

Acceptable Use Policy

Vizbl Systems, Inc.

Effective Date: August 4, 2026 | Last Updated: August 4, 2026

This Acceptable Use Policy ("Policy") governs use of the Vizbl Platform and forms part of the Vizbl Terms of Use, any applicable Master Services Agreement, Platform & Developer Services Agreement, Order Form, and other agreement that incorporates this Policy. Capitalized terms not defined here have the meanings given in the applicable agreement.

This Policy applies to Customers, Developers, Authorized Users, End Users, content contributors, catalog participants, and any person who accesses or uses the Platform. You are responsible for ensuring that persons using the Platform through your account, credentials, applications, websites, integrations, devices, or organization comply with this Policy.

The examples below are illustrative and not exhaustive. Conduct may be prohibited where Vizbl reasonably determines, based on objective and documented considerations, that it creates material legal, security, safety, privacy, operational, intellectual-property, fraud, abuse, or third-party risk, even if the conduct is not specifically listed. Vizbl will not enforce this Policy solely to suppress lawful competition, protected speech, fair comment, or truthful criticism.

Contents

1. Core Rule
2. Illegal, Harmful, and Abusive Conduct
3. Child Safety and Exploitation
4. Sexual Content and Non-Consensual Imagery
5. Hate, Harassment, Violence, and Dangerous Activity
6. Fraud, Deception, Impersonation, and Manipulation
7. Intellectual Property, Confidentiality, and Rights of Others
8. Privacy, Personal Data, Biometrics, and Surveillance
9. Platform Security and Technical Abuse
10. API, SDK, Integration, and Infrastructure Abuse
11. Artificial Intelligence, Computer Vision, AR, and Generated Content
12. Products, Commerce, Advertising, and Regulated Activities
13. Spam, Messaging, and Unsolicited Communications
14. Public Catalog, Reviews, Ratings, and User Contributions
15. Minors and Images of Individuals
16. Export Controls, Sanctions, and Restricted Use
17. Enforcement and Cooperation
18. Reporting Violations
19. Changes and Conflicts

1. Core Rule

You may use the Platform only for lawful, authorized, bona fide business, commercial, creative, visualization, development, catalog, marketing, sales, or evaluation purposes consistent with the applicable agreement, Documentation, and this Policy. You must not use, attempt to use, facilitate use of, or permit use of the Platform in a manner that:

- violates applicable law, regulation, court order, binding governmental requirement, or the legal rights of any person;
- is fraudulent, deceptive, abusive, harmful, exploitative, unsafe, or materially misleading;
- interferes with the Platform, Vizbl, other customers, End Users, or Third-Party Services;
- accesses data, systems, accounts, features, or functionality without authorization;
- circumvents contractual, technical, security, safety, billing, usage, moderation, or access restrictions; or
- causes Vizbl or any third party to violate law or incur material legal, security, safety, privacy, operational, or intellectual-property risk.

Nothing in this Policy prohibits lawful competition, interoperability, security research expressly authorized in writing by Vizbl, truthful comparative advertising, or honest reviews and opinions protected by applicable law. Criticism of Vizbl, including a truthful negative review, is not prohibited merely because it may affect Vizbl's reputation.

2. Illegal, Harmful, and Abusive Conduct

You must not use the Platform to create, upload, host, transmit, publish, display, promote, sell, facilitate, or otherwise engage with content, products, services, or conduct that:

- is unlawful or promotes, solicits, instructs, facilitates, or conceals unlawful activity;
- is defamatory, threatening, extortionate, coercive, malicious, or knowingly false in a manner likely to cause harm;
- facilitates trafficking, exploitation, abuse, stalking, doxxing, blackmail, coercive control, or targeted harassment;
- promotes cruelty to persons or animals, except lawful documentary, educational, journalistic, scientific, or public-interest material presented with appropriate context;
- involves stolen goods, counterfeit goods, fraudulent documents, unlawful services, or evasion of legal requirements;
- is designed to cause physical injury, property damage, panic, or unlawful disruption; or
- otherwise exposes persons, property, systems, or the public to a material and unreasonable risk of harm.

3. Child Safety and Exploitation

The Platform may not be used for any child sexual abuse material, sexual exploitation of minors, grooming, solicitation of minors for sexual purposes, trafficking, sextortion, or any content or conduct that sexualizes, endangers, exploits, or abuses a minor. This prohibition applies to real, fictional, synthetic,

AI-generated, altered, animated, or photorealistic material.

You must not use the Platform to facilitate harmful challenges, predatory contact, concealment of abuse, or collection or sharing of personal information about a minor without lawful authority and required consent. Vizbl may preserve and report apparent child-exploitation material or conduct to competent authorities and legally authorized reporting organizations.

4. Sexual Content and Non-Consensual Imagery

You must not use the Platform to create, upload, host, transmit, publish, display, promote, sell, facilitate, or otherwise engage with:

- non-consensual intimate imagery, sexual deepfakes, voyeuristic content, or sexual content created or shared without the depicted person's valid consent;
- content depicting sexual violence, exploitation, coercion, trafficking, or incest;
- pornographic or sexually explicit content where prohibited by law, the applicable agreement, app-store rules, payment-provider rules, or Vizbl product requirements;
- sexual services or products where prohibited by the Vizbl Prohibited Products Policy or applicable law; or
- content that falsely represents a person as participating in sexual conduct.

5. Hate, Harassment, Violence, and Dangerous Activity

You must not use the Platform to create, upload, host, transmit, publish, display, promote, facilitate, or materially support content or conduct that:

- promotes hatred, dehumanization, exclusion, or discrimination based on race, color, ethnicity, national origin, religion, caste, sex, gender, gender identity, sexual orientation, disability, age, veteran status, or another legally protected characteristic;
- praises, supports, recruits for, or materially assists terrorist, violent extremist, or criminal organizations;
- makes credible threats, incites violence, glorifies mass violence, or provides operational assistance for violent wrongdoing;
- facilitates suicide or self-harm, including targeted encouragement, instructions, or concealment; or
- enables the design, procurement, production, concealment, or use of weapons, explosives, chemical or biological agents, or other dangerous materials in violation of law or the applicable agreement.

6. Fraud, Deception, Impersonation, and Manipulation

You must not use the Platform in a manner that:

- impersonates a person, company, brand, public authority, or Vizbl, or falsely suggests sponsorship, certification, endorsement, affiliation, or approval;
- uses deceptive identifiers, domains, metadata, headers, caller information, accounts, reviews, ratings, product listings, images, or AR experiences;

- facilitates phishing, credential theft, account takeover, payment fraud, chargeback abuse, investment fraud, fake offers, counterfeit documentation, or identity fraud;
- misrepresents Generated Outputs, simulated environments, edited images, virtual try-on results, fitment, scale, product characteristics, safety, certifications, availability, pricing, or performance as verified fact;
- uses synthetic or altered media to deceive a person about a material fact or to interfere unlawfully with civic, judicial, regulatory, financial, or commercial processes; or
- manipulates platform metrics, attribution, traffic, engagement, ratings, reviews, conversions, usage, billing, quotas, or reporting.

7. Intellectual Property, Confidentiality, and Rights of Others

You must not use the Platform in a manner that:

- infringes, misappropriates, or violates copyrights, patents, trademarks, trade dress, trade secrets, database rights, moral rights, publicity rights, privacy rights, contractual rights, or other proprietary rights;
- uploads or processes confidential, restricted, embargoed, export-controlled, or non-public information without authorization;
- removes, obscures, alters, or bypasses copyright, trademark, watermark, attribution, rights-management, provenance, or proprietary notices;
- copies, republishes, distributes, sells, leases, sublicenses, or commercially exploits Platform content or Developer Tools except as expressly authorized;
- uses Vizbl names, marks, designs, interfaces, screenshots, or branding in a manner likely to cause confusion or imply approval without written authorization; or
- uses Customer Content, Vizbl outputs, Platform data, or third-party content to train, benchmark, fine-tune, validate, or improve a competing AI, AR, 3D, visualization, product-imaging, or asset-generation system except where expressly authorized in writing.

8. Privacy, Personal Data, Biometrics, and Surveillance

You must not use the Platform to collect, process, infer, combine, retain, disclose, or otherwise handle data in a manner that:

- collects, uses, combines, infers, stores, transmits, sells, shares, or discloses personal data without a valid legal basis, required notice, and required consent;
- collects or processes precise location, face, body, hand, voice, vehicle, room, device, camera, sensor, biometric, health, financial, government-identifier, or other sensitive data in violation of law or the applicable agreement;
- conducts covert, unlawful, discriminatory, or unauthorized surveillance, profiling, facial recognition, identity matching, emotion inference, or tracking;
- re-identifies or attempts to re-identify de-identified, anonymized, aggregated, or pseudonymized information;
- scrapes, harvests, purchases, combines, or enriches personal data for spam, stalking, discrimination,

fraud, or unlawful targeting;

- publishes personal contact information, credentials, government identifiers, financial information, private communications, or sensitive images without lawful authority; or
- fails to provide required privacy notices, consent mechanisms, app-store disclosures, retention controls, deletion mechanisms, or data-subject rights.

9. Platform Security and Technical Abuse

You must not attempt to or enable any third party to:

Except to the extent expressly permitted by non-waivable law or authorized in writing by Vizbl, you must not:

- access or attempt to access accounts, credentials, systems, source code, models, prompts, keys, tokens, networks, databases, or data that you are not authorized to access;
- probe, scan, test, monitor, intercept, decode, packet-capture, benchmark, or assess the vulnerability, security, availability, or performance of the Platform;
- bypass authentication, authorization, rate limits, quotas, geofencing, moderation, safety filters, watermarks, billing controls, usage controls, digital-rights controls, or other restrictions;
- reverse engineer, decompile, disassemble, translate, derive source code from, or discover underlying models, algorithms, architecture, prompts, data, or non-public functionality;
- introduce malware, ransomware, spyware, viruses, worms, logic bombs, malicious scripts, harmful code, corrupted files, or other destructive components;
- conduct denial-of-service activity, resource exhaustion, traffic flooding, credential stuffing, password spraying, cryptomining, or conduct that imposes an unreasonable or disproportionate load;
- spoof headers, manipulate routing or identifiers, conceal the origin of traffic or messages, or evade security controls; or
- interfere with, damage, disrupt, degrade, disable, or impair the Platform or any connected system.

10. API, SDK, Integration, and Infrastructure Abuse

When using APIs, SDKs, webhooks, integrations, embeds, plugins, credentials, or other Developer Services, you must not:

- use APIs, SDKs, webhooks, embeds, plugins, tokens, credentials, or integrations outside approved Customer Applications, domains, bundle identifiers, package names, environments, use cases, or distribution channels;
- expose, publish, share, transfer, lease, resell, sublicense, or embed credentials or Developer Tools in a manner that enables unauthorized third-party use;
- operate the Developer Services as a standalone product, service bureau, proxy, gateway, infrastructure service, white-label platform, OEM service, or reseller offering except as expressly authorized in an Order Form;
- cache, store, copy, extract, reproduce, or retain Platform data or outputs beyond documented or contractually permitted periods;

- use automated means to scrape, index, crawl, harvest, bulk-download, mirror, or reconstruct the Platform or its data except through expressly authorized interfaces;
- create excessive, duplicative, abusive, fraudulent, or artificial requests, accounts, views, generations, downloads, or events;
- circumvent metering, underreport usage, manipulate identifiers, rotate accounts or credentials to evade limits, or avoid fees; or
- use unsupported, deprecated, modified, tampered, or security-vulnerable versions after Vizbl requires migration or update.

11. Artificial Intelligence, Computer Vision, AR, and Generated Content

When using AI, machine-learning, computer-vision, AR, 3D, virtual try-on, AutoFit, or other automated features, you must not:

- generate, edit, transform, visualize, or distribute unlawful, infringing, deceptive, exploitative, or harmful content;
- create deepfakes, impersonations, fabricated evidence, counterfeit documents, deceptive product imagery, fake reviews, or misleading demonstrations without appropriate authorization, labeling, and context;
- use Generated Outputs as the sole or determinative basis for medical diagnosis or treatment, legal advice, engineering, architecture, construction, manufacturing, emergency response, employment, housing, credit, insurance, education admissions, or other high-risk decisions without qualified human review, legally required notices, meaningful safeguards, and all required approvals;

Customer may not use the Platform or Generated Outputs for weapon targeting, autonomous weapons operation, unlawful surveillance, or any other prohibited military, intelligence, or human-rights-abusive purpose;

- rely on AR, 3D, virtual try-on, AutoFit, placement, measurement, fitment, material, color, scale, or Generated Outputs as guaranteed real-world specifications;
- attempt to defeat safety filters, moderation, provenance, watermarks, content controls, or model restrictions;
- use the Platform for unlawful biometric identification, prohibited emotion recognition, discriminatory profiling, or automated decisions with legal or similarly significant effects where prohibited or without required safeguards; or
- represent AI or automated output as human-created, verified, certified, professionally approved, or uniquely owned where that representation is false or misleading.

12. Products, Commerce, Advertising, and Regulated Activities

You must comply with the Vizbl Prohibited Products Policy and all laws governing the products, services, claims, audiences, jurisdictions, and transactions involved. You must not use the Platform to advertise, visualize, list, promote, sell, or facilitate:

- illegal, stolen, counterfeit, recalled, unsafe, unauthorized, or fraudulently labeled products;

- weapons, explosives, controlled substances, prescription drugs, regulated health products, alcohol, nicotine, gambling, financial products, adult services, or other regulated goods or services except where expressly permitted by Vizbl and lawful in every applicable jurisdiction;
- products or services subject to sanctions, export restrictions, licensing requirements, age restrictions, or professional requirements without required authorization and controls;
- false, unsubstantiated, deceptive, or unfair advertising claims, including claims about price, availability, discount, origin, performance, environmental benefit, safety, fitment, certification, warranty, or results; or
- commerce that avoids taxes, consumer-protection requirements, product-safety requirements, disclosures, age verification, seller identification, or other legal obligations.

13. Spam, Messaging, and Unsolicited Communications

You must not use the Platform, Customer Applications, Platform data, or any integration to:

- send unsolicited bulk messages, spam, chain letters, pyramid schemes, phishing messages, or fraudulent solicitations;
- use false or misleading sender information, routing information, subject lines, identities, domains, or reply-to details;
- harvest addresses, use dictionary attacks, purchase unlawfully obtained lists, or contact persons who have not been lawfully acquired or who have opted out;
- fail to provide legally required sender identification, physical address, advertising disclosures, or a clear and effective unsubscribe mechanism;
- fail to honor opt-out, suppression, consent-withdrawal, or do-not-contact requests within legally required periods; or
- use Vizbl, Customer Applications, or Platform data to facilitate unlawful telemarketing, automated calls, text messages, direct messages, or commercial communications.

14. Public Catalog, Reviews, Ratings, and User Contributions

You must not use public-catalog, review, rating, comment, board, save, like, referral, or other contribution features to:

- submit fake, fabricated, purchased, coordinated, incentivized-but-undisclosed, or otherwise misleading reviews, ratings, likes, saves, comments, or engagement;
- review a product, seller, or service without genuine experience where genuine experience is represented or required;
- suppress, threaten, penalize, or retaliate against a person for an honest review or opinion protected by law;
- manipulate ranking, discovery, moderation, referrals, attribution, or recommendation systems;
- post content unrelated to the applicable product or service, repetitive content, undisclosed advertising, or promotional spam; or
- use reviews or contributions to harass, dox, defame, impersonate, or disclose confidential or personal information.

Vizbl may label, rank, moderate, limit, remove, or decline to publish contributions consistent with the applicable agreement and law. This Policy does not prohibit honest negative feedback, fair comment, or truthful statements about Vizbl, a Customer, or a third party.

15. Minors and Images of Individuals

You must not use the Platform to:

- upload, process, publish, or use an identifiable person's image, likeness, voice, body, face, hand, personal information, or location without all rights, notices, permissions, and consents required by law;
- use an image of a minor without authorization from the minor's parent or legal guardian where required;
- collect personal data directly from children in violation of applicable child-privacy law or without required parental consent;
- create or distribute content that exposes a minor to exploitation, unwanted contact, targeting, embarrassment, or foreseeable harm; or
- use camera-based or virtual try-on features in schools, healthcare, employment, housing, credit, insurance, or other sensitive contexts without required safeguards and written authorization.

16. Export Controls, Sanctions, and Restricted Use

You must not:

- access or use the Platform from, for the benefit of, or in connection with a prohibited or comprehensively sanctioned jurisdiction or restricted party, except as lawfully authorized;
- export, re-export, transfer, release, or provide the Platform, technology, technical data, software, models, or services in violation of export-control or sanctions law;
- use the Platform for prohibited military, intelligence, nuclear, missile, chemical, biological, surveillance, weapons, or human-rights-abusive end uses;
- conceal ownership, control, destination, end user, end use, or source of funds to evade sanctions or export controls; or
- use the Platform for bribery, kickbacks, unlawful payments, money laundering, sanctions evasion, or corruption.

17. Enforcement and Cooperation

Vizbl may investigate suspected violations and may, where reasonably appropriate:

- issue a warning, require remediation, request information, require identity or authority verification, impose limits, revoke credentials, block content, disable features, quarantine assets, or require an update;
- suspend, throttle, restrict, remove, or terminate access, accounts, Customer Applications, integrations, content, or Services;
- preserve records and evidence; notify affected persons, rights holders, service providers, app stores,

payment providers, or authorities; and cooperate with lawful investigations;

- remove or restrict content without prior notice where necessary to address legal, security, safety, fraud, child-protection, intellectual-property, privacy, operational, or third-party requirements; and
- recover fees, investigation costs, remediation costs, damages, or other amounts available under the applicable agreement or law.

Vizbl may take immediate action without prior notice where delay could increase risk. Enforcement decisions may consider severity, intent, impact, history, remediation, legal requirements, and risk to users, customers, Vizbl, or third parties. Vizbl is not obligated to monitor all activity or content and does not assume responsibility for user conduct merely because it has moderation or enforcement rights.

A Customer may request review of an enforcement decision by sending a written request to legal@vizbl.com within ten (10) Business Days after notice of the decision. A request for review does not stay an enforcement action, and Vizbl may decline repetitive, abusive, unsupported, or legally restricted requests. Nothing in this paragraph requires Vizbl to restore content, access, or functionality where doing so would create material legal, security, safety, privacy, intellectual-property, fraud, abuse, or third-party risk.

18. Reporting Violations

Report suspected violations, abuse, unlawful content, security issues, or misuse using the appropriate channel:

Issue	Contact
Abuse or unlawful content	abuse@vizbl.com
Security vulnerability or incident	security@vizbl.com
Copyright or trademark complaint	Use the procedure in the Copyright and Trademark Policy
Legal notice or other policy matter	legal@vizbl.com

Reports should include sufficient information to identify the account, content, application, integration, URL, asset, or conduct at issue and should not knowingly contain false statements. Do not send passwords, secret keys, unnecessary sensitive data, or illegal content by ordinary email.

19. Changes and Conflicts

Vizbl may update this Policy from time to time. For Customers in a paid committed term, a materially adverse change will generally take effect at the next renewal term unless the applicable agreement permits an earlier change. Changes required to comply with law, address security, safety, fraud, child-protection, intellectual-property, or Third-Party Service requirements, or prevent material harm may take effect immediately. For other users, changes take effect when posted or on the stated effective date. Continued use after the applicable effective date constitutes acceptance to the extent permitted by law.

If this Policy conflicts with an applicable signed Master Services Agreement, Platform & Developer Services Agreement, Order Form, or other agreement, that agreement controls to the extent of the conflict. This Policy supplements, and does not limit, any more specific restriction in the Terms of Use,

Prohibited Products Policy, Professional Use Policy, Review Policy, Copyright and Trademark Policy, Privacy Policy, DPA, Documentation, app-store rules, or applicable law.

Vizbl Systems, Inc.

155 S. Fair Oaks Ave, Suite 1005

Pasadena, California 91105, United States

Email: legal@vizbl.com