

Acceptable Use Policy

Last Updated: June 1, 2026

1. *Purpose and Scope*

Decart.ai Inc. (“Decart” or “we”, “us”, “ours”) is committed to promote safe and fair use of its tools, apps, platforms, offers, features, models, model weights, and API (collectively “Offers”). This AUP governs the use of all Offers provided by Decart. By accessing or using the Offers, you agree to this AUP in addition to any applicable license, terms of service, and any requirements and regulations under applicable laws and regulations. The AUP is designed to ensure a safe and responsible online environment, to protect individuals and users right, to uphold applicable legal obligations, including without limitations the EU Digital Service Act (“DSA”), the EU AI Act (“AIA”), Digital Millennium Copyright Act (“DMCA”) and any other applicable regulatory requirements. We take our ethical responsibilities very seriously and have implemented robust safeguards to enhance our safety standards.

2. *Applicability*

This AUP applies to business, users, consumers, developers, integrators, resellers, authorities, individuals, organizations (all collectively hereinunder “you”, “your”) making use of the Offers, whether free, paid or other type of usage, for any purpose. Violations may result in warnings, suspension, termination, model, key revocation, legal action, and reporting to authorities. You may be liable for damages and costs.

If you redistribute models, code, or products implementing Decart models or API (including under the community license or open source, to the extent applicable): Include this AUP (or materially equivalent terms) and any license files; prevent use in prohibited contexts where reasonably possible (e.g., usage warnings, filters, or gating); and clearly label modified versions and do not misrepresent them as official Decart releases subject to the attribution clauses applicable to the license terms governing your use of the Offers.

3. *Prohibited Uses & Activities*

You may not use the Offers:

- In violation of the law, regulations, or other party's right, or for any illegal activity, violation of court orders, evasion of sanctions or export controls.
- In a manner that infringes, misappropriates, or violates the intellectual property rights or trade secrets of a third party.
- In a manner that contributes, endorses, or promotes, illegal content (including as such term is defined under DSA and applicable laws) including, without limitations, content that:
 - Incites, facilitates, or promotes terrorism or violent extremism, or that provides material support for organizations or individuals associated with terrorism, violent extremism, or hateful behavior
 - Depicts, describes, promotes, or facilitates sexual abuse, suggestive content involving minors, sexual violence, non-consensual intimate imagery, or human trafficking
 - Hate speech, bullying, discrimination, or content that promotes discriminatory practices against individuals or groups on the basis of one or more protected characteristics, such as race, ethnicity, religion, national origin, gender, sexual orientation, or any other identifying trait
 - Content that facilitates, incites or threatens violence,
 - Creates instructions to harm self or others,
 - Infringes intellectual property rights
 -

The aforesaid shall include content provided as inputs and generated as outputs or results of the Offers.

- To collect, process, disclose, generate, or infer private or sensitive information about individuals, including information about individuals' identity, health, or demographic information, unless you have obtained the right to do so in accordance with applicable law.
- To create, generate, or facilitate the creation of malicious code, malware, computer viruses or do anything else that could disable, overburden, interfere with or impair the proper working, integrity, operation or appearance of a website or computer system. Including by engaging in actions that circumvent or remove usage restrictions or other safety measures.

- To deceive or manipulate by creating deepfakes, media that impersonate a real person without clear, conspicuous disclosure and verifiable consent from the person (or their authorized agent), create, including through prompts and outputs or results of the Offers, misinformation, spam, or content presented as authentic news, evidence, or reportage among others. This provision includes generating or facilitating false online engagement, including fake reviews and other means of fake online engagement through use of the Offers, including by outputs.
- For military, warfare, nuclear industries or applications, espionage, use for materials or activities that are subject to the International Traffic Arms Regulations (ITAR) maintained by the United States Department of State or to the U.S. Biological Weapons Anti-Terrorism Act of 1989 or the Chemical Weapons Convention Implementation Act of 1997.

4. *Principles to Prevent Child Sexual Abuse*

We have made efforts to prevent misuse of the generative AI technology for sexual harms against children, therefore we prohibit harm or exploitation against children:

- Maintain model and platform safety by continuing to understand and respond to child safety risks, if we receive a report regarding misuse of the Offers or Content containing child sexual abuse material (“CSAM”) or child sexual exploitation material (“CSEM”) we will remove such content and if required by law, report to the authorities.
- We urge you to report CSAM and CSEM Content
- Users are strictly prohibited from using our Offers to:
 - Create, distribute, or promote CSAM or CSEM, including AI-generated CSAM and CSEM
 - Facilitate trafficking, sextortion, or any other form of exploitation of a minor.
 - Facilitate grooming of a minor.
 - Facilitate child abuse in any form, including instructions about how to conceal abuse.
 - Promote or facilitate pedophilic relationships.
 - Fetishize or sexualize minors in any way.

- By defining specific training data and model development policies, we make best efforts to ensure training data does not contain CSAM or CSEM, if detected it is immediately removed, we expect you to act in the same ethics and responsibilities.

Any CSAM solicitation reported will be treated seriously – we reserve the right to terminate your use of the Offers and the right to report to the appropriate authorities upon becoming aware of such solicitation.

5. *Specific AIA Prohibitions*

- The following uses and activities are strictly prohibited: Using the Offers for medical diagnosis, treatment, autonomous weapons, surveillance, or any use where failure could cause death, severe injury, or significant property or environmental damage.
- Engage in, promote, incite, facilitate, or assist in the planning or development of activities that present a risk of death or bodily harm to individuals.
- Untargeted scraping of facial images or real-time remote biometric identification in publicly accessible spaces for law enforcement.
- Evaluating or classifying people based on their social behavior, personal characteristics, or the use of social scoring leading to detrimental or unfavorable treatment
- Inferring emotions of individuals in areas of workplace and education institutions, except where strictly for duly authorised medical or safety reasons.
- Making risk assessments of individuals in order to assess or predict the risk of committing a criminal offence, based solely on the profiling or personality traits and characteristics.
- Exploiting the Offers to deploy subliminal, manipulative or deceptive techniques with the objective of materially distorting the behaviour of individuals or a group of individuals by appreciably impairing their ability to make an informed decision.

The following high-risk uses and activities are prohibited unless otherwise agreed between Decart and you, and only where you can demonstrate full compliance with applicable law:

- Using the Offers to compromise the privacy of others, including the use for biometric categorization, emotion recognition and as a biometric identification system.
- Determining access and admission, evaluating learning outcomes or monitoring and detecting prohibited behavior during tests.
- Making sensitive decisions in the context of employment including the recruitment and selection of individuals and any other decisions affecting terms of work-related relationships such as promotion, termination or work-allocation.
- Making sensitive decisions impacting an individual's enjoyment of essential public and private services and benefits, such as eligibility for public assistance, creditworthiness assessments or assessments concerning the pricing of life and health insurance.
- Using the Offers for law enforcement purposes, as part of critical infrastructure, for migration, asylum and border control management or for the administration of justice and democratic processes.

6. *Transparency and Disclosure*

When using the Decart model:

- You shall disclose content that has been generated or manipulated by AI, as required by law.
- You shall disclose content that constitutes a deepfake - i.e. AI-generated or AI-manipulated image, audio or video content that appreciably resembles real persons, objects, places, entities or events and would falsely appear authentic or truthful - as generated or manipulated by AI, as required by law.
- You shall disclose text which is published with the purpose of informing the public on matters of public interest (e.g. political, social, economic, health, or safety issues) that has been generated or manipulated by AI, as required by law.
- Where the output is marked in a machine-readable format (including watermarks or metadata), you shall not remove, obfuscate, alter, or interfere with such marks unless.

- Maintain internal processes to identify when your use of the Decart model triggers disclosure obligations and to apply appropriate labelling consistently.
- You shall implement content moderation appropriate to your product and audience, including reporting mechanism for prohibited content, human review for edge cases, and age gates where appropriate
- If you distribute outputs, preserve metadata where technically feasible and legally permissible and ensure that downstream distribution channels do not strip such metadata by default.

7. *Safety and Responsible AI Practices*

If we detect that you have violated this AUP, we reserve the right to throttle, suspend, or terminate your use of the Offers, remove any content you publish and to the extent applicable, report to authorities and legal enforcements.

8. *Reporting and Appeals*

- Report suspected violations or safety issues to: security@decart.ai please include relevant ID, timestamps, and sample requests, responses or any additional information that is needed for us to manage this issue.
- Content moderation, if you are not able to report directly from the social feed, image, video, output or app, please submit a report to dsa@decart.ai. Decart reserves the right to remove any infringing and misleading content or terminate the use or account of any user using the Offers in breach of applicable laws and this AUP.
- Copyright Infringement and Intellectual Property Infringement shall be reported separately as stated herein below.
- Authority and Government Reporting shall be submitted here: security@decart.ai
- Appeals If we believe there has been a policy violation, we may remove the content, warn, suspend or terminate the specific user account. If you believe we made a mistake, please submit an appeal at appeal@decart.ai specifying the reason you are appealing and adding supporting documentation and evidence.

9. *Copyright Reporting Specifications*

- a. Removal of Content. Decart respects the legitimate rights of copyright owners, and we will respond to clear notices of alleged copyright infringement. Pursuant to the Digital Millennium Copyright Act (“DMCA”), we have designated a Copyright Agent (as specified below) to receive notifications of claimed copyright infringement in connection with the Offers. Please be advised that we enforce a policy that provides for the termination of inappropriate circumstances of users who are repeat infringers. If you believe that your work has been copied in a way that constitutes copyright infringement, please provide the Copyright Agent with the following information in accordance with the DMCA:
 1. An electronic or physical signature of the person authorized to act on behalf of the owner of the copyright.
 2. A description of the copyrighted work you claim has been infringed.
 3. A description of where the material that you claim is infringing is located on the Platform, with enough detail that we may find it. Providing URLs or images in the body of an email is the best way to help us locate content quickly.
 4. Your address, telephone number, and email address;
 5. A statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law.
 6. A statement by you, made under penalty of perjury, that the above information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner’s behalf.

- b. Counter-Notification. If you believe that the material you posted was removed from the Platform by mistake and that you have the right to post the material, you may elect to send us a counter-notification. To be effective the counter-notification must be a written communication provided to our Copyright Agent that includes substantially the following (please consult your legal counsel or see the DMCA to confirm these requirements):
 1. Your physical or electronic signature.
 2. Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled. Providing URLs or images in the body of an email is the best way to help us locate content quickly.

3. A statement under penalty of perjury that you have a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled.
 4. Your name, address, and telephone number, and a statement that you consent to the jurisdiction of the Federal District Court for the judicial district in which the address is located, or if your address is outside of the United States, for any judicial district in which the Platform may be found or accessed, and that you will accept service of process from the person who provided notification of infringement or an agent of such person.
- c. Misrepresentations. Please note that under the DMCA (at 17 U.S.C. Section 512(f)) any person who knowingly materially misrepresents that material or activity is infringing or was removed or disabled by mistake or misidentification may be subject to liability.
- d. Copyright Agent. Our agent for notice of claims of copyright infringement (“Copyright Agent”) can be reached as follows: Copyright Compliance Department Email: info@decart.ai. Address: 1007 North Orange Street, 10th Floor; Wilmington, DE 19801, USA.

10. *Changes*

We reserve the right to change and update this AUP, the effective date shall be stated above under the “Last Update” publication date. Your use of the Offers is subject to this AUP. If material prohibitions are made, we will provide notice through accounts, website or apps, solely to the extent applicable, otherwise, any changes are enforceable from the date published herein.