Acceptable Use Policy

Version 1.0.0 · Effective 5 November 2026 · EPIC AI Solutions Pty Ltd

These documents are being finalised and will be reviewed before payments open.

This Acceptable Use Policy sets out what you may not do with EPIC. It applies to everyone who uses our website, our API or the models we serve, including members of a pool. It forms part of our Terms and Conditions.

Illegal and harmful activity affects our whole community, so we take these rules seriously. When you create an account, you confirm that you are 18 or older and that you accept this policy.

1. Adults only

You must be at least 18 years old to create an account or use EPIC. You must not create an account for, or give access to, anyone under 18. If we learn that an account belongs to someone under 18, we will close it and delete its data.

2. Content that is never allowed

You must never use EPIC to create, request, store or share any of the following. There are no exceptions to these three rules:

- any sexual content involving a minor, whether depicted or described;
- sexual content depicting an identifiable real person who has not consented to it;
- working malicious software, or instructions for an attack, aimed at an identifiable third party, such as a named person, company, system or network address.

We report child sexual abuse material to the authorities where the law requires it, including to the National Center for Missing & Exploited Children (NCMEC) in the United States.

3. Other things you must not do

- Break any law that applies to you or to us, or help anyone else to do so.
- Infringe anyone’s intellectual property, privacy or other rights.
- Harass, threaten, defraud or impersonate other people.
- Try to get around our safety screening, rate limits or other protections, or hide the purpose of your requests to do so.
- Probe, scan or attack our systems, or test their security, except as our responsible disclosure rules allow.
- Disrupt the service for others, for example by flooding it with requests or sending deliberately malformed traffic.
- Access another person’s account, or try to reach data that is not yours.
- Share your password or API keys with anyone outside your own account and the pools you manage, or publish them.
- Sell, rent, sub-license or otherwise give your slots or access to third parties. A main user may share their slots with their own people through pools, as our Terms and Conditions describe.
- Use automated tools to copy content from our website, other than through our API as documented.

4. Legitimate work in sensitive areas

Some legitimate work, such as security research, red-team consulting, AI safety research or legal work on criminal matters, can look like misuse to an automated filter. An account owner can apply for an opt-out from automated screening, with a written business justification, a named contact and evidence of the legitimate purpose. We review each request by hand.

If we approve an opt-out, a small random sample of that account's requests is kept, encrypted, for a person on our team to check that the opt-out is used as described. An opt-out never permits the three kinds of content that are never allowed.

5. How we enforce this policy

To comply with the law and keep the community safe, we may screen requests automatically for the three kinds of content that are never allowed. A refused request returns an error naming only the category; we do not keep the prompt. We also act on reports from members and the public.

If we find a problem, our team will usually contact you first and guide you through what happens next. We only take further steps when it is necessary. Depending on how serious the problem is, we may:

- disable an API key automatically, for example after repeated refused requests from the same key within an hour;
- suspend an API key, an account or a pool, temporarily or permanently;
- block an account that is linked to three or more incidents, whether on its own or through a pool shared with someone who broke this policy;
- block the manager of a pool that collects too many reports;
- close an account, in serious cases without a refund, to the extent the law allows;
- report illegal activity to the police or other authorities where the law requires or allows it.

When we block an account for breaking this policy or our terms, its email address cannot be used for a new account, an invitation or an email change until we lift the block. This does not apply to people who simply left or deleted their own account.

Every enforcement action is recorded in our tamper-evident audit log.

6. Reporting abuse

If you see EPIC being used in a way that breaks this policy, please tell us at abuse@epic-ai.solutions or through the form at epic-ai.solutions/abuse. You do not need an account to report. We review every report, and we treat reports of harm to a child or an immediate risk to someone's safety as urgent.

7. Appeals

If you think we have made a mistake in acting against your account, an API key or your email address, write to abuse@epic-ai.solutions or support@epic-ai.solutions and explain why. A person on our team will review the decision and reply to you.

8. Changes to this policy

We may update this policy. When we do, we will publish the new version here with a new version number and tell members before the change takes effect. We may ask you to accept the new version before you continue to use your account.