users. Nevertheless, Drop locations, creation times, content, and collection activity can reveal or suggest where you have been. You can manage location permissions in your device settings; restricting background access may limit nearby alerts.

1 Information We Collect

Account and profile information. We process account identifiers, email address, display name, username, profile picture, biography, account status, and settings. When you sign in with Google or Apple, we receive the account and profile information authorized through that sign-in process, such as a provider account identifier, name, email address, and, where provided, profile picture. Apple may provide a private relay email address if you choose Hide My Email. Drop does not receive your Google or Apple password. Authentication and initial account records can be created during sign-in before you finish setting up your Drop profile. We retain encrypted Apple authorization information, accessible only to authorized backend processes, so we can revoke Drop’s Apple authorization when completing account deletion.

Location and map information. With permission, we process device coordinates, accuracy information, and location timestamps to support nearby discovery and eligibility checks for creating or collecting Drops. We store geographic positions associated with Drops. We also process the map area you browse to retrieve eligible Drops for that area. Moving the map to another place does not establish that you are physically there.

When nearby alerts are enabled and the necessary permissions are granted, we process location updates, including updates obtained in the background, to identify Drops in your vicinity and determine eligibility for notifications. We may maintain a recent-location record for this purpose. The feature is not intended to publish your live movements to other users; however, location updates are processed as needed for nearby discovery and alerts. Drop locations and collection records are separate from recent device-location information and may be retained longer.

Content and social activity. We process text, photos, short videos, comments, reactions, collection activity, selected profile highlights, friend and follow relationships, blocking relationships, and direct or inbox messages. We also process information about the recipients selected for private Drops. Uploaded media may contain embedded metadata; users should not assume that every type of metadata is removed from every upload.

Notifications, safety, and policy records. We process notification preferences, browser push subscriptions and native device push tokens where enabled, device or installation identifiers, platform and delivery status, notification activity, safety reports, and related review or enforcement records. Push registration associates an enabled device with the signed-in account. We also record policy acknowledgement information, including the account, acknowledgement time, document version, and relevant acknowledgement text or document reference.

Technical information. Our infrastructure and service providers may process IP addresses, browser and operating-system information, device or installation identifiers, app and SDK versions, request timestamps, map interactions, crash and performance information, errors, and security or access logs in providing the Service. The information varies by platform and provider. Map SDKs may process technical identifiers, usage and diagnostic information to operate, secure, and improve map services. Information collected by an independent provider is also subject to that provider's applicable notice.

Purchases, rewards, and support. When these features are offered, we process order identifiers, purchase amounts, currency, taxes and discounts, payment and refund status, purchased credits, reward eligibility, claim or redemption codes, business promotion requests, and support communications. For Stripe-hosted checkout, we send Stripe the checkout information needed to process and reconcile an order, such as the account email address, an account reference, order identifier, product, and amount. You enter payment details directly on Stripe's payment page. Drop does not receive or store the full card number or card security code through this integration. However, Drop can access limited payment information through Stripe, including the payment method, card brand, last four digits and expiration date where applicable, payment and transaction identifiers, and billing details such as name, email, country, postal code or billing address when supplied. The information available depends on the payment method and checkout. We use it for purchase fulfillment, payment support, refunds, fraud prevention, tax, accounting and legal obligations. We do not use payment or billing details for advertising or cross-app tracking.

2 How We Use Information

We use personal information to:

- Authenticate users and maintain accounts, profiles, settings, and policy acknowledgement records.
- Display maps and eligible Drops; support creating and collecting Drops; and check location-based eligibility.
- Deliver content to its permitted audience and support social activity, inbox messages, and profile highlights.
- Operate sponsored Drops, purchases, and reward redemption where offered.
- Deliver requested or enabled service notifications, including nearby and social-activity notifications.
- Respond to support requests and reports, investigate potential violations, prevent abuse, and enforce our rules.
- Diagnose errors, maintain security, and operate and improve the Service.
- Meet applicable legal obligations and address disputes or legal claims.

An acknowledgement of this Policy is not a substitute for device permission or any separate consent required by law. Where applicable, we obtain separate consent before processing sensitive information for a purpose that requires it.

3 Location Access and Notifications

How location is obtained. Drop requests location access through the applicable device, operating-system, or browser permission system. Google Maps displays map information; map display is distinct from the permission that allows Drop to obtain device coordinates.

Foreground and background use. When permitted, Drop processes location information during active use to show nearby Drops and check creation or collection eligibility. Where background location permission is enabled, Drop also processes location updates when the app is not actively being used to detect nearby Drops and support location-based notifications. The frequency and accuracy of location updates can vary with device settings, operating-system behavior, connectivity, and permission choices. Drop does not represent that every nearby Drop will trigger an alert.

Push notifications. Where supported and enabled, notifications may arrive while the Service is not open. Notification permission is separate from location permission. Notification previews may appear on a lock screen or another visible surface, potentially revealing information about nearby Drops.

Controls and limitations. You can restrict or revoke location and notification permissions in your device or browser settings and use the notification controls available in Drop. Restricting background location access may prevent nearby notifications from working as intended; revoking access may disable location-dependent features. Revocation does not itself erase previously collected records. Location readings may be inaccurate, stale, or delayed.

4 What Other Users Can See

Profiles and social activity. Other eligible users may see your display name, username, avatar, biography, profile counts, and selected public highlights. Your full owner gallery is distinct from your public profile. Following lists are available to the account owner and eligible mutual friends under the Service’s access rules.

Drop locations and content. Visibility depends on the Drop type and applicable eligibility, audience, blocking, and collection rules:

- **Public (Red) Drops:** Eligible users may see a Drop’s pin or discovery information. Follower activity may show an approximate area. Access to associated content can depend on collection and other access rules.
- **Private (Green) Drops:** Selected recipients who satisfy the applicable friendship and access rules can see the exact pin, including from outside the nearby-discovery area. Seeing the pin does not necessarily unlock the content; collection and other restrictions still apply. Share Green Drops only with people you personally know and trust. An in-app friendship does not verify a person’s identity or intentions.
- **Marketing (Blue) Drops:** Eligible users may see exact pins over a wider area, subject to the feature’s access rules. Associated content and rewards remain subject to applicable collection or redemption conditions.

Interactions and location inferences. A Drop’s creator may receive notifications identifying users who collect, like, or comment on that Drop. Comments and other interactions may be visible to users authorized to access them. Business creators can receive these interactions in the same way as other eligible creators. Repeated collection activity, Drop placements, and timestamps may allow other users to infer places you visit, even though Drop does not provide other users with a live device-location feed. Avoid sharing Drops or

interactions that reveal sensitive locations or another person's whereabouts without authorization. Use available blocking and reporting controls if someone misuses these features.

Display preferences are not audience controls. "Hide my Drops" changes your own Explore display; it does not make your Drops private to everyone else. Removing an activity item or circle from your map also does not erase the underlying Drop or other users' authorized access.

Copies and access by staff. Recipients may copy or redistribute information outside Drop. Blocking, removal, or account deletion cannot recall copies already made by others. Private features limit access by other app users; they are not a promise of end-to-end encryption or of inaccessibility to authorized personnel and providers supporting the Service.

5 Service Providers and Other Disclosures

Google. We use Google Maps on the web and through native mobile SDKs to display maps, and Google sign-in through Supabase for authentication. The website also requests Google Fonts and may display Google-hosted profile pictures. These integrations involve requests to Google and processing of associated technical, usage and diagnostic information. Use of Google Maps is subject to the applicable Google Maps/Google Earth Additional Terms of Service (https://maps.google.com/help/terms_maps/) and Google Privacy Policy (https://policies.google.com/privacy).

Supabase. We use Supabase for account authentication, database records, storage of uploaded photos and videos, and backend processing. Depending on the service and configuration, Supabase also processes operational logs and database backups. Data processed there includes the account, content, location, social, transaction, and policy records needed to operate Drop.

Hosting. Website hosting and delivery providers process requests and related technical information necessary to deliver and secure the Service.

Payments. We use Stripe for hosted checkout and, where offered, payment links or invoices. Stripe processes payment, billing and transaction information to provide its services, including payment security, fraud prevention and legal compliance. Drop can access the limited merchant payment and billing information described in Section 1. Stripe's privacy notice is available at https://stripe.com/privacy. Purchasing through a separate Stripe page does not mean that Drop receives no payment information.

Apple sign-in and push delivery. Apple provides Sign in with Apple and Apple Push Notification service for supported iOS features. Android push delivery uses Google's Firebase Cloud Messaging, and web push uses the browser's push service. These providers process authentication or device-delivery information and notification payloads needed for the selected feature. Notifications can include Drop or activity information and a link to the relevant screen. Apple's privacy notice is available at https://www.apple.com/legal/privacy/ and Google's at https://policies.google.com/privacy.

Email delivery. Email delivery providers deliver authentication, support or safety-report messages where enabled. Report emails can contain report text, the relevant Drop information, and reporter or creator identifiers. Reporting is not anonymous to Drop and its authorized service providers.

Automated content screening and safety review. Drop uses Google Cloud services, including Google Cloud Vision for visual content screening, to help assess user-submitted text, captions, messages, photographs, and videos for potential violations of our Terms of Service and Community Guidelines. This screening also applies to content submitted in Private (Green) Drops. Text, photographs, and videos may be

published immediately without waiting for automated screening results or human review. Content flagged as potentially harmful, or for which a safety check is incomplete, is referred to authorized moderators for review. Moderators may determine that content should remain available or be removed for violating our policies. Relevant content and associated technical information may be transmitted to and processed by Google Cloud and other service providers supporting these checks. Automated screening and human review may fail to identify harmful material or may flag permissible content; publication does not mean that Drop has approved or certified content as safe. Drop may also review user reports and related account information to investigate safety concerns.

Legal, safety, and business circumstances. We may disclose information to comply with applicable law or valid legal process, investigate credible threats or fraud, protect legal rights, or address security incidents, subject to applicable limits. Information may also be disclosed in connection with a merger, acquisition, restructuring, or sale of assets, with legally required protections and notices. We may disclose information at your direction or with your consent.

6 Sponsored Drops, Businesses, and Analytics

The Service may display sponsored Drops based on geographic relevance and applicable eligibility rules. Displaying a sponsored Drop is distinct from interacting with the business that created it.

When you collect, react to, comment on, or redeem a business's Drop, that business may receive information associated with the interaction, such as your displayed name, an activity notification, or a redemption code. Information you independently provide to a business, including during an in-person redemption, is subject to that business's practices.

Drop uses relevant content, location and eligibility information, account and device identifiers, and interaction records to display and fulfill Blue business promotions within the Service. This includes routing enabled notifications and handling collection or redemption activity. These in-app promotions are advertising, but Drop does not combine this information with data from other companies' apps or websites for cross-app advertising tracking, sell personal information to data brokers, or disclose users' precise device location or account activity histories to advertisers for independent ad targeting. Drop does not use customer lists for promotional campaigns. Business creators may nevertheless receive the user-visible interactions described above. We and our providers use operational, usage and diagnostic information to maintain and improve the Service, investigate errors, and address abuse. If we introduce materially different advertising or analytics practices, we will provide the notices, choices, and consents required by applicable law before beginning those practices.

7 Retention and Account Deletion

Retention while using Drop. Retention depends on the information and purpose. Account records and content support the active account and its features; Drop locations and collection records support discovery, access, and activity history. We also retain records as appropriate for security, support, policy acknowledgements, payment reconciliation, and applicable legal obligations.

Recent location information used for nearby alerts may be refreshed as newer readings arrive and may stop qualifying for alerts after its validity window expires. Expiration of that validity window is not a guarantee that the database record is erased at that instant. Similarly, a Drop becoming unavailable, expiring, or disappearing from a map does not by itself mean that all associated records or files have been erased.

Requesting deletion. You can request account deletion through the account-deletion feature or by contacting contact@dropapplication.com. After the in-app deletion request is successfully processed, the account is disabled, authored Drops are hidden, and certain associated records are removed. A deletion request is also recorded for completion of the remaining deletion steps. When completing permanent deletion of an Apple-linked account, Drop revokes the retained Apple authorization and removes the associated grant record. Email requests may require identity verification before account changes are made.

Permanent removal. Drop aims to complete removal of associated personal information from active systems within 48 hours after a successfully submitted in-app account-deletion request, subject to lawful retention exceptions. This includes applicable records in active databases, uploaded photos and videos in file storage, and the authentication account. These are separate steps and may require operator action. Email deletion requests may require identity verification before this process begins. The 48-hour period does not guarantee removal of residual backup copies or provider logs, which follow applicable retention cycles. We respond to privacy requests within periods required by law.

Backups and retained records. Residual copies may remain in backups or provider logs until the applicable provider retention cycle ends; such residual copies are not used for ordinary app functions and are subject to applicable access restrictions. We may retain specific information where necessary and legally permitted for accounting, credible safety reports (including threats or stalking), security investigations, dispute resolution, preservation obligations, or other legal requirements. Such retention is limited to the relevant purpose. Information independently copied by another user or business cannot be erased by Drop from that person’s systems.

8 Browser Storage and Privacy Choices

The Service uses browser or application storage and related technologies to maintain authentication sessions and remember preferences, such as whether to hide your own Drops in Explore. Push notifications, where enabled, also use a device subscription. Independent providers may use their own technologies in delivering their services, as described in their applicable notices.

You can sign out, change available account settings, edit your profile, manage selected highlights, block or unblock users, and adjust the permissions described above. Clearing browser or application storage can sign you out or reset preferences; it does not delete your account or erase information held in our backend systems.

9 Privacy Rights and Requests

Depending on your residence and the laws that apply to Drop, you may have rights to access, correct, delete, or obtain a copy of personal information; withdraw consent; object to or restrict certain processing; and opt out of qualifying sales, targeted advertising, or profiling. You may also have rights to appeal a decision, use an authorized agent, or complain to a competent privacy regulator.

Submit requests to contact@dropapplication.com. We may request information reasonably needed to verify your identity or an agent’s authority. We will explain applicable decisions and appeal procedures and respond within legally required periods. We will not unlawfully discriminate against you for exercising applicable privacy rights. Withdrawing permission or consent may affect features that depend on the relevant processing.

10 Security

We use technical and organizational safeguards designed to protect personal information, including authentication and access controls used by the Service and its providers. These measures do not eliminate all risk. Content reporting and moderation are safety processes and do not replace cybersecurity protections. We investigate suspected security incidents and provide notices where required by applicable law.

11 Age Restrictions

Drop is intended for individuals aged 18 or older. You must be at least 18 to register or use the Service. Google or Apple sign-in does not mean that Drop has verified a user's age.

If we learn that an individual under 18 is using the Service, we may restrict or terminate the account and handle associated personal information in accordance with applicable law. A parent, guardian, or other person who believes a minor has registered may contact contact@dropapplication.com.

12 Third-Party Links and Services

The Service may link to business websites or other third-party services. Information you provide directly to those services is governed by their own notices and practices. This Policy describes Drop's practices and does not replace the notices of independent providers, businesses, or other recipients.

13 International Processing

Drop is operated by a United States company. Information may be processed in the United States and other locations where our providers operate. The applicable locations and protections depend on the services used and their configuration.

14 Changes to This Policy

We may update this Policy to reflect changes in our practices, features, or legal obligations. We will update its date and provide additional notice or obtain consent when required. A revised Policy does not itself authorize new processing where separate consent is required. Historical acknowledgement records relate to the version presented to the user at the time.

15 Contact

Drop Application LLC

Lubbock, Texas, United States

Website: https://www.dropapplicationllc.com/

Privacy inquiries and requests: contact@dropapplication.com

Safety reports: support@dropapplication.com