LEGAL · HERSPACE

Privacy Policy

How HerSpace handles your personal information, including local records, AI processing, subscriptions and your rights.

Last updated · 26 October 2026 · **Operated by** · Higher Detail Limited

In short: Your personal entries primarily stay on your device. We use outside providers for sign-in, subscriptions, optional AI and certain operational functions. This notice explains what leaves your device, why and the choices available to you.

Who we are

HerSpace is a personal wellbeing and confidence-building application operated by **Higher Detail Limited** (company number **10640477**), a company registered in England and Wales.

Higher Detail Limited is the controller responsible for the personal data we process to provide HerSpace, except where another organisation independently determines how and why it uses information.

Registered office: 7 Theobalds Court, Crossbrook Street, Cheshunt, Waltham Cross, EN8 8EB, United Kingdom.
Privacy contact: privacy@higherdetail.com.

This notice applies to the HerSpace iOS app and to relevant enquiries you send us. Our app is intended for adults aged 18 or over. We do not knowingly offer accounts to children.

At a glance

HerSpace is designed to keep your personal wellbeing entries on your device. We nevertheless use external services for sign-in, optional AI conversations, subscriptions and limited operational functions. Content you send to an AI feature leaves your device.

- **You control what you record.** You can use features such as journaling, check-ins, Proof and planning without submitting that content to the AI Companion.
- **AI requires separate permission.** Messages, selected conversation context and sometimes relevant Proof excerpts are sent to Google Gemini only when you choose to use AI features and the relevant permission is in place.
- **No advertising use of your reflections.** We do not sell your journal, worries, Proof or AI conversation content or use it for behavioural advertising.
- **Product analytics are optional.** They are off by default; essential security and reliability processing is treated separately.
- **Deletion and privacy rights.** You can delete your account in the app and contact us to exercise additional rights. Some third-party records follow separate retention schedules.

What information we handle

Category	Examples and how we obtain it
Account and authentication	Email address, Supabase account ID, authentication provider, sign-in identifiers, session information and account status. Supplied by you and, where used, Apple or Google sign-in.
Profile and preferences	Display name, optional profile picture, confidence goals, companion style, reminder settings and app-lock preferences. Supplied by you in the app.
Wellbeing entries	Check-ins and feelings, journal entries, parked worries, saved Proof and photographs, small wins, upcoming Brave Moments, debriefs and fear-ladder steps. Supplied by you; primarily saved locally.
AI feature content	Messages, relevant saved conversation context and summaries, limited selected Proof excerpts, and role-play scenarios and dialogue. Selected or entered by you for AI features.
Calendar information	Event details from device calendars that you select or authorise, such as title and time, used to display and prepare for upcoming events.
Subscription records	Product, plan, payment or trial status, entitlement, transaction identifiers, renewal or expiry information supplied by Apple and RevenueCat. We do not receive your full card number.
Technical and operational data	Device or app version, approximate network information, request identifiers, errors, usage/latency metrics and security events where required to run the service.
Communications	Messages you send to our support or privacy address and information necessary to respond.

Free-form entries can reveal sensitive information, including health or mental-health information, even though HerSpace does not ask you for a medical diagnosis. Please avoid entering information about someone else unless you have a good reason and the right to do so.

What stays on your device

HerSpace stores much of your personal content locally using app-managed files and an SQLite database. That includes journals, check-ins, Proof, photos, worries, Brave Moments, imported calendar data and completed Companion conversations. This content is not generally synchronised to a HerSpace cloud-content account.

Local does not mean the information can never leave your phone. You may choose to share an export using the iOS share sheet; relevant content may be transmitted to Gemini when you make an AI request; and your device may create operating-system backups under your Apple settings.

The device operating system manages Face ID or other device authentication. HerSpace uses the success or failure of the device authentication check; it does not collect a copy of your face or fingerprint templates.

Device changes and backups: signing in on a different phone does not guarantee restoration of locally saved entries. Deleting the app or losing access to your device may mean your local content cannot be recovered. Device-backup copies may be managed separately by Apple.

How AI processing works

HerSpace uses the paid **Google Gemini API** through authenticated Supabase server functions to provide the AI Companion and conversational role-play.

When you submit an AI request, we transmit the text you submit and context needed to produce a response. Depending on the feature, this may include recent messages, an earlier-conversation summary, your selected communication style, relevant text snippets from saved Proof, or a role-play scene and its recent dialogue. We do not send your entire local journal or Proof library simply because you open the Companion.

Requests may also be screened for safety and misuse. AI-generated replies can be inaccurate or inappropriate; neither the Companion nor its role-play characters are clinicians or emergency responders.

Paid API and provider retention: under Google's current terms for paid Gemini API services, Google does not use ordinary API prompts and responses to improve its general products. We have disabled optional developer prompt/response logging and voluntary data contribution for our production configuration. Separately, Google states that it retains prompts, supplied context and responses for **55 days** for abuse monitoring and related security purposes, potentially including limited human review. The optional seven-day developer-log retention setting does not shorten that separate period.

Completed Companion conversations are saved on your device. Role-play dialogue is used in the active rehearsal session and is not intentionally saved as a permanent local transcript. An unfinished AI exchange can be lost if the app closes unexpectedly.

We do not use your personal entries to train a HerSpace AI model. Details of Google's separate processing are available in its Gemini API Terms and abuse-monitoring explanation.

Calendars, reminders and exports

If you allow device-calendar access, HerSpace reads the selected calendar data required for its planning features. Access is read-only: we do not create, change or delete the original calendar event. Selected event information is cached on your device.

HerSpace can schedule discreet device notifications and maintain a local in-app reminder history. Notification permission can be changed in iOS settings and, where available, in HerSpace settings. The contents of notifications are designed not to disclose feelings.

You can export certain journal and Proof records as plain-text files and choose a destination using the iOS share sheet. Once you share a file, the receiving app or service controls its own use and retention of the copy.

Why we process data and our lawful bases

When UK or EU data-protection law applies, we identify a lawful basis for each purpose. Depending on the circumstances, these are:

Purpose	Typical basis under UK/EU GDPR
Registering and authenticating your account; delivering requested app functions	Necessary to perform our contract with you (Article 6(1)(b)).
Providing wellbeing reflections and records you choose to create	Contract for ordinary personal data. Where entries amount to special-category health information, an additional Article 9 condition is required; we use explicit consent where it is the applicable condition.
Sending chosen content for optional AI replies and role-play	Consent to the optional processing and, where required, explicit consent for special-category information.
Optional product analytics	Your consent, where applicable.
Detecting misuse, securing accounts, fixing faults and managing reasonable usage limits	Our legitimate interests in operating a safe, reliable service, balanced against your rights (Article 6(1)(f)); or a legal obligation where applicable.

Purpose	Typical basis under UK/EU GDPR
Processing subscriptions and purchases	Contract, and legal obligation for records we must retain.
Answering enquiries and privacy requests	Contract, legitimate interests or legal obligation, depending on the request.

Where the law requires consent, you are told what you are agreeing to and may withdraw it. The legal basis and any special-category condition can differ in other countries. Essential security processing does not depend on optional analytics consent.

Sensitive information and consent

Information about your feelings or difficult experiences is not always legally classified as health information, but some entries may identify your mental-health status or another sensitive characteristic. We apply additional protections and seek specific consent where required by applicable law.

Consent for wellbeing information and consent for optional third-party AI processing are separate choices. Accepting one does not automatically enable the other. If you decline a particular optional processing activity, features requiring it may not be available.

Where we rely on your consent, you can withdraw it at any time through the relevant app control, where available, or by contacting privacy@higherdetail.com. Withdrawal does not undo processing lawfully carried out before the withdrawal. We will explain the effect on any features that need the information.

Analytics and diagnostics

We use **PostHog EU Cloud** for feature availability, diagnostics and, where you have opted in, product analytics. Optional product analytics are **disabled by default**. They are intended to measure feature use rather than capture the contents of journal entries, worries or AI conversations.

Some necessary technical and security processing may take place without optional analytics consent, including authentication events, server-side request allowances, service errors and limited AI token/latency measurements when configured. These events should not contain your raw reflection or conversation text.

HerSpace does not send marketing emails at launch. We may send essential transactional messages relating to sign-in, account security or a significant change to the service.

When we share information

We share only the information reasonably required with the providers that support the relevant feature. The main services are:

Provider	Role and information involved
Supabase	Authentication, account identifiers, backend functions, subscription entitlement projections and service-related records.
Google Gemini	AI prompts, relevant context, generated responses and safety-related processing for AI features you invoke.
PostHog	Feature flags, diagnostics, usage and optional product analytics according to our configuration and your choices.
RevenueCat	Subscription identifiers, purchase status and Pro entitlement information.

Provider	Role and information involved
Apple	App distribution, in-app purchases, subscription billing, device notifications and Apple sign-in where used.
Google sign-in	Authentication information when you choose a Google account to sign in.

Our providers may use vetted subprocessors and, for certain activities, may act as independent controllers under their own terms. We may also disclose information where legally required, to protect rights and safety, or as part of a lawful business transaction subject to appropriate safeguards.

We do not sell your personal wellbeing entries or use them for targeted advertising.

Where information is processed

Our current core Supabase project is hosted in the **United Kingdom (London)**, and our PostHog project uses the **European Union cloud region**. This does not mean that every service, edge function, support operation or subprocessor processes information only in those locations.

Google, RevenueCat, Apple and certain subcontractors may process or access information from other countries, including outside the UK and European Economic Area. Google's Gemini API terms expressly allow certain abuse-monitoring data to be stored or cached in countries where Google or its agents maintain facilities.

When required, international transfers rely on applicable adequacy decisions, contractual safeguards such as standard contractual clauses or the UK international-transfer arrangements, or another lawful mechanism. You may contact us for information about relevant safeguards.

How long we keep information

Retention varies by category, location and provider. Our chosen service-retention limits are summarised below; legal obligations, security investigations and independent-provider terms can require different periods.

Category	Retention approach
Local journals, Proof, check-ins, worries and completed conversations	Until you delete them, delete your account, or the app/device removes the local data; device-backup copies follow the backup provider's rules.
Account and authentication information	While the account exists, then deleted from active HerSpace systems through account deletion, subject to provider and legally required records.
Optional product analytics	Target maximum of 12 months.
Application security and technical logs	Target maximum of 30 days, unless needed for an ongoing security investigation or legal obligation.
AI usage/cost measurements without conversation text	Target maximum of 90 days.
Gemini AI prompts, context and responses used for abuse monitoring	Google currently states a 55-day provider-side period, separate from our disabled optional developer logging.
App Store and subscription histories; backup and audit records	According to applicable law and the relevant provider's retention and deletion procedures.
Privacy or support enquiries	Only as long as necessary to respond, manage follow-up and meet applicable legal requirements.

The 12-month, 30-day and 90-day limits are our intended operating limits for systems we configure and control. They do not shorten independent provider retention. You can ask us about a specific category or request deletion where the law permits.

Account deletion and copies

You can initiate permanent account deletion in the app through **Me → Account → Delete my account and data**. This removes your Supabase authentication account and related active backend records, and starts account-specific local cleanup on the device, including app-managed photos and scheduled notifications. If interrupted, the app is designed to resume cleanup.

Because some records are held only on a particular device, we cannot directly erase an offline device or an Apple-managed backup from our servers. Records held by RevenueCat, Apple, PostHog or Google are not necessarily erased by the in-app deletion function and may require additional requests, provider processing or the expiry of permitted retention periods.

Deleting your HerSpace account does not cancel an active App Store subscription. Cancel that subscription separately through your Apple account to avoid further renewals.

You can delete some entries individually and export your journal and Proof as text files. For other access, deletion or portability requests, email privacy@higherdetail.com.

Your choices and privacy rights

- **Access, correction and portability:** request details about information we hold, correct inaccurate account information and obtain a copy of eligible information.
- **Deletion:** request deletion of eligible information or permanently delete your account.
- **Consent:** withdraw consent where that is our basis for processing. You may stop optional AI processing separately.
- **Objection and restriction:** object to or limit certain processing where available under applicable law.
- **US state rights:** where applicable, request access, correction or deletion; opt out of covered sale, sharing, targeted advertising or profiling; or appeal a decision on a privacy request.
- **Complaints:** contact your local privacy regulator or data-protection authority when the law provides that right.

We do not sell personal data or share it for cross-context behavioural advertising. We do not use AI-generated replies to make decisions that produce legal or similarly significant effects about you.

To make a request, email privacy@higherdetail.com. We may ask for enough information to verify identity and protect your records. We will respond within the period required by applicable law and explain any valid exception.

Regional notices

People in the UK and EEA have the rights described by their applicable data-protection laws, including the right to complain to a supervisory authority. Our UK lead contact is Higher Detail Limited at the address above; UK residents may also contact the Information Commissioner’s Office.

Where California or other US state privacy laws apply, we provide the rights available under those laws and do not discriminate unlawfully for exercising them. Other countries, including Canada, Brazil and Australia, may provide additional rights.

Some information handled by HerSpace may be regulated as **consumer health data** under Washington State law. Where that law applies, a dedicated consumer health data privacy policy and additional rights and controls may be required alongside this general notice.

Security

We use account authentication, restricted database access, session protection and device-based controls to help secure the service. Optional device locking relies on iOS-provided authentication. We limit the sensitive content sent to our operational analytics and AI services.

No method of storage or transmission is perfectly secure. Your device settings, backups and the other apps to which you export information can also affect security. Please protect your account and report suspected unauthorised access to us.

Changes to this policy

We may update this Privacy Policy as the app, law and providers change. We will post the revised date on this page and give additional notice or seek renewed consent where legally required. Material new uses of sensitive information will not be introduced solely by silently changing this document.

Contact

Higher Detail Limited
Company number 10640477
7 Theobalds Court, Crossbrook Street
Cheshunt, Waltham Cross, EN8 8EB
United Kingdom

Email: privacy@higherdetail.com
Website: herspaceapp.com
Terms of Service: herspaceapp.com/terms