

Data Retention Policy

Last updated: May 21, 2026

Explains retention and deletion expectations for Memory Vault data.

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.

Purpose

This Data Retention Policy explains how long Memory Vault keeps account, memory, sharing, support, and operational data. It applies to the web app and the related iOS app using the same Worker and database.

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.

Retention schedule

Data category	Default retention approach
Account/profile data	Retained while the account is active or until account deletion is completed, unless legally required to keep limited records longer.
Memories, labels, people tags, dates, locations, confidence, revisions, and encrypted payloads	Retained until the user deletes the item or the account is deleted. Deleted items should be removed from the live database, subject to backups/logs and technical limitations.
Shared memories, connection records, edit suggestions, and imported-copy metadata	Retained while relevant to active connections, sharing workflows, dispute/safety review, or until deleted/revoked where supported. Imported copies may remain as separate records for the importing user.
Magic-link login tokens	Should be short-lived and expire after the configured login period or after use.
Operational logs and email delivery logs	Retained only as long as needed for security, debugging, abuse prevention, and provider operations. Specific periods depend on the configured infrastructure provider.
Local drafts, session state, and caches	Retained on the user device until cleared, expired, overwritten, logout occurs, or the app/browser storage is removed.
Support/issue reports	Retained as long as needed to resolve the issue, maintain a record of safety/security matters, and improve the app.

Deletion requests

Users may request deletion of their account and associated server-side data through the support channel or through in-app deletion controls if available. Before App Store release, the iOS app should provide an account deletion path from within the app if users can create or access accounts there.

Deletion may not remove data already exported by the user, copied into another user's vault by an import action, sent to an AI provider for a completed request, retained in provider logs, or required to be kept for legal/security reasons.

Backups and logs

Backups, database snapshots, logs, and provider records may persist for a limited time after deletion from the live app. The operator should configure provider retention settings to the shortest practical period consistent with recovery, security, and legal needs.

User exports

Exported JSON or CSV files are outside the app's control once downloaded or shared. Users should store exports securely, especially if they include private or sensitive memories.