

Acceptable Use Policy

DRAFT FOR REVIEW - NOT YET ADOPTED

Effective date remains pending. Publishing this copy does not establish acceptance.

Draft updated October 1, 2026. Effective date: pending adoption with the Terms of Service.

Scope

This policy covers Whumpo instructions, uploads, generated work, hosted websites and applications, and use of Digifender LLC's infrastructure. It applies to free and paid use alike. Buying capacity or credits never authorizes prohibited content. The Terms of Service describe account eligibility and the private preview.

Prohibited content and activity

- Illegal activity, child sexual exploitation or child sexual abuse material, including attempts to create, obtain or distribute it.
- Sexual content of any kind, including pornography, sexual services and nonconsensual intimate imagery. Whumpo has no adult-content exception.
- Copyright piracy and other infringement, including unauthorized streaming, download or distribution services. Lawful original, licensed and public-domain media are not automatically piracy.
- Fraud, scams, phishing, credential theft, impersonation intended to deceive, deceptive clicks and click fraud.
- Hate directed at protected groups, targeted harassment, credible threats, doxxing or abuse of another person's privacy or safety.
- Gambling services, wagering, betting and casinos, including activities that may be permitted in some jurisdictions.
- Malware, unauthorized access, destructive attacks, or unauthorized interference with systems or data. Do not evade tenant isolation, authorization reviews, quotas, security controls or content holds, or help someone else do so.
- Abusive automated traffic, spam, or use of shared infrastructure that intentionally disrupts service for others. Do not resell access, run unauthorized scanning against others, or use stolen credentials or accounts.

Graphic violence alone is not a blanket prohibited category. Threats, targeted abuse, exploitation and unlawful material remain prohibited. Good-faith reporting, prevention, removal and lawful security education are not themselves violations, but do not upload prohibited material as evidence. Describe the issue and provide the relevant URL or identifier instead.

Responsibilities for data and publication

Use only content and data you have authority to process, and respect intellectual-property, privacy and publicity rights. Review generated material before publication. Do not use the private preview for emergency or safety-critical systems or for collecting sensitive regulated information that the Service is not equipped or contracted to handle. The current AI testing route is limited to non-sensitive test material; see the Privacy Policy.

Customer websites must present accurate business information and appropriate visitor notices. Our platform policy is not a substitute for your own visitor terms, privacy notice or lawful basis for collection.

Enforcement and review

We may hold an upload, refuse an action, restrict or remove content, suspend access or terminate an account when reasonably necessary to enforce this policy, meet legal obligations or protect people and systems. Some protections are implemented as holds pending review; this is not a claim that every upload or message has been scanned. An automated flag, failed test or model refusal is not proof that a person committed a violation or crime.

We seek to keep action proportionate to the issue and provide notice and a chance to correct mistakes when lawful and safe. We may act immediately where necessary. Ask for human review at legal@digifender.com, identifying the account, content or action and why you believe the decision was mistaken. Do not attach illegal or intimate material. Nothing in this policy promises a response time that the preview cannot support.

Reporting abuse

Send a URL, a concise description and a safe way to contact you to legal@digifender.com. For copyright notices and counter-notices, use the Copyright and Abuse Policy. We may preserve or disclose information where legally required and coordinate with appropriate authorities. Do not use email reports as an emergency channel; contact appropriate emergency services for an imminent threat.