

Black Forest Labs — Usage Policy

Snapshot retrieved on 16 October 2026 from <https://bfl.ai/legal/usage-policy> for reference. The official page remains authoritative and may change over time.

Usage Policy

Last Revised on August 4, 2026

Black Forest Labs is committed to ensuring the secure use of our frontier AI models (“FLUX Models”) and our products and services (“Services”). This Usage Policy (“Policy”) supplements the Black Forest Labs Terms of Use (“Terms of Use”) and Developer Terms of Service, and applies to your access and use of our FLUX AI Models and Service, including any inputs (“Input”) you provide, outputs you create (“Output”) or any actions or results from the FLUX Models or Services undertaken on your behalf (“Tasks”). It also applies to your use within and outside our Website and our Services, whether directly or indirectly, as well as any attempts to use our Website and Services. If you access or use any FLUX AI Models, any adaptations for, or modified versions of the FLUX AI Models, or the Services, you agree to this Policy. Any restrictions in this Policy covering the FLUX AI Models also apply to derivatives of the FLUX AI Models. Capitalized but undefined terms in this Policy have the meanings set forth in the Developer Terms of Service.

You agree you will not use, or allow others to use, the FLUX Models or our Services, including Output or any Task to:

- realistically depict a real person in a sexual, intimate, degrading, defamatory, fraudulent, misleading, or otherwise abusive manner without their verified, documented, and informed consent.

- generate unlawful content, including child sexual abuse material or non-consensual intimate imagery, or any content depicting minors in any sexual, violent, obscene, or otherwise harmful manner, or any content to promote or facilitate the exploitation or harm of minors in any way.

- generate disinformation or content, including realistic content featuring real people, intended to, or likely to, mislead voters or for the purpose of political campaigning, electoral advertising, or voter suppression.

- generate content that falsely represents events, things or people in a manner likely to deceive a reasonable viewer without appropriate or lawful disclosures.

- circumvent, remove, alter, suppress, or otherwise interfere with any C2PA Credentials, digital watermarks, or other content provenance signals attached to, embedded in, or otherwise associated with Outputs, or develop or distribute any tool designed to facilitate such interference.

- to harass, abuse, threaten, stalk, defame or bully others.

- for any military, surveillance or law enforcement purpose, or for inferring sensitive information about a person or biometric processing purposes, including use in a high risk AI system, as defined by applicable law.

- engage in unlawful impersonation, including unlawful use of a real person’s name, image, voice and/or likeness or to generate, discover, or disseminate personal information in violation of a person’s privacy rights.

- to gain unlawful access to, disrupt, or impair the use or availability of the Services or FLUX Models.

- for fully automated decision making that adversely impacts an individual's legal rights or otherwise creates or modifies a binding, enforceable obligation.

to violate, circumvent, duplicate, decompile, reverse engineer, disassemble or decode the security, integrity, or availability of any computer or communications system, user, network, software application or program, computing device or other resource, including the FLUX Models and Services, for unlawful or commercial purposes.

to engage in, promote, incite, or facilitate unlawful discrimination or other unlawful conduct in the provision of employment, employment benefits, financial services, housing, education, or other essential goods and services.

create, use or distribute output in a fraudulent or misleading way.

to generate, edit, store, or transmit any content that infringes, misappropriates, or otherwise violates any third-party rights, including intellectual property rights.

You understand and accept that, given the probabilistic nature of artificial intelligence technologies, the use of the Services may in some situations lead to erroneous results that do not accurately reflect the desired output. It is therefore your responsibility to evaluate the usability and suitability of any Output or Task on a case-by-case basis, in particular by human review of any Output or Task.

You understand that an Output may not be unique compared to (i) other users' output and (ii) existing content. You must therefore ensure that your generation, publication, and distribution of Outputs complies with applicable intellectual property law.

In addition, for users or organizations based in or established in the European Union: you cannot use, change, modify, or develop the Services in a way that would turn them into a "high-risk AI system" under the EU AI Act (Regulation (EU) 2024/1689). For users or organizations located in the European Union: you must not use the Services for any AI practices that are prohibited under the EU AI Act (Regulation (EU) 2024/1689), including but not limited to:

- use subtle, manipulative, or deceptive techniques to influence people's behavior in ways that prevent them from making informed decisions and could cause harm,
- take advantage of people's vulnerabilities related to age, disability, or social situation,
- create or expand facial recognition databases without consent,
- use real-time remote biometric identification in public spaces for law enforcement,
- rate or classify people based on their social behavior or personal characteristics (including social scoring or predictive profiling) leading to unfair treatment,
- assess or predict whether someone might commit a crime based solely on their personal characteristics or profiling,
- assess an people's emotions at work or in schools, unless it's needed for medical or safety reasons,
- integrates the Services into an AI System that generates or manipulates child sexual abuse material (CSAM) or realistic images, videos, audio or similar material of a person's intimate parts, or of a person engaged in sexually explicit activities, without that person's freely-given, specific, informed, unambiguous and explicit consent for that generation or manipulation;
- and/or
- categorize individuals based on their biometric data to figure out or infer sensitive information such as their race, political opinions, religious beliefs, or sexual orientation.

Please report any violations of this Policy or any potential issues that could result in a violation of this Policy to legal@blackforestlabs.ai.