

LifeWrap Privacy Policy

Effective Date: June 21, 2026 **Last Updated:** June 21, 2026

This Privacy Policy explains how **LifeWrap LLC** ("**LifeWrap**," "**we**," "**us**," or "**our**") collects, uses, discloses, and protects information about you when you use the LifeWrap mobile application and any related websites or services (collectively, the "**Service**").

By using the Service, you acknowledge the practices described in this Privacy Policy. If you do not agree, you must not use the Service.

Quick Reference

- **Who we are:** LifeWrap LLC, a California limited liability company.
- **Service type:** A social networking and lifestyle application for users 18 and older.
- **Where we operate:** United States, European Union, United Kingdom.
- **Contact for privacy questions:** privacy@lifewrap.app
- **EU/UK Representative:** [EU REPRESENTATIVE — REQUIRED BEFORE PUBLICATION]
(required if you offer the Service in the EU/UK; see Section 14)

1. Information We Collect

We collect information in three ways: (a) information you provide to us, (b) information collected automatically, and (c) information from third parties.

1.1 Information You Provide

Category	Examples
Account Information	Name, email address, password (stored hashed), username, date of birth, profile photo
Profile Information	Bio, profile preferences, settings

User Content	Photos, videos, captions, activity logs, journal entries, location tags you add to entries, names or handles of people you tag, comments
Communications	Messages you send to us (e.g., support requests, feedback)
Survey/Feedback	Optional responses to surveys or research we conduct

1.2 Information Collected Automatically

Category	Examples
Device Information	Device model, operating system and version, unique device identifiers (e.g., IDFV), language, time zone, mobile carrier (where available)
Usage Information	Features accessed, screens viewed, taps, in-app actions, session duration, dates and times of access, error and crash data
Approximate Location	Approximate location derived from your IP address (city/region level), unless you grant precise location permission
Precise Location <i>(only if you grant permission)</i>	GPS-based location data tied to specific entries you create
Log Data	IP address, device timestamps, referring URLs, app version

1.3 Information from Other Sources

- **Sign-In Providers:** If you sign in using **Apple** Sign-In or another supported sign-in provider, we receive the information that provider shares with us in accordance with your privacy settings (typically a name and an email or relay address).
- **Other Users:** Other users may tag you, mention you, or include your name in their User Content. We may receive that information about you even if you do not have an account.

1.4 iOS Permissions

The Service may request the following iOS permissions. You may grant or deny these at any time in your device settings. **Denying a permission may limit certain features.**

Permission	Why We Request It
Camera	To capture photos and videos directly within the Service.

Photos	To allow you to select photos and videos from your library to add to entries.
Notifications	To send you transactional and engagement notifications.
Location (optional)	To attach approximate or precise location to entries you create, only if you choose.

Location safety. Location information can reveal sensitive details about you, including your home, workplace, routines, and real-time whereabouts. We grant you control over whether and when you share location, and we encourage you to review your privacy settings and to avoid sharing precise or real-time location where it could compromise your safety. Please see the “Safety, Location Information, and Assumption of Risk” section of our Terms of Service for important information about the risks of sharing location.

1.5 Sensitive Information

We do not intentionally collect government identifiers, health data (we do not access HealthKit), biometric identifiers, or precise geolocation unless you specifically grant precise location permission. We do not perform automated face recognition on photos. **Please do not share sensitive information through the Service unless you choose to do so as User Content; any User Content you publish is at your own risk.**

2. How We Use Information

We use information for the following purposes:

Purpose	Examples
Provide the Service	Create and maintain your account, store and display your User Content, enable tagging and social features, provide customer support
Operate and improve	Analyze usage, debug, fix errors, develop new features, conduct internal research
Personalize	Tailor your in-app experience, recommend content or activities
Communicate	Send transactional notifications (account, security, service updates), respond to inquiries
Engagement (only as	Send promotional notifications about new features (you can opt out)

<i>permitted)</i>	
Safety and integrity	Detect, prevent, and address fraud, abuse, security incidents, and violations of our Terms of Service
Legal compliance	Comply with legal obligations, respond to lawful requests, enforce our agreements
Aggregated/de-identified analytics	Generate aggregate statistics that do not identify you personally
Train or improve product features	We use de-identified or aggregated content to operate and improve the Service, including its search, recommendation, and safety features. We do not use identifiable User Content to train generative AI models, and we do not share your User Content with third parties to train their generative AI models, except with your explicit, opt-in consent.

2.1 Legal Bases (EU/UK Users)

If you are in the EU or UK, we rely on the following legal bases under GDPR and UK GDPR:

- **Performance of a contract** (Article 6(1)(b)) — to provide the Service you have requested.
- **Legitimate interests** (Article 6(1)(f)) — for analytics, security, abuse prevention, and product improvement, balanced against your rights.
- **Consent** (Article 6(1)(a)) — for optional features that require permission, such as precise location, marketing communications, or any future tracking-based advertising. You may withdraw consent at any time.
- **Legal obligation** (Article 6(1)(c)) — to comply with applicable laws.

3. How We Share Information

We do not sell your personal information for money. We do not “share” your personal information for cross-context behavioral advertising as those terms are defined under the California Consumer Privacy Act (“**CCPA**”) as amended by the California Privacy Rights Act (“**CPRA**”). We share information only as follows:

3.1 With Other Users

User Content you choose to make visible — including profile information, photos, captions,

and tags — is visible to other users in accordance with your privacy settings within the Service. **Anyone who can see your User Content may copy, screenshot, save, or redistribute it; once shared, we cannot control how others use it.**

3.2 With Service Providers

We share information with third-party vendors who provide services on our behalf, only to the extent necessary for them to perform those services and under contractual obligations to protect your information. Our service providers include:

⚠ **Verify before publishing.** The provider list below reflects a typical configuration and MUST be reconciled against your production build and your App Store Connect “Data Collection” / privacy-label answers before this Policy goes live. Any SDK that collects user or device data and is not listed here is both a disclosure gap and an App Store review risk.

Function	Provider
Authentication	Apple Sign-In; Supabase Authentication
Backend hosting and storage	Supabase; Vercel
Image and media storage / CDN	Supabase Storage
Crash and performance monitoring	Sentry
Product analytics	PostHog
Email delivery	Resend
Push notifications	Apple Push Notification service; Expo push notifications
Customer support	Not applicable at launch

A current list of our material subprocessors is available upon request at privacy@lifewrap.app.

3.3 Legal and Safety Disclosures

We may disclose information when we believe in good faith that disclosure is necessary to:

- (a) comply with applicable law, regulation, legal process, or governmental request;
- (b) enforce our Terms of Service, including investigation of potential violations;

- (c) detect, prevent, or address fraud, security, or technical issues;
- (d) protect against harm to the rights, property, or safety of LifeWrap, our users, or the public, as required or permitted by law; or
- (e) respond to a verified claim of intellectual property infringement.

3.4 Business Transfers

If LifeWrap is involved in a merger, acquisition, financing, reorganization, bankruptcy, or sale of all or a portion of its assets, your information may be transferred as part of that transaction. We will notify you (e.g., via email and/or notice on the Service) of any such change in ownership or control.

3.5 With Your Direction or Consent

We may share information with third parties when you direct us to do so or otherwise consent.

3.6 Aggregated and De-identified Information

We may share aggregated or de-identified information that cannot reasonably be used to identify you for any purpose.

4. Tracking, Cookies, and App Tracking Transparency

4.1 In-App Tracking

The Service uses limited first-party analytics to understand usage. **We do not currently use the Service to track you across other companies' apps and websites for advertising purposes.** If we ever change this, we will request your permission through Apple's **App Tracking Transparency ("ATT")** prompt and update this Policy.

4.2 Cookies and Similar Technologies (Website)

Our website **lifewrap.app** uses only strictly necessary cookies required to operate the site. We do not use non-essential, advertising, or cross-site tracking cookies on the website. If this changes, we will update this Policy and obtain your consent where required.

4.3 Do Not Track

Our Service does not currently respond to "Do Not Track" browser signals. We do honor verified **Global Privacy Control (GPC)** signals from California residents as a request to opt

out of “sale” or “sharing” under CCPA.

5. Data Retention

We retain personal information for as long as necessary to:

- provide the Service to you;
- comply with our legal, accounting, or reporting obligations;
- resolve disputes; and
- enforce our agreements.

When we no longer need personal information, we will delete or anonymize it. Specific retention guidelines:

Data	Retention
Account information	Until you delete your account, plus up to 30 days for backup purging
User Content	Until you delete it or your account, plus up to 30 days for backup purging
Server logs	Up to 90 days , except where required for security incident review
Analytics data	De-identified or aggregated within 24 months
Records required by law (e.g., tax, fraud)	As required by applicable law

6. Security

We implement reasonable administrative, technical, and physical safeguards designed to protect your information, including encryption in transit (TLS) and encryption at rest where supported by our service providers, role-based access controls, and audit logging.

No method of transmission or storage is 100% secure. While we strive to use commercially acceptable means to protect your personal information, we cannot guarantee its absolute security. You are responsible for keeping your account credentials confidential.

If you suspect unauthorized access to your account, contact us immediately at security@lifewrap.app.

7. Your Choices and Controls

Control	How to Use
Edit your profile and content	Within the app, you can edit, delete, or hide individual entries and profile fields.
Notification settings	Adjust within the app or in iOS Settings → Notifications → LifeWrap.
Photos / Camera / Location / Contacts permissions	iOS Settings → Privacy & Security → the relevant permission (Camera, Photos, Location) → LifeWrap.
Marketing emails	Click “unsubscribe” in any marketing email. Transactional emails (e.g., security, account) cannot be opted out of while your account is active.
Delete your account	In the app: Settings → Account → Delete Account , or email privacy@lifewrap.app with the subject “Account Deletion.” See Section 8.

8. Account Deletion

You may delete your account at any time using the in-app deletion flow at **Settings → Account → Delete Account**, or by contacting us at privacy@lifewrap.app. When you delete your account:

- Your profile and User Content will be removed from public visibility within the Service within **30 days**;
- Backups containing your information will be purged in the ordinary course of our backup rotation, typically within **30–60 days**;
- We may retain a minimal record of your deletion request for legal and audit purposes; and
- **Content you have shared with other users (e.g., a photo a user has saved or**

screenshotted, or content already received by another user) is outside our control and may persist.

9. Children's Privacy

The Service is **not directed to children under the age of 18**. We do not knowingly collect personal information from anyone under 18. If you believe a person under 18 has provided personal information to us, please contact privacy@lifewrap.app and we will take prompt steps to delete that information.

10. California Privacy Rights (CCPA / CPRA)

If you are a California resident, you have the rights described in this Section. The categories below mirror the CCPA's enumerated categories of personal information.

10.1 Categories of Personal Information We Collect, Disclose, "Sell," or "Share"

CCPA Category	Collected?	Disclosed for a Business Purpose?	"Sold"?	"Shared" for Cross-Context Behavioral Advertising?
Identifiers (name, email, IP, device ID, account ID)	Yes	Yes (to service providers)	No	No
Customer records (Cal. Civ. Code §1798.80)	Yes	Yes	No	No
Commercial information	Limited (in-app purchases, if any)	Yes	No	No
Internet/network activity	Yes	Yes	No	No
Geolocation data (approximate; precise only with	Yes	Yes	No	No

permission)				
Audio/visual information (photos, videos you upload)	Yes	Yes (to storage providers)	No	No
Inferences from the above	Yes (limited; for product features)	Yes	No	No
Sensitive personal information	We do not use sensitive personal information for purposes that require disclosure under CPRA §7027.			

We do not knowingly sell or share personal information of minors under 16.

10.2 Your California Rights

You have the right to:

- **Know** what personal information we have collected, used, disclosed, and (if applicable) sold or shared;
- **Access** a copy of your personal information in a portable format;
- **Delete** personal information we hold about you, subject to applicable exceptions;
- **Correct** inaccurate personal information;
- **Limit** the use and disclosure of sensitive personal information (we do not use SPI in ways that trigger this right);
- **Opt out** of the sale or sharing of your personal information (we do not sell or share, but you may submit a request as a precaution); and
- **Non-discrimination** for exercising your rights.

10.3 How to Exercise California Rights

Submit a verifiable consumer request by:

- Email: privacy@lifewrap.app with the subject line "California Privacy Rights"
- Postal mail: **LifeWrap LLC, Attn: Privacy, [MAILING ADDRESS — REQUIRED BEFORE PUBLICATION]**

We will verify your identity using account information and may require additional verification for sensitive requests. You may use an authorized agent to make a request on your behalf, subject to verification of the agent's authority.

We will respond within **45 days** of receipt, with a possible extension of an additional 45 days where reasonably necessary, with notice to you.

10.4 Shine the Light

California Civil Code §1798.83 permits California residents to request information regarding our disclosure of personal information to third parties for direct marketing purposes. **We do not disclose personal information to third parties for their direct marketing purposes.**

11. Other U.S. State Rights

Residents of other U.S. states, including without limitation **Colorado, Connecticut, Delaware, Iowa, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia**, may have rights similar to those described in Section 10, subject to the requirements and exceptions of their applicable state privacy laws. To exercise any such rights, contact privacy@lifewrap.app. We will respond within the timeframe required by your state's law.

12. EU/UK Privacy Rights (GDPR / UK GDPR)

If you are in the European Economic Area, the United Kingdom, or Switzerland, you have the following rights under applicable law:

Right	Description
Access	Request confirmation of whether we process your personal data and a copy of that data.
Rectification	Request correction of inaccurate or incomplete personal data.
Erasure ("Right to be Forgotten")	Request deletion of your personal data, subject to applicable exceptions.
Restriction	Request that we restrict the processing of your personal data in certain circumstances.
Portability	Receive your personal data in a structured, commonly used, machine-

	readable format and transmit it to another controller.
Objection	Object to processing based on legitimate interests, including profiling.
Withdraw Consent	Withdraw consent at any time where processing is based on consent (without affecting the lawfulness of prior processing).
Lodge a Complaint	Lodge a complaint with your local supervisory authority (e.g., the UK ICO at ico.org.uk , or the relevant EU DPA).

To exercise any of these rights, contact privacy@lifewrap.app. We will respond within **one month**, with a possible extension of two additional months for complex requests, with notice to you.

12.1 Data Controller

For EU/UK users, **LifeWrap LLC** is the data controller of your personal information. Our contact details are in Section 17.

12.2 EU/UK Representative

[EU & UK REPRESENTATIVES — REQUIRED BEFORE PUBLICATION]

⚠ **Action item:** If you have not yet appointed an EU/UK representative, you must do so before launching in those regions. Common providers include Prighter, EDPO, and VeraSafe.

13. International Data Transfers

LifeWrap is based in the United States, and our service providers may operate from, or store data in, the United States, the European Economic Area, the United Kingdom, and other jurisdictions. When we transfer personal information outside of your country of residence, we use appropriate safeguards, including:

- the **EU Standard Contractual Clauses** and the **UK International Data Transfer Addendum** (or UK IDTA), where applicable; and
- supplementary technical and organizational measures such as encryption.

You may request a copy of the relevant transfer mechanism by contacting privacy@lifewrap.app.

14. Automated Decision-Making

We do not engage in solely automated decision-making that produces legal effects concerning you or similarly significantly affects you under GDPR Article 22. We may use limited automated features (e.g., recommendation logic, abuse detection) that do not have such effects.

15. Third-Party Links and Services

The Service may contain links to or integrate with third-party websites, services, or content. This Privacy Policy applies only to LifeWrap. We are not responsible for the privacy practices of any third party. We encourage you to review their privacy policies before providing them with information.

16. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you by (a) posting the updated Privacy Policy in the Service, (b) updating the "Last Updated" date, and/or (c) sending notice to the email address associated with your account. **Your continued use of the Service after the effective date of any change constitutes your acceptance of the updated Policy.**

17. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or your personal information, please contact us:

LifeWrap LLC [MAILING ADDRESS — REQUIRED BEFORE PUBLICATION] Email: privacy@lifewrap.app

Data Protection Officer / Privacy Lead: the LifeWrap Privacy Team EU Representative (Article 27 GDPR): [REQUIRED BEFORE PUBLICATION] **UK Representative (Article 27 UK GDPR):** [REQUIRED BEFORE PUBLICATION]

This Privacy Policy is provided in English. Translations are for convenience only; in the event of a conflict, the English version controls.

