A NOTE FROM THE MAINTAINER

Security & Privacy

Plain commitments. What we do, what we don't, and why.

> Sissy Conditioner is built on a simple principle: **what happens on your phone stays on your phone.** Your media, your prompts, your session history, the name you choose for yourself — none of it leaves your device. We treat your privacy the way we'd want our own treated.

Your content stays on your device

Everything you put into the app — photos, videos, audio, custom prompts, session history, achievements, your profile name and picture — lives in the private storage area Android gives to each installed app. We don't have a cloud backup. We don't sync your content to our servers. From our side, the content is invisible.

If you uninstall the app, that content is permanently removed from your device along with it. If you want to preserve it, the app includes a manual backup feature that exports everything to a single encrypted file — protected by a passphrase you choose, and decryptable only by you.

The remote-control feature is private — even from us

If you choose to use the optional partner-control feature, the commands sent between the two phones are end-to-end encrypted. Each phone holds the secret key needed to read the messages it receives; those keys are generated on the phones themselves and never transmitted. Our server relays the encrypted messages without ever seeing what's inside them.

This means that even in the unlikely event of a server-side compromise, the contents of those commands would remain unreadable. Our infrastructure is technically incapable of decrypting them.

The feature is optional and entirely off until you turn it on.

What we deliberately do not collect

- **No usage tracking.** We do not record what you tap, when you tap it, how long you spend in a session, or which features you use.
- **No analytics or telemetry.** The app has no first-party or third-party analytics SDK of any kind.
- **No crash reporting.** We don't have a service watching for app crashes and uploading reports.
- **No advertising identifiers.** We don't read your device's advertising ID and we have no ad partners to share it with.
- **No identifying details beyond the bare minimum.** When you download the app, we verify your Patreon subscription is active. Once the app is installed, no further check-in with us happens.

Protections you can turn on

All of the features below are optional and off by default. You decide how much protection you want.

- **App lock.** Require a fingerprint, face unlock, or PIN every time the app opens.
- **Self-destruct.** Wipe all app data after a number of failed unlock attempts that you set. Cannot be reversed once triggered.
- **Force-quit protection.** If you're in the middle of a locked session and force-quit the app, the lock is automatically resumed on next launch — closing the most common "I'll just close the app" workaround.
- **Encrypted backup.** Export your full app state to a single encrypted file. Choose your own passphrase. Without that passphrase, the file is unreadable.
- **Volume lock.** Pin the audio volume to a level you set, so an attempted volume change during a session bounces back.

How the app is delivered

The app is distributed only through a Patreon-gated download. When you go to download, you sign in with Patreon, your subscription status is verified, and a one-time download link is granted. The app itself is cryptographically signed; if any third party tries to redistribute a modified copy under our name, the modified copy will refuse to run on your device.

We do not list the app on any public app store, and we do not distribute it through any other channel. If you obtained it anywhere else, please ask the creator directly — that copy may not be trustworthy.

If something feels wrong

If you believe you've found a security issue — anything from a small bug in a privacy-relevant feature to a more serious concern — please contact the maintainer directly via Patreon message. Reports are handled confidentially. The maintainer commits to replying within three business days, and to working with you on a remediation plan if the report is confirmed.

> **Bottom line.** The app is built so that the maintainer is the worst-positioned person on the planet to invade your privacy. Most of the data simply never reaches us. The data that does reach us, for the brief moments it has to, is encrypted in a way we cannot open. That is not an accident — it's the design.
