

PRIVACY POLICY

Effective Date: 20-07-2026

Last Updated: 20-07-2026

This Privacy Policy explains how **EternalGranth**, operating as **EternalGranth**, collects, uses, stores, shares, and protects personal information when you use the EternalGranth mobile application, website, customer support, and related services collectively referred to as the “Service”.

In this Privacy Policy, “EternalGranth”, “we”, “us”, and “our” refer to **EternalGranth**.

By using the Service, you acknowledge the practices described in this Privacy Policy.

1. Scope of This Privacy Policy

This Privacy Policy applies to personal information processed through:

- the EternalGranth mobile application;
- the EternalGranth website;
- user accounts;
- Google Sign-In;
- Sign in with Apple;
- scripture-based AI conversations;
- question-credit and subscription systems;
- payment-verification records;
- customer support;
- analytics, security, and crash-reporting systems; and
- account and data-deletion requests.

This Privacy Policy does not govern third-party services that operate under their own privacy policies, such as Google, Apple, payment platforms, or external websites.

2. Information We Collect

The information we collect depends on how you use the Service and which permissions or features you choose.

2.1 Account and Identity Information

When you sign in using Google, Apple, or another supported provider, we may receive:

- your name;
- email address;
- provider-specific user identifier;

- profile image, where provided;
- authentication tokens or verification information; and
- account sign-in method.

When you use Sign in with Apple, Apple may provide a private relay email address instead of your personal email address.

We do not receive your Google or Apple password.

2.2 Questions, Chats and User Content

When you ask a question or use chat features, we may process:

- the text of your question;
- selected scripture or spiritual perspective;
- AI-generated response;
- chat title;
- conversation history;
- feedback or ratings;
- language preference; and
- date and time of interactions.

Questions may reveal personal or sensitive matters, including information concerning spiritual beliefs, emotional condition, relationships, family, health, work, or personal decisions.

Please submit only the information necessary to receive the requested response.

2.3 Purchase and Credit Information

When you purchase question credits or subscriptions, we may receive or store:

- product or plan purchased;
- transaction identifier;
- purchase token or receipt information;
- payment status;
- purchase date;
- currency;
- country or storefront;
- credit balance;
- subscription status; and
- refund or cancellation status.

Payments may be processed by Google Play, Apple App Store, or another payment provider.

We generally do not receive or store your full debit-card, credit-card, bank-account, UPI PIN, or payment-password information.

2.4 Device and Technical Information

We may automatically collect:

- application version;
- language and locale;
- IP address;
- login timestamps;
- request timestamps;
- crash reports;
- performance information;
- security logs; and
- diagnostic information.

We may use this information to operate the application, identify technical issues, prevent abuse, and improve reliability.

2.5 Usage Information

We may collect information about how the Service is used, including:

- features accessed;
- scriptures selected;
- number of questions asked;
- free questions or credits used;
- session duration;
- buttons or screens viewed;
- subscription or purchase interactions;
- error events;
- account-deletion activity; and
- general engagement patterns.

2.6 Communications and Support Information

When you contact us, we may collect:

- your name and email address;
- support request;
- attachments or screenshots;
- transaction information;
- technical details;
- complaint history; and
- our correspondence with you.

2.7 Information We Do Not Intentionally Request

We do not intentionally request:

- account passwords;

- complete payment-card details;
- banking passwords;
- UPI PINs;
- government identification documents;
- biometric data;
- precise GPS location;
- personal medical records; or
- information about another person without their permission.

Please do not include such information in your questions or support requests.

3. How We Use Information

We may use personal information to:

1. create and manage your account;
2. authenticate you through Google, Apple, or another provider;
3. provide three free questions or other promotional benefits;
4. maintain question-credit balances and subscription entitlements;
5. process and verify purchases;
6. generate scripture-based AI responses;
7. save and display chat history;
8. remember your language and scripture preferences;
9. provide customer support;
10. investigate failed payments or missing credits;
11. maintain application security;
12. prevent account sharing, fraud, automated usage, and abuse;
13. diagnose crashes and technical issues;
14. analyse and improve performance and user experience;
15. comply with laws and legal requests;
16. enforce our Terms and Conditions;
17. protect users, our rights, and our systems;
18. send essential service-related notices; and
19. perform other activities with your consent where consent is required.

We do not use your questions to make legally significant decisions about employment, credit, insurance, housing, or eligibility for essential services.

4. AI Processing

To generate a response, your question and relevant conversation context may be transmitted to one or more AI, cloud-computing, retrieval, database, or infrastructure providers acting on our behalf.

Depending on how the Service is configured, these providers may process:

- question text;

- recent conversation context;
- selected scripture;
- language;
- generated answer;
- technical metadata; and
- safety or abuse-detection signals.

We take reasonable steps to send only the information needed to provide the response.

You should not enter confidential information, passwords, payment credentials, government identifiers, or unnecessary sensitive information into an AI conversation.

AI-generated responses may be inaccurate or incomplete. Privacy protections do not make an AI response spiritually, factually, medically, legally, or professionally reliable.

5. Legal Grounds for Processing

Depending on your location and applicable law, we process personal information on one or more of the following grounds:

5.1 Performance of a Contract

We process information where necessary to:

- create your account;
- provide questions and responses;
- maintain chat history;
- manage credits;
- fulfil purchases; and
- provide requested support.

5.2 Consent

We may rely on consent for:

- optional communications;
- optional analytics or advertising technologies;
- processing requiring explicit consent;
- device permissions; and
- processing children's data where parental consent is legally required.

You may withdraw consent where applicable, although this will not affect processing already lawfully completed.

5.3 Legitimate Interests or Permitted Uses

Where legally available, we may process information for legitimate operational interests, including:

- securing the Service;
- preventing fraud;
- diagnosing errors;
- improving performance;
- enforcing our agreements; and
- protecting legal rights.

We consider the impact of this processing on users' rights and interests.

5.4 Legal Obligations

We may process or retain information to comply with:

- accounting and tax obligations;
- lawful government requests;
- consumer-protection requirements;
- fraud-prevention obligations;
- court orders; and
- other legal duties.

6. How We Share Information

We do not sell personal information for money.

We may share limited information in the following circumstances.

6.1 Service Providers

We may use service providers for:

- artificial-intelligence processing;
- cloud hosting;
- authentication;
- databases;
- analytics;
- crash reporting;
- security;
- customer support;
- email delivery;
- purchase verification; and
- payment processing.

These providers may process information only as necessary to perform their services, subject to their contractual obligations and applicable law.

6.2 Google and Apple

If you use Google Sign-In or Sign in with Apple, information is exchanged with the selected authentication provider to complete login, maintain account security, and manage authentication.

Purchases made through Google Play or Apple App Store are processed according to the applicable platform's terms and privacy practices.

6.3 Legal and Safety Disclosures

We may disclose information where we reasonably believe it is necessary to:

- comply with applicable law;
- respond to a valid legal process;
- protect a person from serious harm;
- investigate fraud or security incidents;
- enforce our Terms;
- protect our users, rights, property, or systems; or
- establish, exercise, or defend legal claims.

6.4 Business Changes

If EternalGranth is involved in a merger, acquisition, financing, restructuring, or sale of assets, information may be transferred as part of that transaction.

Where required, we will provide notice before personal information becomes subject to a materially different privacy policy.

6.5 Aggregated or De-identified Information

We may create and use aggregated or de-identified statistics that do not reasonably identify an individual, such as:

- total questions asked;
- popular scripture categories;
- general usage trends;
- crash rates; or
- purchase-conversion statistics.

We may use this information for analytics, research, product improvement, or business planning.

7. Advertising

Choose and retain the statement that matches the application's actual implementation.

Advertising Is Used

EternalGranth may display advertisements through third-party advertising providers.

Advertising providers may process information such as:

- advertising identifier;
- IP address;
- device information;
- clicks;
- application interactions; and
- fraud-detection signals.

We do not intentionally provide the text of your private spiritual questions to advertisers for targeted advertising.

Where required, we will request consent before using advertising identifiers or personalised advertising. You may be able to manage advertising choices through the application, device settings, or consent interface.

8. Analytics and Crash Reporting

We may use analytics and crash-reporting tools to understand:

- application performance;
- technical failures;
- feature usage;
- device compatibility;
- user flows; and
- general engagement.

Where legally required, optional analytics will be based on consent or made subject to available controls.

Analytics information should be configured to avoid collecting unnecessary chat content or sensitive information.

9. Data Retention

We retain personal information only for as long as reasonably necessary for the purpose for which it was collected.

Typical retention principles include:

- account information is retained while the account remains active;
- saved chats are retained until deleted by the user, account deletion, or expiry under our retention practices;
- credit and subscription records are retained while needed to provide purchased benefits;
- transaction and tax records may be retained for the period required by law;

- security logs may be retained for a limited period to investigate fraud and abuse;
- support communications may be retained while required to resolve complaints and maintain records;
- backup copies may remain temporarily until they are securely overwritten; and
- information required for legal claims or regulatory obligations may be retained for the applicable legal period.

Our current standard retention periods are:

- Account profile: Until account deletion, plus up to 30 days for technical deletion;
- Saved chats: Until deleted by the user or account deletion;
- Security and access logs: Up to 30 days;
- Customer-support records: Up to 1 years after resolution;
- Purchase and accounting records: As required by applicable tax and accounting law;
- Backups: Up to 30 days after deletion from active systems.

Information may be retained longer where necessary for fraud investigation, legal compliance, dispute resolution, or legal claims.

10. Account and Data Deletion

You may initiate account deletion through:

App → Profile/Settings → Account → Delete Account

When an account is deleted, we will delete or de-identify personal information associated with it, subject to information we must retain for legal, accounting, security, fraud-prevention, or dispute-resolution purposes.

Account deletion may permanently remove:

- profile details;
- saved chats;
- selected preferences;
- usage history associated with the account;
- unused credits;
- promotional benefits; and
- account access.

Deleting your EternalGranth account:

- does not delete your Google or Apple account;
- may not automatically cancel an active App Store or Google Play subscription; and
- does not necessarily erase transaction information retained by Apple, Google, or another payment provider.

After deletion begins, some information may remain in encrypted backups until those backups are overwritten under our normal retention cycle.

11. Data Security

We use reasonable technical and organisational safeguards designed to protect information, such as:

- encrypted network transmission;
- authentication controls;
- restricted administrative access;
- secure cloud infrastructure;
- monitoring and logging;
- security updates;
- data minimisation;
- access-control policies; and
- backup and recovery procedures.

However, no electronic system or method of transmission is completely secure. We cannot guarantee absolute security.

You are responsible for securing your device, email account, Google account, Apple account, and login access.

If you believe your account has been compromised, contact **help@eternalgranth.com** promptly.

12. Data Breaches

If a personal-data breach occurs, we will investigate and take reasonable steps to contain and address it.

Where applicable law requires, we will notify relevant authorities and affected users within the legally required period.

Notifications may include information concerning:

- the nature of the incident;
- information potentially affected;
- measures we have taken;
- protective actions users may take; and
- how to contact us.

13. Device Permissions

Depending on the features you use, the application may request permissions such as:

- microphone access for voice questions;
- speech-recognition access;
- notification permission;

Permissions are requested only when relevant to a feature.

You can manage permissions through your device settings. Disabling a permission may prevent the relevant feature from working.

Where voice input is enabled, audio may be processed by the device, operating-system provider, speech-recognition provider, or our authorised service provider. The application should separately disclose whether audio recordings are stored or deleted after transcription.

14. Notifications and Communications

We may send essential communications concerning:

- account security;
- purchases;
- credit balances;
- subscription status;
- important Service changes;
- account deletion;
- legal updates; and
- support requests.

With permission, we may also send:

- daily spiritual quotes;
- reminders;
- new-feature announcements;
- promotional offers; or
- engagement notifications.

You can manage optional push notifications through application or device settings.

Essential account, security, purchase, and legal notices may still be sent where necessary.

15. Changes to This Privacy Policy

We may update this Privacy Policy to reflect:

- changes to the Service;
- new providers or technologies;
- new data practices;
- legal requirements;
- new countries of operation; or
- security and operational improvements.

We will update the “Last Updated” date when revisions are published.

Where a change materially affects your rights or requires consent, we will provide additional notice or request consent as required by law.

16. Contact Us

For privacy questions, rights requests, complaints, or account-deletion assistance, contact:

EternalGranth

Email: help@eternalgranth.com