

Privacy Policy for Falorax Focus

Last Updated: July 2026

1. Introduction

This Privacy Policy governs the data handling practices of Falorax Focus ("the App"). We are committed to maintaining the highest standards of user privacy and data security. By installing and using the App, you explicitly consent to the practices described in this policy.

2. Zero Data Collection Policy (Information We Do NOT Collect)

Falorax Focus operates on a strict zero-data-collection model. The App does NOT collect, transmit, upload, or share any personal or non-personal data to external cloud servers, databases, or third parties. Specifically, the App does NOT access, track, or record:

- Personal Identifiable Information (PII) such as names, email addresses, or phone numbers.
- Real-time or historical location data.
- Device storage contents (contacts, SMS, photos, or personal files).
- Keystrokes, passwords, or notification data.
- Third-party analytics data or user behavior tracking.

For app and website blocking, the App reads limited on-screen information locally and in real time (described in Section 4). This information is used only to enforce your blocking choices and is never collected, stored, or transmitted.

3. Local Storage and Data Retention

All application data is generated and stored locally and exclusively within your device's sandboxed storage environment using Android's Room Database and DataStore. This data includes:

- Session Logs: Start time, duration, and completion status of focus intervals.
- Aggregated Statistics: Daily focus minutes, active session counts, and recorded distraction attempts.
- App Configuration: User-defined blocked app lists (package names), Usage Limits, Study Mode allowed websites, Feed Blocking preferences, Pomodoro settings, and strict mode preferences.

Data Retention: This data remains on your device for as long as the App is installed. You may delete individual logs from within the App settings. Uninstalling the App permanently deletes all local data. Because we do not maintain cloud backups, this data cannot be recovered once deleted.

4. Android Accessibility Service Declaration

To provide its core app and website blocking features, the App uses Android's AccessibilityService API to read limited information about what is currently on screen — in real time, on your device, and only to decide whether to block:

- Foreground app detection: the package name of the app currently open, so it can block apps you have selected (during focus sessions) and enforce always-on features such as Usage Limits and Feed Blocking.
- Study Mode: the web address shown in your browser's address bar, compared only against the list of websites you have allowed. If a site is not on your list, you are redirected away from it.
- Feed Blocking: the on-screen layout identifiers used to recognise short-video feeds (such as Reels or Shorts), so those feeds can be blocked while the rest of the app keeps working.

This information is used only in the moment, solely to enforce your own blocking choices. The Accessibility Service does NOT log keystrokes or passwords, capture screenshots, record or store the content of pages or apps, or read your notifications or messages. It operates entirely offline, and nothing it reads is ever saved, logged, or transmitted off your device.

5. Sensitive Permissions Usage

To perform its core utility features effectively, the App requests the following native Android permissions:

- Usage Access Permission: Used to identify the foreground application's package name and to measure per-app usage time for Usage Limits. It does not profile or log your general app usage habits beyond enforcing your own limits and blocking.
- Display Over Other Apps (System Alert Window): Used exclusively to render the blocking screen overlay and the optional floating timer. No background ads or malicious overlays are generated.
- Notifications (optional): Used only to show the ongoing focus-session controls in your status bar.
- Ignore Battery Optimization (optional): Requested only so blocking stays reliable while the screen is off. This is optional and never forced.

6. Children's Privacy (COPPA & GDPR Compliance)

Since Falorax Focus does not collect, harvest, or transmit any data from any device, the App is inherently compliant with the Children's Online Privacy Protection Act (COPPA) and General Data Protection Regulation (GDPR). We do not knowingly target or collect data from children under the age of 13.

7. Third-Party Libraries and SDKs

The App does not embed any third-party software development kits (SDKs), advertising frameworks, tracking pixels, or crash-reporting libraries that collect user data. The codebase is self-contained and privacy-first.

8. Changes to This Privacy Policy

We reserve the right to update this Privacy Policy at any time to reflect changes in app functionality or legal requirements. Any modifications will be updated within this document. Continued use of the App after updates constitutes acknowledgment and acceptance of the revised terms.

9. Contact and Support

If you have any questions, compliance inquiries, or feedback regarding this Privacy Policy, please reach out to us at:

Developer Email: florax558@gmail.com