

Acceptable Use Policy

Last updated: May 21, 2026

Safety and content rules for Memory Vault.

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 Acceptable Use Policy keeps Memory Vault safe, respectful, and suitable for personal memory storage and consent-based sharing. It applies to both the web app and iOS app.

Allowed use

- Capturing and organizing your own memories and life events.
- Using labels, people, dates, locations, maps, timelines, and AI narratives for personal reflection.
- Sharing selected public memories with trusted connections when you have the right and consent to do so.
- Suggesting edits to shared memories in good faith.

Prohibited use

- Harassment, bullying, stalking, coercion, blackmail, threats, or intimidation.
- Sharing another person's private information, images, memories, or sensitive details without permission.
- Impersonation, fake identities, deceptive connection requests, or misleading verification responses.
- Uploading unlawful content or content that infringes someone else's rights.
- Sexual exploitation of minors, child sexual abuse material, grooming, or any attempt to facilitate harm to a child.
- Instructions or coordination for violence, self-harm, terrorism, exploitation, cyber abuse, fraud, or other illegal conduct.
- Attempts to bypass access controls, encryption, payment systems, rate limits, or account protections.
- Automated scraping, spam, denial-of-service behavior, malware, or abusive API usage.

User-generated content and reporting

Because the app supports user-generated memories and sharing, users must be able to report objectionable content or abusive behavior. Reports should be sent through the Report an issue process or in-app reporting controls if available.

The operator may review reported public/shared content and connection activity, restrict accounts, remove content, disable sharing, or take other action when needed for safety, legal compliance, or service integrity.

Enforcement

Violations may lead to removal of content, disabling of sharing features, suspension or termination of access, preservation of relevant records, or reporting to appropriate authorities where required.