



LEGAL · AGREEMENT

Acceptable Use Policy

SFER LABS LLC · Version 1.0 · Effective August 11, 2026

This Acceptable Use Policy ("AUP") is issued by SFER LABS LLC and applies to all use of Idelio, including Inputs, Outputs, API integrations and downstream applications. Examples are illustrative; conduct with substantially similar risk is also prohibited.

1. Law and rights

You may not use the Service to:

- a) violate law, sanctions, export controls, court orders or another person's contractual rights;
- b) infringe or misappropriate copyright, trademark, design, patent, trade secret, privacy, publicity or data-protection rights;
- c) submit content you do not have authority or lawful basis to process;
- d) scrape personal data unlawfully, bypass access controls or build dossiers about people from sensitive or private information; or
- e) remove legally required AI disclosures or provenance to deceive others.

2. Harm, exploitation and sexual content

You may not create, facilitate or distribute:

- a) child sexual abuse or exploitation material, grooming, sexualization of minors or any content involving a person who may be underage;
- b) non-consensual intimate imagery or sexualized depictions of an identifiable person;
- c) trafficking, coercion, credible threats, instructions to cause serious physical harm or targeted harassment;
- d) hateful or dehumanizing content targeting protected characteristics where intended or likely to facilitate discrimination or harm; or
- e) instructions materially enabling suicide, self-harm or dangerous acts, except appropriately framed prevention, education or support content.

3. Deception, impersonation and information integrity

You may not use the Service for:

- a) subliminal, manipulative or materially deceptive techniques, or exploitation of vulnerability due to age, disability or social or economic circumstances, in a manner intended or reasonably likely to cause significant harm;
- b) fraud, phishing, scams, fake documents, credential theft, identity theft or deceptive fundraising;
- c) impersonation likely to mislead, defame or harm a person or organization;
- d) deceptive deepfakes or synthetic media presented as authentic evidence, news or communication;
- e) undisclosed fake reviews, fabricated testimonials, astroturfing or manipulation of public metrics;
- f) targeted political persuasion or voter suppression using sensitive personal data, or materially deceptive election content; or
- g) false claims that Output was verified, cleared, unique, human-created or guaranteed by us.

Parody, satire, fiction and authorized brand work may be permitted when lawful, appropriately disclosed and unlikely to cause material deception or harm.

4. Privacy and biometrics

You may not use the Service to identify, track, surveil or infer sensitive characteristics about a person without a lawful basis and required consent. Prohibited uses include unapproved facial recognition, emotion recognition in restricted contexts, biometric categorization by sensitive traits, social scoring and mass collection of faces or voices.

5. High-impact decisions and professional domains

Unless we expressly approve the feature and written use case, you may not use the Service to make or materially support decisions determining a person's eligibility, selection, access or terms in:

- a) employment or worker management;
- b) credit, lending, insurance or financial services;
- c) housing or essential utilities;
- d) education admissions, assessment or discipline;
- e) healthcare diagnosis, treatment or access;
- f) legal services, law enforcement, migration or public benefits; or
- g) another area producing legal or similarly significant effects.

The Service may not replace a qualified professional or required human review.

6. Cybersecurity and platform integrity

You may not:

- a) generate, deploy or meaningfully facilitate malware, ransomware, destructive payloads or unauthorized intrusion;
- b) evade safety systems, probe for protected prompts, extract model weights or use automated methods to reproduce the Service;
- c) overload, disrupt or interfere with the Service or another system;
- d) resell, sublicense or expose an API except under an authorized plan;
- e) use Output or access to build a competing model or service where prohibited by applicable provider terms communicated for the feature; or
- f) conceal abusive activity through coordinated accounts or manipulated telemetry.

Good-faith, authorized security research must follow any published vulnerability-disclosure rules.

7. Weapons and severe harm

You may not use the Service to develop or deploy weapons, weapons of mass destruction, or systems designed to select and engage targets without meaningful human control; to facilitate trafficking in controlled substances; or to materially enable other severe unlawful harm.

8. Enforcement

We may use automated signals and proportionate human review to detect violations. Depending on severity, history and legal requirements, we may warn, block requests or Output, reduce functionality, suspend or terminate an account, preserve evidence, notify an organization administrator, remove public material or report to authorities.

We may act immediately where needed to prevent harm or comply with law. A restriction is not a determination that content is unlawful. Appeals may be submitted to support@idelio.pro. We may request enough information to investigate while minimizing additional personal data.

9. Reporting

Report suspected violations, infringement or urgent safety concerns to support@idelio.pro. For an IP complaint, identify the protected work/right, relevant Output or location, your authority, the requested action and a good-faith statement that the use is unauthorized. We may forward the complaint to the affected user where appropriate and lawful.