

Privacy Policy for NovaLync
Effective Date: July 2026
Last Updated: September 2026

H&G Nextgen Private Limited ("we", "us", or "our") operates the NovaLync mobile application (the "Service"). This Privacy Policy explains how we collect, use, disclose, and safeguard your personal information when you use our application.

By installing or using NovaLync, you consent to the data practices described in this policy.

1. Information We Collect

We collect information strictly necessary to provide a personalized, secure, and fraud-free experience:

A. Personal Information

- **Account Profile:** When registering via Google Sign-In, Apple ID, or Email, we collect your display name, email address, and profile photo URL.
- **Authentication Credentials:** All logins are processed securely through Firebase Authentication. We never store your passwords in plaintext on local storage or external servers.

B. Progression & App Usage Data

- **Daily Task Records:** Your completed task IDs, selected learning journey (Communication, Wealth & Tech, or Zen Mode), and daily 10-task quota state.
- **Nova Coins & Ledger:** Authoritative coin balances, daily points breakdown, active cycle scores, and boost slot history.
- **Squad Mining & Team Sync:** Squad membership, daily mining slot synchronization timestamps (Morning, Afternoon, Night), and cooperative synergy multipliers.
- **Pioneer Referrals:** Your unique referral code (NVA-XXXXXX), the referral code of the pioneer who invited you, and referral rewards claimed (+1,000 for referrer, +500 for referee).
- **Local Preferences:** Language selection (Telugu, English, Hindi) and onboarding completion status stored locally in SharedPreferences.

C. Device & Security Telemetry (Anti-Fraud Protection)

To protect our rewards ecosystem from bots, emulator farms, and multi-account farming:

- **Hardware & Device Identifiers:** Anonymized device hardware hash to enforce single-claim referral limits per physical device.
- **Network & Security Logs:** Server-derived IP address (maintained in a rolling FIFO history capped at 5 entries), connection type, and login timestamps.
- **App Attestation:** We utilize Google Play Integrity via Firebase App Check to verify that requests originate from authentic, untampered NovaLync installations.

2. Zero-PII Analytics Policy

We use Google Analytics for Firebase and Firebase Crashlytics solely for monitoring application stability, diagnosing crashes, and understanding feature engagement. We do NOT pass your personal name, email, or exact physical location to analytics tracking services.

3. Third-Party Services

Our application integrates trusted third-party SDKs that process data under their respective privacy policies:

- Google Play Services: App delivery, installation attribution, and Play Integrity attestation.
- Firebase (Google Cloud): Authentication, Cloud Firestore database, Cloud Functions, and Firebase Cloud Messaging (FCM).
- Google Mobile Ads (AdMob): Serving rewarded video ads and interstitials to support our free micro-learning platform.

4. Data Retention and Security

Your progression data is stored securely in Google Cloud Firestore with automatic offline SQLite caching. We implement industry-standard security protocols:

- HTTPS / TLS encryption for all data in transit.
- Deny-by-default database security rules preventing unauthorized data modification.
- Server-side authoritative validation for all coin increments and daily limits.

5. In-App Account & Data Deletion (Erase Protocol & 6-Month Grievance Holding)

You have the complete right to request the permanent deletion of your account and associated data at any time:

- In-App Deletion: Open Profile -> System Protocols -> tap 'Delete Account'. This immediately triggers an automated serverless deletion of your active user document, referral links, and Firebase authentication credentials.
- 6-Month Grievance & Regulatory Vault: In strict accordance with financial transparency, fraud audit, and digital consumer dispute protocols, core ledger audit metadata (UID, email hash, totalPointsAtDeletion, streaks, referralCode, and deletion timestamp) is retained securely in the 'deleted_accounts' encrypted database for a period of exactly 180 days (6 months).
- Automatic Purge: Once the 180-day grievance window lapses, all held archive records are permanently, irrevocably destroyed by automated system cron cycles.
- Manual Request: You may also email our Data Protection Officer at contact@handgnextgenpvtltd.com with your registered email.

6. Contact Information

If you have any questions, concerns, or privacy requests:

Company: H&G Nextgen Private Limited

Support Email: contact@handgnextgenpvtltd.com