

Privacy Policy

English

v1.1 · Effective October 27, 2026

Operator: 北京简观万境科技有限公司
Beijing Jianguan Wanjing Technology Co., Ltd.
help@twinlore.app

1. Scope and Definitions

1.1 Operator, Covered Services and Definitions. In this policy, “personal information” means information that identifies, relates to, or can reasonably be linked to an individual, and other information included within that concept under applicable privacy law. 北京简观万境科技有限公司 (Beijing Jianguan Wanjing Technology Co., Ltd., “we,” “us,” or “our”) is responsible for personal information processing described here. This policy covers the TwinLore app, accounts, cloud workspace, support, and company and brand websites expressly linking to it. Visiting an informational page does not create an app account; feature-specific processing applies when you use that feature.

1.2 Separate Permissions and Third-Party Services. This policy describes our practices and does not constitute blanket permission for all data uses. Device permissions, third-party AI processing and optional “Help improve” have distinct purposes; processing requiring consent will use the appropriate choice. This policy does not govern third-party websites you independently visit, recipients of exports, or your independent third-party accounts. A company email alone does not give your employer access to your private workspace.

1.3 Editions and Applicable Law. This policy applies to invited TwinLore Beta testing, TestFlight distribution and Services expressly referring to it. Chinese and English describe the same processing practices. Language or download-store region does not determine applicable law or hosting location. Our obligations reflect the actual operator, processing locations, people served and applicable law; the distribution channel does not exclude applicable protections.

2. Collection and Use of Personal Information

2.1 Sources of Information. We receive information you provide, information generated by service use, information returned by sign-in or payment services you use, and external source material accessed at your request. Categories depend on the features you actually use.

2.2 Account and Identity Information. This includes email or other enabled sign-in identifiers, provider-issued account identifiers, verification and sign-in status, and preferences, for registration, access, recovery, account separation and fraud prevention. Authentication credentials are handled by the authentication system rather than as ordinary conversation content.

2.3 User Content and Saved Work. This includes conversations, notes, boards, page versions, references, uploaded files and images, audio you submit, and material you ask us to read, for answering, editing, generating interactive results, saving work and executing tasks. Relevant history, personal memories, preferences, skills and task state support context retrieval and continuity for your own use.

2.4 Operational, Security and Diagnostic Information. Request times, errors, app versions, resource use, task status and access/security records support operation, troubleshooting, metering and abuse prevention. Diagnostic traces recording actual requests or errors may contain content excerpts and are not necessarily anonymous statistics.

2.5 Notification, Transaction and Contact Information. When notifications or Live Activities are enabled, device push tokens, related task identifiers and notification content deliver status updates; device settings may display them on the lock screen. Once subscriptions are offered, transaction identifiers, plans, entitlements, renewal/refund status and necessary accounting records deliver and reconcile access. Apple handles payment information it collects; this does not give us your full card number. Invitation requests, names, emails, company details, support messages and attachments you submit are used to handle the request or issue.

2.6 Permissions and Deletion Records. Document-bundle versions, individual document versions and content checksums, acceptance language, adult declarations, permission states and times, request identifiers and necessary deletion status support your choices, compliance and preventing deleted accounts from reappearing after backup restoration. Camera, microphone, photo, file and notification access is limited by features and device permissions; selecting one file does not authorize access to all files. Maps may process a location you provide; this policy does not authorize continuous device-location tracking.

2.7 Reports and Provenance Information. When you submit a complaint or report, we may process the relevant content, page or message identifiers, time, contact details and necessary operational records you provide or that are needed to investigate, act, respond and review. Access is limited to personnel or providers who need it for those purposes, and retention follows Section 7. A report does not authorize access to all private content or general model training. Where provenance information is provided to meet applicable law or license requirements, necessary information may include generated-content attributes, service or model identifiers and content identifiers. Public labels should not include unrelated account emails, conversation text or sensitive information.

3. AI, Voice and Personal Memory

3.1 Request Processing and Context. The system may select the current message, relevant history, references, attachments, existing pages, personal memories and task instructions for enabled AI providers. A request may involve multiple model and tool calls. Enabling AI does not itself send all account data to every provider. Relevant recipients and data are disclosed before processing and explicit permission is obtained.

3.2 Voice Processing and Background Tasks. Speech recognition processes submitted audio into text; text-to-speech processes selected text into spoken output. Original audio, transcripts and playback audio may have different retention rules. Enabled background processes may organize personal vocabulary, memory and reusable skills, or update work through your scheduled tasks. This serves your own account and is not automatically general model training. Memories, summaries and inferences can be wrong; available controls let you review, change or delete them. Context compression does not mean source data has been deleted. A single recording can continue beyond two minutes. After it stops, the full audio is used for transcription, and the original recording and transcript follow the account file-saving flow. Lock-screen recording is subject to system permission and interruptions; check the result after recording. Speaker labels in multi-speaker transcription are automated inferences, not verified identities.

3.3 Third-Party AI Permission and Withdrawal. Current registration requires acceptance of service terms, adult confirmation and third-party AI permission; “Help improve” is separate. You can later disable AI in Privacy & data: this stops new AI requests and background AI updates and cancels work where still possible; already transmitted requests may not be recalled. Disabling does not itself delete saved work, and supported viewing, export and deletion remain. Creating, editing, uploading and AI tasks are unavailable without required permission. Re-enabling does not automatically replay missed tasks. Settings do not erase acceptance of an already accepted agreement version. This does not restrict applicable rights to withdraw processing permission, request correction or delete your account. New document versions require active confirmation; the historical-content controls described above remain available while confirmation is pending.

3.4 Access and Storage Limits. Access remains subject to account status, the applicable plan and Section 7 retention rules. We do not promise permanent free storage, self-service export of every data type or custom conversion; statutory access and deletion rights remain unaffected.

4. Disclosure and International Processing

4.1 Service Providers. We use hosting, storage, authentication, AI, speech, tool-query, email, notification, payment and operational providers, supplying data relevant to their roles with contractual and security protections as applicable. Third-party AI processing follows the relevant notice and your valid permission; changes to provider information do not replace legally required notice or consent for a purpose. Current core services use Alibaba Cloud hosting and storage in Hong Kong, ESA access protection, and Authing account authentication and verification email services. AI recipients include DeepSeek, Alibaba Cloud Model Studio, and Google Gemini services accessed through OpenRouter; processing categories are described in the AI Data Notice. Task notifications use Apple notification services; search uses Tavily, and maps use Amap or Apple Maps according to the feature. Necessary data is provided only to recipients serving the relevant function.

4.2 International Processing. Our operating company is in China. Current beta accounts and their primary application data are hosted in Hong Kong. AI and other providers process necessary data in relevant regions; this does not mean all model processing, backups or personnel access occur in Hong Kong; information may be processed outside your country, where data-protection rules may differ. Consent does not bypass applicable restrictions on international access or transfers. Independent provider reuse or training cannot be concealed under the label “service provider.”

4.3 Other Disclosures. We may provide data to recipients you direct; to advisers, authorities or relevant parties when legally required or reasonably necessary for fraud prevention, security, rights or claims; and lawfully in financing, mergers, reorganizations or sale of the relevant business, subject to applicable protections and notice. Service use does not automatically make private conversations public. Independent third-party services have their own rules.

5. Optional Model Training and Product Improvement

5.1 Optional Permission and Default Settings. This option is off by default. “Help improve TwinLore” is a separate optional choice. Declining or later disabling it does not affect normal use subject to your account, plan and other necessary permissions. You can disable it at any time in Privacy & data. We will not unlawfully discriminate for exercising privacy rights; this does not fix future plan prices or establish a discount or incentive program.

5.2 Scope of Permission. After you opt in, we may select eligible inputs, outputs, related feedback and necessary context, within the scope disclosed and validly authorized, for model training or fine-tuning, quality and safety evaluation, human problem analysis and product improvement, including improving our own models and services. Samples are limited to eligible content created after the relevant permission took effect; opting in does not retroactively include your entire history. Permission allows these uses but does not establish that training is currently operating or require us to run it.

5.3 De-Identification and Access Controls. If we run such a program, we apply reasonable removal of personal information or de-identification, access restrictions and appropriate confidentiality obligations based on data risks and purposes. We do not guarantee all processed free text is unidentifiable; pseudonyms or removing names do not necessarily make data anonymous. Linkable data remains subject to this policy and valid permission. Lawfully created de-identified or aggregate data that no longer identifies individuals may support statistics, research, evaluation and improvement, without evading prior commitments, applicable law or withdrawal requirements. Data required by law to remain de-identified will not be re-identified, except for legally permitted testing or evaluation.

5.4 Withdrawal and Existing Samples. Disabling stops new selection or new processing for the optional purpose, and retained personal information is handled under applicable law and your requests. Identifiable samples selected but not yet used in future training do not gain unlimited use rights from past consent. An individual contribution to an already trained model may not be separately reversible, without excusing deletion or other measures required by law. Anonymous statistics already lawfully created and no longer linkable to you may not be locatable for individual removal.

5.5 Separation of Processing Purposes. Updating your own memory and skills, handling support you request, investigating incidents or preventing abuse does not grant general training rights. Feedback permission does not automatically cover your entire history. Materially different purposes, data categories or independent training recipients require applicable notice and renewed permission before use, rather than reliance solely on an old toggle.

6. Websites and Communications

6.1 Website Visits and Contact. Website processing is limited to actual functions, such as access logs, contact emails you send or active application forms. An invitation request is not a paid subscription; we may verify contact information and send related invitations or service messages.

6.2 Communication and Notification Choices. Necessary account, security, transaction, task and legal notices differ from marketing. If marketing emails are offered, they will include applicable unsubscribe and sender information. Opting out of marketing does not stop necessary service notices. Device notification permissions can be changed in system settings; this does not cancel server tasks or delete an account.

7. Retention, Deletion and Account Closure

7.1 Retention Criteria. Retention reflects account and feature needs, your choices, security, accounting, legal duties and disputes, not indefinite archiving. Account content is kept as needed for relevant features, subject to your deletion actions and disclosed plan rules. Any future automatic deletion solely for inactivity must first specify thresholds, scope, notice and reasonable export opportunities; this policy does not itself authorize immediate deletion or retroactive shortening of existing paid periods.

7.2 Account Closure and Deletion. Initiate deletion in the app’s account settings. The system first restricts further account activity, then processes deletion of related records, files, memory, work pages and authentication identity. Deleting a page does not itself close the account or erase independently saved copies elsewhere. Deletion involves relevant systems, providers and backup cycles and must meet applicable legal deadlines. Receipt is not proof every copy is erased and does not permit continued ordinary use of data that must be deleted.

7.3 Lawful Retention and Backups. Limited information lawfully retained for compliance, accounting, security or claims is restricted to those purposes. Backup restoration should honor recorded deletion requests; prevention records retain necessary identifiers and status rather than original conversations or credentials. Export needed material first; recovery is not guaranteed. Account deletion or uninstalling does not cancel an Apple subscription; cancel separately.

8. Your Rights and Choices

8.1 Settings and Request Channels. Use provided functions to review or change content, export supported materials, delete content or accounts, and adjust AI/improvement choices and device permissions. Send privacy requests unavailable through self-service to help@twinlore.app with “Privacy request”; use “Privacy appeal” for appeals. We may handle requests manually through email and existing systems without an additional dedicated portal, custom reports or export of all internal records, while fulfilling statutory access/portability in a compliant form.

8.2 Statutory Privacy Rights. Depending on law and processing, you may have rights to know/access, obtain copies, correct, delete, withdraw consent, restrict sensitive-data use, or opt out of sale, sharing, targeted advertising or certain profiling. Lawful exceptions may apply. We may require reasonable, proportionate verification; authorized agents may act where legally permitted. Do not send passwords, verification codes or full payment details. Where required, we explain denials and appeals and respond within applicable deadlines, including lawful extensions, without unlawful discrimination.

9. U.S. State Privacy Rights

9.1 Applicability and Exercise of Rights. If your state’s privacy law applies to our relevant processing, you may exercise the rights it provides through Section 8, including, where applicable, access, correction, deletion, obtaining a copy, appeal, and opting out of sale, sharing, targeted advertising or certain profiling. These rights are subject to the law’s scope and exceptions. State definitions of “sale,” “sharing” and sensitive information may differ and are not limited to exchanging data for money. Sections 2 through 6 describe categories, sources, purposes and recipients of personal information. Use the channels in Section 8 to submit a request.

10. Children’s Privacy and Sensitive Information

10.1 Age Restrictions. Users must be at least 18 and of legal adult age where they live; the Services are not directed to children under 13. An adult checkbox is a declaration, not government identity or age verification. If we learn an ineligible person supplied personal information, we take appropriate restrictions, deletion or other measures required by law. Contact us if you become aware of this. An accepted adult declaration remains a historical record in settings and later agreement reviews and cannot be unchecked directly. If it was incorrect, request correction through support email or in-app feedback. We will review and handle it as required by law; a retained checkmark is not age verification.

10.2 Sensitive Information. Do not submit unnecessary government identifiers, passwords, full financial-account details, health or other sensitive information, or others' data you lack authority to process. Where processing sensitive personal information is necessary, we limit it to specific, necessary purposes and apply strict safeguards proportionate to the risks. Where applicable law requires, before processing we separately explain its necessity, purposes and effects, obtain separate consent or another legally required form of consent, and complete required personal-information impact assessments and records. General AI permission does not replace separate consent required by law. The Services are not emergency assistance or a regulated professional service. This warning does not exclude duties applying when we actually process sensitive information.

11. Data Security

11.1 Security Measures and Risks. We apply reasonable technical and organizational measures proportionate to service and information risks, such as access controls, account separation, transmission protection and operational auditing; measures may change with risks. No system guarantees absolute security. Protect accounts and devices and report suspected unauthorized access. This policy does not promise particular certifications, end-to-end encryption, zero retention, dedicated security services or uninterrupted, incident-free operation. Legally required incident notices and other mandatory duties remain applicable.

12. Changes to This Policy and Contact Us

12.1 Policy Changes and Notice. We may revise this policy for service, provider or legal changes and publish its version and effective date. Material changes receive appropriate app, website or email notice as required by law or platform rules. When a new version of the Terms of Service, Privacy Policy or AI Data Notice is published, the app requests renewed confirmation of the entire bundle before processing that requires consent. Silence, a prior login or continued use alone does not authorize a materially new use requiring consent or retroactively change commitments about old data.

12.2 Language and Contact. Chinese and English express the same policy; language choice does not change your rights or our processing scope. Discrepancies are interpreted under applicable law and corrected. Contact help@twinlore.app for privacy questions or requests; see the Terms of Service for subscriptions, use rules and liability.