Usage Policy

Effective 22 Nov 2026 Version 1.0 For everyone

The short version

- Use Electron Hub lawfully and follow each model's own usage policy.
- Child sexual abuse material is never allowed, and we report it.
- No sexual imagery of real people without consent, weapons of mass harm, malware or fraud.
- Don't evade limits, moderation or bans, or share and resell access.

This summary helps you find your way. The full text below is what applies.

This Usage Policy is part of the Terms of Service and applies to everything you do with Electron Hub: the web app, the API, every plan and every Model. Each Model's own usage policy also applies (see Model Provider Terms); where it is stricter, the stricter rule applies to that Model.

1. Prohibited content

You may not use the Service to create, request, store, transmit or attempt to obtain:

- **child sexual abuse material**, or any sexualised content involving a minor or a person who appears to be a minor, including fictional, drawn or AI-generated content and "aged-up" framing (zero tolerance);
- content that sexualises a real, identifiable person without consent, non-consensual intimate imagery, or "nudified" images of real people;
- images or video of real, identifiable people (including public figures), deceptive impersonations or deepfakes, or content meant to defame, harass, threaten, stalk, intimidate or dox anyone;
- instructions, code or material that meaningfully helps create biological, chemical, nuclear or radiological weapons, explosives or other weapons capable of mass harm;

- malware, ransomware, phishing kits, exploits used without authorisation, or tools for credential theft, spam or fraud;
- content that promotes or incites terrorism, violent extremism or violence against people;
- content that encourages or instructs self-harm or suicide;
- unlawful discrimination, or hateful content targeting people for protected characteristics;
- content that infringes intellectual property, privacy or publicity rights, or discloses another person's personal data without a lawful basis;
- election interference, coordinated inauthentic behaviour or disinformation campaigns;
- any other content or activity that is illegal where you are or where we operate.

2. Images and video

Prompts for image and video generation, and images you submit for editing, are checked by automated moderation systems (which may include third-party moderation services) before generation. **Sexually explicit images and video are not allowed on these features for any user or plan.** If moderation is unavailable, we may refuse requests rather than process them unchecked. Generated media is stored at publicly accessible URLs (Terms Section 8.6), so do not put personal or confidential information in media prompts.

3. High-risk uses

Model output can be wrong. You may not rely on the Service without qualified human review for medical, legal, financial, insurance, credit, employment, housing, education-admission, immigration, law-enforcement or other decisions that significantly affect a person, or to operate safety-critical systems. You may not use the Service for fully automated decisions with legal or similarly significant effects on people.

4. Protecting the Service

You may not:

- probe, scan, attack, overload or disrupt the Service, or access it except through the interfaces and API we provide;
- bypass, disable or work around rate limits, spend limits, queues, fair-use limits, moderation, Model access rules or security measures, including by splitting requests,

rotating accounts, keys or IP addresses, or using prompt-injection or "jailbreak" techniques against our systems or moderation;

- create or use multiple accounts to obtain more free allowances, Neutrinos, rewards or promotions, or to evade a suspension;
- share, sell, rent or publish access to your account or keys, or resell access to Models through the Service without our written agreement;
- scrape the Service or harvest other users' data;
- reverse engineer, copy or replicate the Service, our routing or our pricing data, except to the extent the law allows despite this restriction;
- use the Service, or its output, to develop or train a model that competes with a Model you used, where that Model's terms prohibit it;
- misrepresent output as human-made where that would deceive people, or remove watermarks, labels or provenance information from output;
- use the Service in a way that makes us breach our agreements with Model Providers or payment providers, or the law.

5. Evading moderation

Trying to evade moderation, for example through obfuscation, misspellings, coded language, foreign-language substitution, splitting a prompt across requests or using the API to avoid checks in the app, is itself a serious breach, whether or not prohibited content is produced.

6. Security research

If you find a vulnerability, report it as described in Security & Disclosure. Do not access other users' data, degrade the Service, or disclose the issue publicly before we have had a reasonable chance to fix it.

7. Enforcement

We may monitor use of the Service for compliance with this Policy, including automated checks of image and video prompts and review of usage patterns. Where we reasonably believe this Policy has been broken, we may refuse or stop requests, remove content, limit features, revoke keys, suspend or close accounts, and report conduct to law enforcement. **If we become aware of apparent child sexual abuse material, including AI-generated**

material, we preserve it and report it to the National Center for Missing & Exploited Children or another competent authority as the law requires. If we close an account for a serious or repeated breach of this Policy, Terms Section 15.4 explains what happens to its Credits. You can appeal a decision as described in Terms Section 15.5.

8. Reporting misuse

To report content or conduct that breaks this Policy, email support@electronhub.ai with as much detail as you can, including the account, request ID or URL involved.