GREEKHOURS

Trust Pledge

What GreekHours does with your chapter's data, who can see it, and what happens if something goes wrong. Every statement verified against the live system.

Version 2.0 · Verified against production September 8, 2026
Prepared for chapter leaders, academic officers, advisors, and campus stakeholders

What this is

When a chapter chooses a new way to track hours, someone has to stand behind that decision and answer questions about what the app collects, who can see it, and what happens if something goes wrong. This document answers those questions plainly. Every statement in it was checked against the running GreekHours system on the date above. Where a control is a commitment rather than a built feature, it says so.

Common questions

What does GreekHours collect?

Your name, your sign-in identity from Apple, Google, or Microsoft, your chapter and role, your hours, and your location during a study session. Nothing else.

Does it track my location?

Only while you are in a study session, to confirm you are where you said you would be. Never outside a session. Raw location is deleted after 120 days, and it never appears in any report shared outside the chapter.

Who can see my data?

Officers in your chapter with an assigned role, and only within their role. No other chapter. GreekHours staff only for support and operations.

Can compliance be shared with advisors or nationals without exposing people?

Yes. Reports can be shared as a read-only link with names removed, or as chapter totals only. Links expire and can be revoked.

What happens if there is a security problem?

GreekHours investigates within one business day and notifies your chapter's designated contacts within 72 hours of confirming any incident that affects chapter data.

The eight commitments

Each commitment has three parts: what we commit to, what it means for your chapter, and how you can check it.

1 We collect only what hour tracking needs, and we never sell it.

GreekHours collects your identity from your sign-in provider, your chapter and role, your hours, and your location during a session. We use it to run hour tracking, reporting, and support. We do not sell personal information and we do not operate as a data broker.

How to check: Privacy Policy at greekhours.com/privacy. The full list of third parties that touch your data is in the fact sheet. Website analytics and campaign tags are disclosed there too and never receive member data.

2 Location is for verifying a session, never for tracking you.

GreekHours checks your location when a session starts and while it runs. During an active session, verification can continue if the app is in the background, so that leaving the study location ends the session. When no session is running, GreekHours does not collect location at all. Coordinates are converted to a place name using Google's geocoding service, which receives coordinates only and no identity. Raw coordinates and the place name are deleted 120 days after the session or at semester end, whichever protects you more. What remains is the verification result, the duration, and the hours credited.

How to check: location fields are excluded from every shared report tier. The mobile apps contain no third-party analytics or crash-reporting tools that could receive location.

3 No passwords, ever.

You sign in with Apple, Google, or Microsoft. GreekHours never stores a password for your account, so there is no GreekHours password to be leaked, guessed, or reused.

How to check: the sign-in screen offers only those three options. There is no "create a password" flow.

4 Encrypted in transit and at rest.

Every connection uses HTTPS with TLS 1.2 or higher. The database, including uploaded photos, and its backups are encrypted at rest on Microsoft Azure with platform-managed keys.

How to check: Azure App Service and PostgreSQL configuration. Backups are retained for 7 days, which means anything deleted is fully gone within a week.

5 Access is scoped by role and by chapter.

Five roles control what a chapter member can see and do: student, Chapter Admin, Study Admin, Service Admin, and Event Admin. A student sees their own hours. Scoped admins see their area. Chapter Admins see their chapter. A separate Global Admin role is held only by GreekHours staff, for support and operations, and is not a chapter seat. Chapter data is scoped so one chapter cannot reach another's.

How to check: the role list in the fact sheet. A detailed role-permissions summary is available to advisors on request.

6 Your data is yours: share it on your terms, delete it on request.

Compliance reports can be shared as read-only links in three detail levels, scoped by date and category, with an expiration date and a revoke control. Anonymized Detail removes names, emails, and identifiers and uses random labels generated per report that cannot be linked across reports. Summary Only shows chapter totals with no member rows. Every level excludes location and any financial or fine detail. Any member can delete their account from inside the app, and anyone can submit a deletion request through the public form. We acknowledge deletion requests within 5 business days and complete them, or report status, within 30 days.

How to check: the report tiers and retention tables in the fact sheet. Deletion paths are linked from the Privacy Policy.

7 AI stays in bounds.

Athena, the in-app support assistant, runs on Anthropic's Claude model through Microsoft Azure AI Foundry, hosted by Azure. It processes your conversation and limited chapter context to answer your question. Conversations are stored in the United States and deleted after 120 days. You can delete any conversation, or all of them, at any time. If you escalate a conversation to support, a copy is kept for 120 days. Under Microsoft's and Anthropic's enterprise terms, your content is not used to train their models. The current deployment uses Azure's Global Standard routing, which means AI processing may run in Azure regions outside the United States; your stored data does not.

How to check: the Athena delete controls in the app. Microsoft's Azure AI data-handling documentation is available on request.

8 We monitor, we respond, we tell you.

GreekHours runs application logging and monitoring, and logs are written so they do not contain coordinates or personal details. Security concerns can be reported to security@greekhours.com or through the standard security.txt contact file. We begin assessing any security report within 1 business day. If we confirm an incident that affects chapter data, we notify your chapter's designated contacts within 72 hours of confirmation, unless law requires a delay. Every incident is documented with what happened, what we fixed, and what we changed.

How to check: greekhours.com/security and greekhours.com/.well-known/security.txt. Send a test message; you will get a reply.

Fact sheet

Architecture

GreekHours is a native iOS and Android app, a web admin portal, and API services, backed by a PostgreSQL database, running on an enterprise-grade Microsoft Azure environment with privacy

and security controls built in: a web application firewall, security alerting, and continuous monitoring, on top of encryption in transit and at rest. Chapter and member data is stored in the West US 2 Azure region; the Athena AI endpoint runs in West Central US. Azure's edge networking and security services are global by design; they process traffic and do not store chapter or member records.

Third parties that touch data

Third party	What it receives	Whose data
Microsoft Azure	Hosting, database, backups, logs, AI processing	Members and officers
Anthropic Claude via Azure AI Foundry (Azure-hosted)	Athena support conversations and limited chapter context	Members and officers who use Athena
Apple, Google, Microsoft	Sign-in identity	Members and officers
Apple and Google	Push notification delivery tokens	Members and officers
Google Geocoding	Session coordinates, to produce a place name; no identity	Members, during sessions
Stripe	Subscription billing	Chapter officers only
Website analytics and campaign tags	Website visits and marketing attribution	Website visitors only; never member data

The mobile apps contain no third-party analytics, advertising, or crash-reporting tools.

Roles

Role	Sees and does
Student	Own hours and sessions
Study Admin, Service Admin, Event Admin	Their area, for their chapter
Chapter Admin	Their chapter
Global Admin (GreekHours staff, not a chapter role)	Support and operations

The five chapter roles are held by members of your chapter. Global Admin is GreekHours staff only.

Shared report tiers

Tier	Shows	Never shows
Full Detail	Members by name, hours by category, compliance status	Location, financial or fine detail
Anonymized Detail	Random per-report labels, hours by category, compliance status, date-only "as of"	Names, emails, identifiers, exact timestamps, location, financial detail
Summary Only	Chapter totals	Any member rows

All tiers: read-only link, date and category scoping, expiration, revocation, rate-limited.

Retention schedule

Data	Kept for	Then
Raw session coordinates and place name	120 days after the session or semester end, whichever protects you more	Deleted; result, duration, hours remain
Photo evidence location data	Location metadata stripped on upload	Deleted
Athena conversations	120 days after last use or semester end, whichever protects you more	Deleted; members can delete sooner
Escalated support transcripts	120 days	Deleted
Shared report links	120 days from creation or end of semester, whichever is sooner	Expires; can revoke sooner
Dormant account with no chapter	No sign-in for two semesters	Notice, then deleted 30 days later
Chapter whose subscription lapsed	Access ends at lapse; data kept two semesters	Notice, then deleted; can request sooner
Application logs	90 days; no coordinates or personal details	Expire
Database backups	7 days	Roll over; deleted data gone within a week

Scope

> This is an operational trust summary, verified against the live system. It is not a legal contract; the Terms of Service and Privacy Policy govern.
>
> Chapters with institution-specific requirements should route final review through their campus process.

Evidence you can ask for

Everything on this list exists and can be produced on request.

1. Privacy Policy: greekhours.com/privacy
2. Terms of Service: greekhours.com/terms
3. Security disclosure page: greekhours.com/security
4. Machine-readable security contact: greekhours.com/.well-known/security.txt
5. Deletion request path, linked from the Privacy Policy
6. Role-permissions summary
7. Shared report controls summary
8. Third-party list (fact sheet)
9. Retention schedule (fact sheet)
10. Microsoft Azure compliance and Azure AI data-handling documentation

Keeping this true

This document is re-verified against production once per semester and after any architecture change. The "verified against production" date at the top is the last time every statement was checked.

John Daniels
Founder, GreekHours

Signature

Date

This document is provided for chapter decision support and does not constitute legal advice. Chapter advisors and institutional counsel should be consulted for formal legal requirements.