

Noble - Privacy Policy

Effective Date: March 21, 2026

This Privacy Policy ("Policy") describes how Noble Software Limited ("we," "us," or "our") collects, uses, stores, and discloses information in connection with our software products and related services, including:

- NobleAIM
- Noble Trainer (including the Marketplace)
- Noble Remote

(collectively, the "Service")

Noble Software Limited (registered in England and Wales), with its registered address at 82A James Carter Road, Mildenhall, IP28 7DE, United Kingdom, is the data controller responsible for your personal data as described in this Policy.

By installing, accessing, or using the Service, you acknowledge that you have read, understood, and agree to be bound by this Policy. If you do not agree, do not install, access, or use the Service.

1. Information We Collect

1.1 Licence Validation (All Products)

When you activate or validate your licence, the following is sent to our server (hosted on Cloudflare Workers):

- Your License Key (forwarded to Whop for subscription validation)
- A hashed device identifier (used for device binding and enforcement)

We receive from Whop:

- Membership ID (anonymous identifier)
- Licence validity status, plan name, and renewal dates
- Whether cancellation is pending

We do NOT receive or store your email address, payment information, or billing details. All payment processing is handled solely by Whop.

1.2 Device Identification (NobleAIM)

To enforce the one-device limit, the Software generates a hardware identifier (HWID) derived from your Machine GUID, computer name, and CPU brand. This identifier is hashed using SHA-256 before transmission and is non-reversible. It is sent to our server during licence validation for device binding.

1.3 Application Telemetry (NobleAIM)

During licence validation, the Software also sends:

- Application version
- Session duration (time since last validation)

This data is used for analytics and service improvement.

1.4 Integrity Events (NobleAIM)

The Software includes a protection layer that detects tampering, debugging,

or unauthorised modification. When a tampering event is detected, the Software sends an integrity report to our server (/api/tamper) containing:

- Your HWID (hashed)
- The type of integrity violation detected
- A timestamp

Integrity events are used solely to protect the Software from unauthorised modification and to enforce licensing terms.

1.5 Marketplace Data (Noble Trainer)

- Display name (derived from your Whop username at activation)
- Models and content you upload to the Marketplace (files and metadata)
- Interaction data such as download counts and likes

1.6 Data Stored Locally on Your Device (All Products)

The following data is stored locally and is NOT transmitted to our servers:

- (a) License File: Stores your License Key locally.
- (b) Log Files: Diagnostic logs that may contain file paths, hardware information (GPU name, driver version), window titles, process names, and error messages. File paths may include your Windows username.
- (c) Crash Logs: Written locally if the software crashes.
- (d) Configuration Files: Your settings, profiles, and preferences.
- (e) Captured Frames (Noble Remote): Frames captured from gameplay windows are written to local shared memory only. They are not sent to any server.

None of these local files are automatically uploaded to our servers. If you contact us for support and voluntarily share files, they may contain the information described above.

1.7 Update Checks (All Products)

Products periodically check for updates by requesting a version file from our servers. These requests contain standard HTTP headers (User-Agent, IP address) but no personal data beyond what is inherent in any HTTP request.

1.8 Server Logs

Server logs may temporarily contain request timestamps, request paths, response status codes, and error messages. We do NOT log authorisation headers or full request bodies. Cloudflare may independently log IP addresses per their own policies.

2. How We Use Your Information

We use the information collected to:

- a) Validate your licence and enforce licensing terms (contract performance);
- b) Enforce device limits (contract performance);
- c) Detect tampering, debugging, or unauthorised modification of the Software (legitimate interest);
- d) Operate the Marketplace and provide the Service (contract performance);
- e) Provide update notifications (legitimate interest);
- f) Analyse application usage, version distribution, and session data to improve the Service (legitimate interest);
- g) Prevent fraud, abuse, and unauthorised access (legitimate interest);

h) Comply with legal obligations (legal obligation).

2.1 Legal Basis for Processing (UK GDPR)

- a) Contract Performance (Article 6(1)(b)): Processing necessary to provide the Service, including licence validation, session management, device activation, Marketplace operation, and update delivery.
- b) Legitimate Interests (Article 6(1)(f)): Processing necessary for fraud prevention, abuse detection, service improvement, and security. We have assessed that these interests do not override your fundamental rights. You have the right to object to processing based on legitimate interests (see Section 7).
- c) Legal Obligation (Article 6(1)(c)): Processing necessary to comply with applicable laws and regulations.

3. Third-Party Services

The Service relies on the following third-party providers:

3.1 Whop (whop.com)

- Purpose: License key validation and subscription management
- Data shared: Your License Key
- Data received: Membership ID, validity status, plan name, renewal dates
- Privacy policy: <https://whop.com/privacy>

3.2 Cloudflare (cloudflare.com)

- Purpose: Hosts our APIs (Workers), databases (D1, KV), and file storage (R2)
- Data processed: License Key, HWID (hashed), integrity events, application version, session duration, standard HTTP metadata
- Privacy policy: <https://www.cloudflare.com/privacypolicy/>

WE ARE NOT RESPONSIBLE OR LIABLE FOR THE PRIVACY PRACTICES, DATA HANDLING, SECURITY, OR POLICIES OF ANY THIRD-PARTY SERVICE PROVIDER.

4. International Data Transfers

The Service is hosted on Cloudflare's global infrastructure. Your data may be processed and stored in any country where Cloudflare operates, which may include countries outside the United Kingdom or European Economic Area. Cloudflare maintains appropriate safeguards for international transfers as described in their privacy policy.

5. Data Security

We implement commercially reasonable technical and organisational measures to protect your information, including:

- License Keys are transmitted over HTTPS (TLS encryption in transit)
- Device identifiers are SHA-256 hashed before transmission (non-reversible)
- User profiles and configuration data are encrypted locally
- The Software uses certificate pinning to prevent man-in-the-middle attacks
- Session data expires automatically

However, no method of electronic storage or transmission is completely secure. We do not warrant or guarantee the absolute security of your data. You are solely responsible for maintaining the confidentiality of your License Key.

6. Data Retention

Server-Side:

- Device identifiers (HWID): Retained for the duration of your subscription
- Integrity events: Retained for up to 30 days
- Subscription metadata from Whop: Not stored - returned in real-time
- Server logs (Cloudflare): Retained per Cloudflare defaults (typically up to 72 hours for Workers logs, up to 30 days for other services)
- Marketplace data (Noble Trainer): Retained until you delete it or request deletion

Local (on your device):

- License file: Retained until you deactivate or delete it
- Log files: Overwritten on each application launch
- Crash logs, configuration files: Retained until you delete them manually

We may retain certain data for longer periods where required by law, to resolve disputes, or to enforce our agreements.

7. Your Rights and Choices

You may:

- (a) Deactivate your device using the option within the software.
- (b) Delete local data (license files, logs, configuration) at any time.
- (c) Delete Marketplace content (Noble Trainer) through the software.
- (d) Contact us to request details of any data we hold, or to request deletion.

If you are located in the United Kingdom or European Economic Area, you have additional rights under UK GDPR, including:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object to processing based on legitimate interests

To exercise these rights, contact us using the details in Section 10. We will respond within one month of receipt, as required by UK GDPR. We may verify your identity before processing any request.

You also have the right to lodge a complaint with a supervisory authority. In the United Kingdom, this is the Information Commissioner's Office (ICO):

Website: <https://ico.org.uk>

Telephone: 0303 123 1113

8. Children's Data

The Service is not directed to individuals under the age of 18. We do not knowingly collect personal information from anyone under 18. If we become aware

that we have collected data from a person under 18, we will take reasonable steps to delete it.

9. Changes to This Policy

We may update this Policy by publishing a revised version on our website or within the Service. Material changes will be notified at least 14 days before they take effect. Your continued use of the Service after the effective date constitutes your acceptance of the revised Policy.

10. Contact

For privacy concerns or data requests, contact:

Noble Software Limited (registered in England and Wales)

Registered Address: 82A James Carter Road, Mildenhall, IP28 7DE, United Kingdom

Website: nobleaim.co.uk

Email: noblesupp@outlook.com