CliqWave — Privacy Policy

Effective Date: February 16, 2026

Last Updated: February 16, 2026

This Privacy Policy explains how Greek Time Corp ("Greek Time," "we," "our," or "us") collects, uses, discloses, and protects information about you when you use our CliqWave mobile applications, websites, and related services (collectively, the "Services"). If you do not agree with this policy, please do not use the Services. By using the Services, you consent to the practices described here.

Quick Summary

- We collect only what we need to run a group communication platform (accounts, messages, media you upload, device/app info).
- Precise location is opt-in and used only for features you enable (e.g., nearby events).
- We never sell your data. We allow limited sharing for service providers and safety.
- You control: profile, marketing choices, permissions (camera, photos, mic, notifications, precise location), and can request access/deletion.

1) Who We Are & How to Contact Us

Controller: Greek Time Corp

Address: 1001 S Harrison, West, TX 76691

Email (privacy): privacy@cliqwave.com

Support: support@cliqwave.com

2) Scope

This policy covers information we collect when you:

- Use the CliqWave mobile app or website.
- Communicate with us (e.g., support, feedback, social media).
- Participate in events, surveys, beta tests, or promotions we host.

This policy does not cover third-party sites or services you access through the Services (e.g., links shared in chat).

3) Information We Collect

We collect the categories of information below. Some data is provided by you; some is created by your use of the Services; some is obtained from third parties (e.g., app stores).

1. A. Information You Provide

- Account & Profile: name, username/handle, email, phone (optional), profile photo, school/organization, role, graduation year (optional), Greek organization affiliation (optional), biography (optional).
- Content: messages, posts, reactions, polls, events, attendance, files and media you upload (images/videos/documents), and metadata (timestamps, group IDs).

- Preferences & Consents: settings, notification choices, marketing preferences, permission opt-ins (e.g., location, contacts).
- Support & Feedback: issue reports, feature requests, emails, and forms.

2. B. Information Collected Automatically

- Usage & Device: app and OS version, device model, device identifiers (e.g., vendor/device ID; we do not collect your phone's advertising ID unless you opt into marketing personalization), language/locale, time zone, crash logs.
- Activity: pages/screens viewed, taps/clicks, session duration, referral/UTM info, feature usage (e.g., polls created, messages sent).
- Network & Security: IP address, country/region, connection type; system events for fraud/abuse prevention.

3. C. Location Data (Opt-In)

- Approximate location may be inferred from IP for security and basic analytics.
- Precise location (GPS, Bluetooth, or similar) is collected only if you explicitly enable it in your device settings or in-app and is used solely to power features you turn on (e.g., nearby events, geofenced check-ins). You can disable this at any time in your device settings.

4. D. Information from Others

- Organizations & Group Admins: rosters, roles, and metadata your organization provides (e.g., chapter/club name, officer status).
- Sign-in Providers: if you use a third-party sign-in, we receive basic profile details per that provider's disclosure.

Sensitive Data: We do not require sensitive personal data (e.g., precise geolocation, government IDs, health, or biometric data). If you choose to share sensitive data in free-text content, you do so at your own discretion. Do not upload unlawful or inappropriate content.

4) Why We Use Your Information (Purposes & Legal Bases)

- Provide and maintain the Services (account creation, authentication, messaging, media hosting, event tools, attendance, search).

Legal bases (EU/UK/BR): Contract; Legitimate interests.

- Safety, moderation, and integrity (detect spam, abuse, policy violations; protect users and organizations). Some checks are automated.

Legal bases: Legitimate interests; Legal obligation; Vital interests in emergencies.

- Improve and develop features (analytics, debugging, research, A/B tests, quality assurance).

Legal bases: Legitimate interests; Consent where required (e.g., certain analytics/cookies on web).

- Communications (service messages, updates, security alerts).

Legal bases: Contract; Legitimate interests; Legal obligation.

- Marketing (with your consent where required). You can opt out of marketing at any time.

Legal bases: Consent; Legitimate interests, as applicable.

- Compliance and enforcement (terms, policies, legal rights, requests from authorities consistent with law).

Legal bases: Legal obligation; Legitimate interests. We do not use your personal information for fully automated decisions that have legal or similarly significant effects without human review.

5) How We Share Information

We do not sell your personal information. We disclose limited information to:

- Service Providers / Sub-processors who process data for us under contract (access limited to what's needed and subject to confidentiality/security obligations), including:
- Google Cloud Platform (GCP): hosting, databases, logs, cloud functions.
- Amazon Web Services (AWS): compute, storage, databases, queues, and related infrastructure.
- Cloudflare: media storage/CDN, image/video optimization, DDoS protection.
- Email/SMS and push notification providers: to send transactional communications.
- Analytics, crash, performance, and marketing measurement tools (e.g., Meta Pixel): to understand and improve the app and measure the effectiveness of marketing.
- Organization Admins and Members: Your profile, messages, media, and activity in a group are visible to members of that group. Admins may export limited group records (e.g., attendance) per feature design.
- Legal, Safety, and Rights: To comply with law, enforce terms, or protect anyone's safety, property, or rights.
- Business Transfers: If we undergo a merger, acquisition, or asset sale, your information may transfer as part of that transaction with notice as required by law.

Public/External Sharing: Content you post in public or broadly-accessible areas (if any) may be visible outside your group. Use caution when sharing links and personal details.

6) Data Retention

- Account data: retained while your account is active; if you delete your account, we generally delete or anonymize within 30-90 days, subject to legal or safety holds.
- Messages and media: retained per product functionality and your organization's settings; deleted account removal typically removes personal pointers to content, but copies may persist in backups for up to 90 days.
- Logs and security data: typically 12-24 months for fraud/abuse, audit, and service integrity.
- Legal holds: retained as required by law or to resolve disputes.

7) Security

We use technical and organizational measures aligned with industry practices to protect information, including encryption in transit, hardened network boundaries, least-privilege access, and continuous monitoring. No system is 100% secure. Incident Response: If we learn of a breach affecting your information, we will investigate, notify affected users and/or authorities as required by law, and take steps to mitigate harm.

8) Your Choices & Controls

- Permissions: You can control access to camera, photos, microphone, contacts, notifications, and precise location in your device settings. The app works without precise location, though some features may be limited.
- Marketing: Opt out of marketing emails via the unsubscribe link; control push notification types in app settings.
- Profile & Content: You can view, edit, or delete your profile and content you posted (subject to group/admin policies and technical limits).

- Cookies & Similar Tech (web): We use cookies and similar technologies (including pixels like the Meta Pixel) to measure marketing effectiveness and improve our web experience. Manage preferences via your browser settings and controls where applicable.

9) Your Privacy Rights

- Access and port your data.
- Correct inaccurate data.
- Delete data.
- Opt out of: (a) targeted advertising, (b) sale or sharing of personal information, and (c) certain profiling. We do not sell personal information.
- Limit use/disclosure of sensitive personal information (we don't use SPI for additional purposes).
- Withdraw consent where processing is based on consent.
- Appeal a decision if we deny your request (US state laws).

To exercise rights, email privacy@cliqwave.com. We will verify your request and respond as required by law. Authorized agents may submit requests with proof of authority. We will not discriminate against you for exercising your rights. California (CPRA) Notice at Collection: We collect the categories listed in Section 3 for the purposes described in Section 4, retain them as described in Section 6, and share them with the parties in Section

5. We do not sell personal information or share it for cross-context behavioral advertising.

EEA/UK (GDPR): You may lodge a complaint with your local supervisory authority. Where we rely on consent, you may withdraw it at any time.

10) Children's Privacy

The Services are intended for college-age and adult users. We do not knowingly collect personal information from children under 13 (or under the age required by your country). If you believe a child has provided us information, contact privacy@cliqwave.com and we will take appropriate steps to delete it.

11) International Data Transfers

If you access the Services from outside the United States, your information may be processed in the U.S. and other countries with different data protection laws. Where required, we use appropriate safeguards (e.g., Standard Contractual Clauses) for transfers.

12) In-App Moderation & Safety

- We use a combination of automated systems and human review to detect spam, fraud, and content that violates our policies (e.g., sexual content involving minors, illegal drugs sales, threats, harassment). Automated systems may analyze text, images, videos, and metadata.
- Moderation actions can include warnings, content removal, feature limits, or account suspension. Serious violations may be escalated to relevant authorities or your organization as required by law and our terms.
- We may preserve content when we reasonably believe it's necessary for safety, legal obligations, or to investigate violations.

13) Third-Party Services

The Services may link to or integrate with third-party services (e.g., social media links, external websites shared by users). Their privacy practices are governed by their own policies. Please review those policies before sharing information.

14) Do Not Track & Global Privacy Control

Some browsers offer Do Not Track (DNT) or Global Privacy Control (GPC) signals. Our web Services honor GPC for opt-out signals where legally required. Otherwise, we currently do not respond to DNT.

15) State-Specific Disclosures (U.S.)

Residents of certain U.S. states (including CA, CO, CT, UT, VA, TX, OR, FL) have specific rights noted in Section 9. You can exercise rights via privacy@cliqwave.com. Appeals: If your request is denied, you may submit an appeal by replying to our decision email with “Appeal” in the subject line. If denied again, you may contact your state Attorney General.

16) Data Categories Mapping (CPRA)

Category	Examples	Source	Purpose	Shared With
Identifiers	name, email, phone, user ID, device ID, IP	you; device	account, security, communications	service providers; group admins (limited)
Customer Records	profile, school/org, role	you; org admins	operate services, roster features	service providers; org admins
Protected Classification (optional)	none required	n/a	n/a	n/a
Commercial Info	subscriptions, in-app purchases	you; app store	billing, support	payment processors
Internet/Network Activity	app usage, logs, crash	device	analytics, security	service providers
Geolocation	precise (opt-in); approximate by IP	device; IP	features you enable; security	service providers
Audio/Visual Content	images, videos you upload	you	messaging, media features	service providers; group members
Inferences	feature usage segments	analytics	improve services	service providers
Sensitive PI	not required; only if you choose to share in content	you	none	none

17) How to Exercise Your Rights

Email privacy@cliqwave.com with:

- What you're requesting (access/copy, correction, deletion, opt-out, etc.).
- The email/phone tied to your account.
- Any additional verification we request to protect your account.

We will respond within the timeframe required by law (often 30-45 days).

18) Changes to This Policy

We may update this policy from time to time. If we make material changes, we will notify you by email, in-app notice, or other appropriate method. The "Effective Date" above reflects the latest version.

19) Contact

Greek Time Corp

Email (privacy): privacy@cliqwave.com

Support: support@cliqwave.com

Address: 1001 S Harrison, West, TX 76691