EAGLE CORPORATION

(Australasia) Pty Limited

DeepFake DEFENDER

Privacy Policy

Eagle Corporation (Australasia) Pty Limited

Trading as DeepFake DEFENDER

ABN 67 089 764 358 · ACN 089 764 358 · ASIC Key 1-74110561520

Registered 28 January 2026 · Canberra, Australia

Document Version 1.0

Effective Date: 15 May 2026

The Short Version

> *DeepFake DEFENDER collects nothing.*
>
> *It stores nothing.*
>
> *It transmits nothing about you.*
>
> *Your browsing stays entirely on your device.*

If that is all you wanted to know, you can stop reading. The detailed sections below explain how this is achieved, what limited exceptions exist, and what your rights are.

1. About This Policy

This Privacy Policy applies to the DeepFake DEFENDER iOS application ("the App") and to the website at https://www.deepfakedefender.com.au ("the Website"), together "the Service".

The Service is operated by Eagle Corporation (Australasia) Pty Ltd, ABN 67 089 764 358, ACN 089 764 358, ASIC Key 1-74110561520, trading as DeepFake DEFENDER ("the Company").

This policy explains how the Service handles — or, more precisely, does not handle — personal information. It applies to all users of the Service worldwide.

2. Information We Do Not Collect

DeepFake DEFENDER is designed from the ground up to operate without collecting any personal information. Specifically, the App does not collect, store, transmit, or share:

- Your name, email address, phone number, or any account credentials.
- Your social media account details or login information.
- Your browsing history, social media feeds, or the content you view.
- Your device identifiers, advertising IDs, or IP address.
- Your location data.
- Any images, videos, or media from your social media feeds.
- Usage analytics, crash reports, or diagnostic data sent to the Company.
- The contents of your Sanity Log (a local-only encounter record under your control).
- The contents of your My Vocabulary list (custom terms you teach the on-device classifier).

No account is required to use the App. The App works immediately upon opening with no sign-in, no registration, and no data entry.

The App contains no Google Analytics, Firebase Analytics, Mixpanel, Segment, Amplitude, or any other third-party analytics SDK. The Company does not automatically collect telemetry, usage data, or location data through the Service.

3. How the App Works

DeepFake DEFENDER operates an on-device content analysis engine. When you browse a supported social media platform inside the App's protected browser, the analysis engine reads visible text elements from the page — captions, usernames, metadata — entirely within the App's local memory.

This data:

- Never leaves your device under normal operation.
- Is never written to disk or stored between sessions.
- Is never transmitted to the Company or any third party by the App itself.

All classification, scoring, and threat detection runs locally on your iPhone using on-device heuristics. Nothing you browse is logged.

Live coverage at launch includes X, Instagram, Facebook, TikTok, and YouTube. The in-app browser loads each platform's mobile site, and the typical and expected user experience is signed-in — the platform's own algorithms, personalised feed, security settings, and account features apply as they would in that platform's own app or website.

When you sign in, you do so through the platform's own login wall inside the in-app browser; your credentials and authentication go directly to the platform and are not seen, handled, or stored by the Service. Platforms vary in what they show to anonymous visitors who choose not to sign in: where a platform restricts content behind a login wall (as TikTok and parts of X do), the in-app browser will display that login wall and the user can choose whether to proceed.

For YouTube in v1.0, in-app sign-in is not yet supported and the in-app browser operates in public mode (browse, search, and watch public videos), with full sign-in coming in v1.1. Web traffic flows directly between your device and the social media platform you are visiting; the Company does not act as an intermediary, proxy, or recipient of that traffic. The respective platforms' own privacy policies apply to content shown in their pages, including any tracking or analytics those platforms perform.

The Sanity Log is a local-only feature that records counts of categories and platforms you have encountered, with user-selectable retention windows. The log never records the content of posts, URLs visited, images, video, or any identifier. The log lives on your device, is never transmitted, and clears when the App is removed.

My Vocabulary is a user-curated list of terms you choose to teach the on-device classifier. Each entry consists of the term, a category, and a weight. Entries are stored on your device only, never transmitted, never shared, and clear when the App is removed.

4. Optional AI Enhancement (Bring-Your-Own-Key)

DeepFake DEFENDER includes an optional feature, disabled by default, that uses an external Artificial Intelligence (AI) Application Programming Interface (API) to provide deeper analysis of certain posts. To use this feature you must provide your own API key from a supported provider — currently Anthropic, OpenAI, or xAI.

4.1 When the AI Enhancement Activates

If you choose to enable the AI enhancement, the feature activates only on posts where the local classifier flags a content pattern as warranting deeper analysis — specifically posts indicating possible influence operations, foreign state messaging, or ambiguous synthetic-content signals. Most posts you scroll past are never sent to any external service.

4.2 What is Sent, and to Whom

When the AI enhancement is enabled and a post triggers deeper analysis, a short text sample from that post is sent directly from your device to your chosen AI provider's API endpoint, using your API key. The Company is not part of this transmission. The Company does not see, log, or store the content of these requests, the responses, or any analysis results.

You should review the privacy policy of any third-party AI service whose API key you provide. Different AI providers have different data-retention practices.

4.3 Your Choice and Your Costs

Use of the AI enhancement is entirely your choice. The feature is disabled until you affirmatively enable it. You may disable it at any time. If you have not provided an API key, no external AI requests are ever made.

Any costs charged by the AI provider for use of your API key are your responsibility and are billed directly by the provider to you. The Company does not invoice you for AI-provider usage.

5. API Key Storage and Security

If you provide an API key, the App stores it exclusively in iOS Keychain — Apple's system-level secure-storage facility — on your device only. The Company does not transmit, log, copy, or have access to your API key under any circumstances.

API keys can be deleted by you at any time within the App via Dose of Sanity → Clean Reset + Forget API Key, or by uninstalling the App.

6. Information You Provide Voluntarily

If you contact the Company through the support email, the contact form on the Website, or any other support channel, the information you provide (your message, your reply-to email address, and any attachments) is retained by the Company for the purpose of responding to your enquiry and maintaining a record of communications. This information is not used for marketing, is not sold or shared, and is held in the Company's email systems located in Australia and the United States (depending on the email provider used).

If you sign up to receive launch notifications via the Coming Soon page on the Website, the email address you provide is held by the Company solely for the purpose of sending you a launch announcement. You may unsubscribe at any time. The list is not used for ongoing marketing and is not shared with third parties.

7. Crash Reporting

iOS may collect crash reports under your standard Apple device privacy settings. If you have opted in to sharing crash data with developers via your iOS Settings, Apple may forward anonymised crash diagnostics to the Company. These diagnostics contain no personally identifiable information and cannot be used to identify you. You can opt out at any time in iOS Settings → Privacy & Security → Analytics & Improvements → Share With App Developers.

8. Cookies and Similar Technologies

The App does not set cookies. The Website may set strictly necessary cookies for site functionality (such as session tokens for the contact form). No advertising or tracking cookies are used. The Website does not employ third-party advertising networks.

9. Children

The Service is not directed at children under the age of majority in their jurisdiction. The Company does not knowingly collect any information from children. If you believe a child has used the Service contrary to this policy, please contact the Company at the email address in section 13 so that the Company can take any appropriate action.

10. International Users

The Company is based in Canberra, Australia. By using the Service, you acknowledge that any minimal information stored is held in accordance with Australian privacy law, including the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Users in jurisdictions with stronger or different privacy regimes — including the European Union's General Data Protection Regulation (GDPR), the United Kingdom's UK GDPR, the United States' California Consumer Privacy Act (CCPA), and equivalent regional laws — retain all rights they have under those local laws, including rights to access, correct, and delete personal information held by the Company. To exercise those rights please contact the Company at the address in section 13.

11. Data Retention

Because the Company does not collect personal information from users through the App's normal operation, there is no personal data to retain or delete in respect of App use.

Information voluntarily provided to the Company through support channels or the Website contact form is retained for as long as is reasonably necessary to respond to and resolve the matter, after which it is archived in accordance with the Company's standard records-management practices and applicable law.

API keys and user preferences are retained on your device until you delete them or uninstall the App. They are never copied to any server controlled by the Company.

Your Sanity Log and My Vocabulary entries are retained on your device for as long as you keep them. Both can be cleared at any time from Dose of Sanity, and both clear automatically when the App is removed.

12. Your Rights

You may at any time:

- Delete user-provided API keys and preferences within the App, or by uninstalling the App.
- Opt out of Apple's analytics-sharing in iOS Settings → Privacy & Security → Analytics & Improvements.
- Request access to, correction of, or deletion of any personal information the Company holds about you that arose from voluntary contact (support, contact form, or launch notification list), by emailing the Company at the privacy contact address in section 13.
- Lodge a complaint with the Office of the Australian Information Commissioner (OAIC) if you believe the Company has handled your personal information in breach of the Australian Privacy Principles. The OAIC website is at www.oaic.gov.au.

13. Contact

Privacy questions, concerns, or requests may be directed to:

- *Eagle Corporation (Australasia) Pty Limited*
- *Trading as DeepFake DEFENDER*
-
- *Privacy enquiries: privacy@deepfakedefender.com.au*
- *Support enquiries: feedback@deepfakedefender.com.au*
- *Website: https://www.deepfakedefender.com.au*
- *Policies: https://www.deepfakedefender.com.au/policies*
-
- *Canberra, Australia*
- *ABN 67 089 764 358 · ASIC Key 1-74110561520*

14. Changes to This Policy

The Company may update this Privacy Policy from time to time. Material changes will be reflected in a new version number, and the current version will always be available at https://www.deepfakedefender.com.au/policies. The current version of this policy is Version 1.0, effective 15 May 2026.

The current bundled version is displayed within the App on first launch and within Dose of Sanity → Privacy Policy. A "Check for Updates" function within the App opens the latest version published on the Website. Material changes that affect User rights or obligations will be presented for acknowledgement on next launch of an updated App version.