

SESSION FORGE

Privacy Notice

Effective date: October 1, 2026 · Last updated: October 1, 2026

1. About this Privacy Notice

Session Forge LLC ("Session Forge," "we," "us," or "our") operates Session Forge, an online virtual tabletop and session-management service. This Privacy Notice explains how we collect, use, disclose, and retain personal information through our websites, application, related features, and communications (the "Service"). It also explains available choices and how to contact us. The Service is intended for adults age 18 or older in the United States.

A "Session" is an ongoing shared workspace within the Service for gameplay, collaboration, and content; it may span multiple game meetings and is distinct from a login session.

This Notice describes information practices. It is not a waiver of privacy rights or, by itself, consent to processing that requires separate consent. Our Terms of Use address eligibility, content permissions, subscriptions, storage availability, and other conditions of using the Service. Mandatory privacy rights remain applicable regardless of subscription status.

2. Information we collect and its sources

Account information. When you register, sign in, or manage an account, we and our authentication provider process your email address, username, password or other authentication credentials, account identifiers, authentication status, and account preferences such as language. We also retain account roles and records of the Terms version you accepted and when you accepted it. Google Firebase provides authentication, password-reset, and related account functions.

Sessions, communications, and uploaded content. We process information you or other users enter into the Service, including Session membership and roles, display names and aliases, notes, characters, maps, game entities and templates, chat messages and rolls, invitations, friend relationships, images, videos, audio, and other supported files. Associated information includes author and recipient identifiers, content and Session identifiers, timestamps, permissions, archive or deletion flags, settings, and saved window layouts. Files can contain embedded information, such as names, voices, faces, locations, or other metadata; do not assume an upload removes that information. Other users may provide information about you in messages, invitations, shared Sessions, or support reports.

Optional feature information. If you use AI, dictation, or connected-device features, the Service processes the prompts, content, context, microphone audio, transcription text, integration configuration, and related information described in Section 5. The information depends on the feature you use.

Purchases, if offered. When paid subscriptions or digital purchases are available, we and our payment provider process the information needed to complete and administer the transaction. This may include account and checkout identifiers, the selected offering and quantity, payment and subscription status, invoice or transaction references, and billing or payment information supplied through checkout. The checkout identifies any additional information required for that transaction.

Technical, activity, and diagnostic information. Operation of the Service generates information such as IP addresses, referring pages, connection and authentication events, login and logout times, Session activity, requested operations, account identifiers, and errors. Error records can include submitted content or request details needed to understand a failure. Our hosting and feature providers also receive technical information needed to handle requests. These records are separate from advertising or marketing analytics.

Support and legal communications. If you email us or submit a support, privacy, copyright, safety, or other report, we receive your contact information, correspondence, and any supporting information you provide. We may retain verification details and records of our response where permitted or required.

The Service is not designed to request government identification numbers, medical records, financial-account credentials outside an appropriate payment flow, or other highly sensitive personal records for ordinary gameplay. User content can nevertheless contain sensitive information. Provide only information you have authority to provide and that is appropriate for the feature and its recipients.

3. How we use information

We use the information described above as relevant to:

- Create and authenticate accounts, maintain settings, and record acceptance of applicable Terms.
- Store, retrieve, display, convert, cache, synchronize, and deliver content; support Sessions, messages, invitations, collaboration, and features you use.
- Process requested AI, speech, and connected-device operations.
- Administer offered subscriptions, purchases, payment issues, and applicable refunds or cancellations.
- Maintain, troubleshoot, secure, and improve the Service, including investigating failures, misuse, fraud, and reported violations.
- Respond to requests and send account, security, support, transaction, policy, and other service-related communications.
- Comply with applicable obligations, preserve legally required evidence, resolve disputes, and protect legally recognized rights and safety.

These purposes do not mean we continuously review every message or upload. We may access information for the purposes described in this Notice; we do not undertake general proactive screening of all user content. Applicable legal duties and responses to information we receive still apply.

4. Who can receive information

Other users. Session participants and administrators can receive your identity and content according to the feature, membership, role, and visibility settings involved. Messages, invitations, and friend requests disclose information to their recipients. **Accepted friends can receive your account email address, username, and account identifier.** Account usernames may also be checked for availability. A small Session is still a sharing environment: recipients may save, copy, export, or redistribute information. Removing access cannot retrieve copies already obtained. Privacy and content restrictions still apply to recipients as provided by law and the Terms.

Providers supporting the Service. We disclose relevant information to providers of authentication, hosting and storage, communications, requested AI and speech processing, connected features, and payment processing. Current integrations include Google Firebase for authentication, Amazon Web Services for media storage, OpenAI for AI features, AssemblyAI or your browser's speech service for dictation, and Home Assistant Cloud/Nabu Casa when you configure that integration. Stripe is used by the payment integration when paid checkout is offered. Not every provider receives every category of information. We may change providers as the Service develops, with updated disclosures or other steps where required.

Authorized operation and support. The operator and authorized administrators or providers may access account information and stored content as needed for the purposes in Section 3, including support, troubleshooting, security, and handling reports. Session privacy settings restrict sharing among users; they do not mean stored content is inaccessible to the operator or service providers.

Legal and protective disclosures. We may disclose information when required by law or when reasonably necessary and legally permitted to respond to valid legal process, investigate reported violations, address fraud or security issues, protect rights or safety, or establish, exercise, or defend legal claims. A notice, counter-notice, or similar dispute submission may be forwarded to the affected party or authorities as required or permitted for that process.

Business transfers. Information may be disclosed to relevant advisers and parties in connection with a proposed or completed financing, merger, acquisition, reorganization, sale of business assets, or insolvency proceeding, subject to applicable confidentiality and legal restrictions. A transfer does not itself authorize uses inconsistent with applicable privacy obligations.

We may also disclose information at your direction or with a separate permission where appropriate. Information processed by another service under its own relationship with you is subject to that service's policies as well as any applicable obligations of Session Forge. This does not eliminate our responsibility for processing for which we are legally responsible.

5. AI, microphone, connected-device, and payment features

AI features. When you request AI assistance, the Service sends your entered prompt or editor text and relevant Session context to OpenAI. Depending on the feature, that context can include existing note names and identifiers and category names and identifiers; it is not necessarily limited to the words just typed into the prompt. Returned output may be inserted into the editor or saved as ordinary Session content. Submitted prompts or context may also appear in diagnostic records if processing fails. Do not submit information you lack authority to have processed by the provider. The content license in our Terms does not independently authorize training machine-learning models; this Notice does not grant that permission either.

Dictation. Using dictation captures microphone audio and obtains transcription through AssemblyAI or, in supported browsers, the browser's speech-recognition service. Speech recognition may involve off-device processing. Transcribed text is returned to the application and can be inserted into the active field; if saved or sent, it is then treated like other saved content or messages. Browser permissions and the recording controls let you control microphone access. Obtain any required permission from people whose speech you capture. We do not promise that a provider immediately deletes all audio or text after transcription.

Home Assistant. If you enable this integration, we store integration names, account associations, encrypted webhook URLs, and encrypted key material to save and synchronize your configuration. Your browser also stores integration and unlock information. Running an automation sends a request directly from your browser to the configured Home Assistant Cloud/Nabu Casa endpoint, which receives the webhook request and ordinary network information. Removing an integration from Session Forge does not by itself revoke the external webhook or erase the destination's records.

Payments. If you use an offered paid feature, payment processing involves Stripe and relevant financial intermediaries. We exchange account and transaction references and receive payment, checkout, subscription, or invoice information needed to administer access and transactions. Information you supply directly to the processor is also subject to its applicable privacy terms. Do not email us payment-card details.

These providers have their own processing, security, and retention arrangements. This Notice does not promise that every integration runs only on your device, that provider retention is zero, or that all information sent to a provider is immediately erased when a feature finishes.

6. Browser storage, advertising, analytics, and communications

The Service uses browser storage and authentication technologies to maintain access, cache Session and media information, save preferences, and support integrations. This includes IndexedDB, local storage, and session storage; integrated providers may use cookies or similar technologies for their functions. Signing out does not necessarily clear information stored on the device. The app's Clear Cache function clears its IndexedDB cache, not your server account or every item of browser storage. Browser controls can remove additional site data or restrict storage and permissions, but doing so can affect features and sign-in. Protect devices shared with other people.

We do not currently use advertising networks or third-party marketing analytics tools, and we do not currently send promotional emails. We do collect the operational, activity, security, and diagnostic information described in this Notice. Service, billing, security, legal, and support messages are distinct from promotional messages.

We do not currently provide personal information to others in exchange for money or disclose it to advertising networks for targeted advertising. We disclose information to the providers and other recipients described in this Notice to operate the Service and provide the features you use.

We do not currently conduct cross-site advertising tracking. The Service does not change its functional logging or storage in response to a browser's legacy Do Not Track setting. Integrated providers may receive identifiers and information about your interaction with their services and may recognize you across other sites or services, depending on their practices and your settings. Browser Do Not Track and legally recognized opt-out preference signals, such as Global Privacy Control, are different. Where applicable law requires us to honor an opt-out preference signal, we will do so.

We may introduce analytics, advertising, or promotional communications in the future. Before changing these practices, we will update relevant disclosures and provide any notice, choices, opt-out mechanism, or consent process required by law. Merely using the current Service is not advance consent to a materially different use of previously collected information.

7. Retention, in-app deletion, and stored media

In-app deletion generally is not physical erasure. Deleting or archiving content in the interface ordinarily marks records as deleted or archived and removes them from ordinary views. Database records and associated files may remain. We do not currently run a general process that automatically erases database records when an in-app delete control is used. They may remain unless you request deletion by email or we remove them for another permitted reason, subject to applicable retention limits. A deletion or archive flag does not guarantee that content can be restored.

Retention purposes and limits. We retain information according to its nature and purposes, account and Session status, applicable purchase commitments, requests we receive, and legal requirements. Account, content, and configuration records may be retained to provide account access, storage, synchronization, and continuing authorized collaboration. Operational and diagnostic records may be retained for troubleshooting, security, and investigating incidents. Transaction, acceptance, correspondence, and dispute records may be retained for accounting, evidence of agreements or permissions, request handling, or legal claims. Retention remains subject to limits imposed by applicable law, including any requirements to delete information even without a request. We may remove information earlier when no longer needed or otherwise permitted.

Non-subscriber media. We may remove stored media, including videos, images, and audio, associated with an account that does not have active paid access covering that storage. For discretionary cleanup, we may use a threshold of **12 months after the later of the upload date and the most recent date on which paid access covering that media ended**. If no paid access covered the media, the upload date is the reference date. This is not a guaranteed minimum storage period or a promise to delete on that date. Earlier removal, including for resource management, enforcement, service changes, or shutdown, remains possible under the Terms, subject to applicable law and express purchase commitments. Paid access does not create a permanent-storage guarantee. Keep independent copies of important files.

Privacy deletion requests. To request deletion of personal information from retained records, email the contact in Section 12; an in-app delete control is not the same request. We review and reasonably verify requests and handle them under applicable law. We may retain information when legally permitted or required, such as for accounting obligations, legal holds, security and fraud prevention, resolving disputes, or protecting others' legally recognized rights. These exceptions are limited to their applicable purposes and do not automatically justify keeping every record. We may delete, deidentify, or separate identifying information where appropriate and legally sufficient; merely hiding a record does not necessarily fulfill a privacy deletion obligation.

Shared content, backups, and other copies. Your departure from a Session or account closure does not necessarily remove every shared contribution. Retention of shared content remains subject to applicable privacy rights and the Terms; collaboration alone does not override a valid deletion right. Independent copies obtained by other people may remain outside our control. Where backups or archives exist, removal from them may occur later than removal from active systems where law permits, and lawfully retained copies remain restricted to the purposes that justify retention. Providers acting for us are included in a deletion request to the extent required by applicable law; independent providers may have separate legal retention duties. Clearing server records does not necessarily clear copies already stored in a browser.

Canceling a subscription, closing an account, deleting an item in the app, and requesting deletion of personal information are different actions. Tell us what you want when contacting us. Subscription and closure consequences are addressed in the Terms; privacy rights are not reserved for paying customers.

8. Your controls and privacy requests

You can use available account controls to change your username, password, or language; use Session and message controls to choose available sharing options; manage browser permissions; and clear local data as described above. Email us for other account-information corrections, account closure, or privacy requests. You do not need to buy a subscription to submit a request.

Depending on your state of residence, our activities, and the law's applicability, you may have rights to know whether we process your personal information; access information and obtain a portable copy; correct inaccuracies; request deletion; and opt out of covered sales, targeted advertising, or certain profiling. Additional rights may include limiting certain uses of sensitive personal information, obtaining a list of specific third parties to whom we disclosed personal information, using an authorized agent, or appealing a refusal. These rights have legal conditions and exceptions. Listing them does not mean we currently conduct each type of processing or that every listed right applies to every person.

Send requests to sessionforgellc@gmail.com, preferably from the account email address. Identify the account and request and provide enough detail to locate the relevant information. We may request reasonably necessary verification, clarification, or proof of an agent's authority and may decline requests that cannot be verified where verification is required. Do not send your password or unnecessary identity documents. We respond within applicable legal time limits and provide required information about any lawful extension or denial. Applicable law governs any permitted fees or limits for excessive or unfounded requests and prohibits unlawful discrimination for exercising protected rights.

If applicable law gives you a right to appeal a refusal, email the same address with the decision and why you disagree. Using "Privacy Appeal" in the subject can help identify it but is not required. We will process the appeal and provide further complaint information as required by that law. You may also contact your state's attorney general or other competent regulator. This process does not require you to waive a statutory complaint or remedy.

9. Security and processing locations

We use authentication, access controls, and selected encryption and other safeguards in the Service. No method of storage or transmission is completely secure. The Service is not represented as universally end-to-end encrypted or inaccessible to the operator. Encryption used for a cache or integration does not mean all uploaded media or database records have the same protection. Security and incident-response obligations imposed by law remain applicable.

Session Forge is offered to U.S. customers, but hosting, authentication, support, and feature providers may process information in other locations in accordance with their arrangements and applicable law. The U.S.-only customer restriction is not a guarantee that every copy of information stays in the United States.

10. Adults-only service

The Service is not intended for anyone under 18, and minors are not permitted to create accounts or use it. We do not knowingly seek personal information directly from children under 13. If you believe a child has provided information through an unauthorized account or use, contact us so we can assess and address it as required by law. The age restriction does not replace any legal duties that apply when we learn of children's information.

11. Changes to this Notice

We may update this Notice as the Service, practices, or legal requirements change. We will post the revised Notice with its updated date. For material changes, we will provide a conspicuous notice through the Service or an email to the account address, as appropriate, and any additional notice or consent required by law before implementing the relevant change. Changes do not retroactively remove privacy protections or authorize incompatible uses where separate permission or another legal basis is required. Review the current Notice when using a new feature or making a privacy choice.

12. Contact

For privacy questions, corrections, account closure, or deletion requests, contact **Session Forge LLC** at **sessionforgellc@gmail.com**. Our business mailing address is **2051 Chatham Rd #42024, Springfield, IL 62704, USA**.