Privacy Policy

Last updated: May 21, 2026
Applies to Memory Vault web and iOS unless stated otherwise.

This policy document is a practical product draft for the Memory Vault web and iOS app. It should be reviewed and adapted by the app owner or legal counsel before public release, especially if the operator, jurisdiction, analytics, support process, or third-party service list changes.

Scope and summary

This Privacy Policy explains how Memory Vault handles information when you use the web app or the related iOS app.

iOS app note: the iOS app is intended to use the same Memory Vault account, Cloudflare Worker API, D1 database, privacy model, sharing model, and magic-link authentication as the web app. Unless an iOS-only item is explicitly stated, the same policy applies to both web and iOS use.

Memory Vault is a personal memory-management application. It lets users create memory entries, organize those entries with people, labels, dates, locations, and confidence markers, view them on timelines, maps, and bubble-style visualizations, connect with trusted people, share selected public memories, review suggested edits, and generate AI-assisted narratives from selected memories.

The product is designed to minimize unnecessary data collection. The app does not need advertising identifiers and is not intended to sell personal data or track users across unrelated apps or websites.

Information you provide or create

- Account information: email address used for passwordless magic-link sign-in, profile name, birth date or age fields if you add them, birth place, current location, short bio, and public share ID.
- Memory content: titles, text, time fields, date precision, labels, people tags, context notes, locations, privacy level, confidence level, status, edit history, imported/shared-memory metadata, and related revision data.
- Connection and sharing data: connection requests, verification prompts and responses, person-link mappings, shared public memories, imported memory metadata, and edit suggestions.
- Encryption setup data: encryption salt, encrypted verification/check data, encrypted payload metadata, and encryption version. Your passphrase should not be sent to the server by the normal app workflow.
- Support or issue-report data: any information you choose to include when reporting a problem.

Private and ultra-private memories are intended to be encrypted in the client before being stored. Public memories remain readable by the service so that sharing, comparison, maps, timelines, and AI features can work. If a private or ultra-private memory is decrypted in the app and then deliberately included in an AI request, its decrypted text may be sent for that request.

Information generated automatically

- Authentication/session data needed to keep you signed in and protect API access.
- Operational logs and request metadata produced by the hosting, database, email, and AI providers, such as IP address, user agent, timestamp, endpoint, error details, and delivery status.
- Location-cache records derived from memory location names so map features can display coordinates without repeatedly geocoding the same places.

- Local app/browser state such as session token, selected view, temporary unsaved draft, map/geocode cache, and translation preferences.

The web app includes Google Translate integration. If you use translation, Google may process the page text and may set translation-related cookies. Translation is optional.

How information is used

- Provide login, account access, vault storage, editing, export, import, timeline, map, bubble, profile, and sharing features.
- Send magic-link emails and optional connection notifications through the configured email provider.
- Generate AI narratives only when you request them and based on the selected memory scope.
- Maintain security, prevent unauthorized access, troubleshoot problems, and improve reliability.
- Comply with legal obligations and enforce acceptable-use rules.

Third-party services and processors

Service or category	Purpose	Typical data involved
Cloudflare Workers and D1	API hosting, database storage, routing, caching, operational security	Account, memory, profile, sharing, connection, request, and log metadata
Resend or configured email provider	Magic-link login and optional notification email delivery	Email address, message metadata, delivery logs
OpenAI API or configured AI provider	AI narrative generation when requested	Selected memory text and prompt content sent for that request
Leaflet/OpenStreetMap map tiles	Interactive map display	Map tile requests and general request metadata
Google Translate	Optional page translation in web app	Page text and translation-related browser cookies when translation is used

If the iOS app adds Apple services such as TestFlight, App Store distribution, crash diagnostics, or iCloud in the future, those should be reflected in the App Store privacy details and in this policy before release.

Sharing and visibility

Memories marked public may be shared with accepted connections and may be used for connection timeline comparisons. Private and ultra-private memories should not be shareable through the normal sharing workflow.

A connection does not automatically receive your whole vault. Sharing is intended to be explicit, memory-specific, and revocable where the interface supports it. Imported copies may become separate records in the receiving user's vault.

AI narrative use

AI narrative generation is user-initiated. The app narrows or selects memories based on your chosen scope and sends the relevant prompt and memory evidence to the configured AI provider. AI output may be inaccurate or incomplete and should be treated as assisted drafting, not a definitive record.

Do not include highly sensitive private or ultra-private memories in an AI request unless you are comfortable with those decrypted contents being processed by the configured AI provider for that request.

Your choices and rights

- You can edit or delete individual memories, labels, and people records where the app provides controls.
- You can export your memories through the export features available in the web app.
- You can choose whether to create public, private, or ultra-private memories.
- You can decline or revoke sharing where the app provides those controls.
- You may request access, correction, deletion, or account-level assistance through the support channel.

Apple account-deletion note: if the iOS app allows account creation or sign-in, Apple generally expects account deletion to be available from within the app or clearly reachable from the app. If full account deletion is not yet implemented in the shared Worker, add it before App Store submission or provide a compliant in-app deletion request workflow.

Security

Memory Vault uses passwordless magic-link sign-in and authenticated API requests. Private and ultra-private memory text is intended to be encrypted before server storage. The strength of this protection depends on the correct implementation of the app, the security of the device/browser, and the strength and safekeeping of the user's passphrase.

No system can guarantee perfect security. Users should avoid storing information that would cause severe harm if disclosed unless they are comfortable with the remaining risks.

Children and sensitive content

Memory Vault is not intended for unsupervised use by young children. Users should not store or share personal information about children unless they have the authority and consent to do so.

The app can contain sensitive personal memories. Users are responsible for deciding what to enter, what to encrypt, and what to share.

Contact and updates

Questions or requests should be sent through the support contact listed on the app website or App Store listing. This policy may be updated as the app, iOS version, infrastructure, or third-party service list changes.