



DCSAI Technologies

LEGAL DOCUMENT · v1.0 · MAY 2026

Acceptable Use Policy

What you can and cannot do with the DCS Services

Acceptable Use Policy

This Acceptable Use Policy ("**AUP**") governs use of the products and services provided by DCS AI Technologies L.L.C ("**DCS**"). The AUP is incorporated by reference into the Master Services Agreement and applies to all customers, users, and visitors of any DCS service. By using the Services, you agree to comply with this AUP.

We keep the AUP short and specific. The rules below are not a wishlist — every rule exists because we have seen the underlying behaviour cause real harm. Violating the AUP can result in suspension or termination of your account, forfeiture of any prepaid fees, and referral to law enforcement where applicable.

1. Prohibited Content

You may not use the Services to create, store, transmit, or distribute content that:

- **Is illegal under applicable law** in any jurisdiction where you operate or where the affected party resides.
- **Sexually exploits or endangers minors.** This includes any form of CSAM, grooming content, or content sexualising minors. Zero tolerance; immediate termination + law enforcement referral.
- **Incites or threatens violence** against any person or group based on race, religion, ethnicity, nationality, gender identity, sexual orientation, or disability.
- **Facilitates terrorism** — recruitment, financing, planning, or glorification of terrorist acts.
- **Infringes intellectual property rights** of others, including copyright, trademark, patent, trade secret, or right of publicity.
- **Violates privacy rights**, including non-consensual sharing of personal information, intimate images, or doxxing.
- **Contains malware** — viruses, trojans, ransomware, exploit code intended to compromise systems.
- **Is fraudulent or deceptive** — phishing, social engineering, scams, impersonation of real people without consent.

2. Prohibited Activities

You may not use the Services to:

- **Send unsolicited bulk communications.** Includes spam email, unsolicited WhatsApp / SMS messages, robocalls, and unsolicited marketing across any channel. Consent must be opt-in and provable.
- **Make unauthorised credential-stuffing attempts,** password sprays, brute-force attacks against any system.
- **Conduct denial-of-service attacks** against any system, whether DCS-operated or otherwise.
- **Probe or scan vulnerabilities** of any system you do not have explicit permission to test. This includes DCS's own infrastructure unless you are operating under our public bug bounty program.
- **Reverse-engineer the Services** beyond what is permitted by applicable law, attempt to access source code, or attempt to extract model weights from inference responses.
- **Train a competing model** using outputs from the DCS Platform or DCS-provided LLM APIs without our prior written consent.
- **Operate a high-risk autonomous system** (medical diagnostics, legal advice, financial advice, life-safety decisions) without appropriate human oversight, qualified review, and disclaimers.
- **Generate deepfakes** of real people without their consent. Synthetic media depicting public figures must be clearly labelled as synthetic.
- **Generate election disinformation** — false claims about candidates, voting procedures, or election results.

3. Resource Use

You may not use the Services in a way that imposes disproportionate load on shared infrastructure:

- **Respect rate limits.** Published rate limits are not suggestions. Circumventing rate limits via multiple accounts or IP rotation is a violation.
- **Do not run mining or other computationally-intensive non-DCS workloads** on Compute workers you do not own.
- **Do not stockpile resources** — e.g., creating many empty workspaces, storing large files you never access, dispatching test jobs at high frequency.
- **Do not abuse free tiers** by creating multiple accounts to evade quotas.

4. AI-Specific Restrictions

Because DCS is an AI platform, we have specific rules about AI use:

- **No autonomous actions affecting real-world systems without human oversight** — agents must not be given unrestricted access to financial accounts, physical control systems, or other high-stakes systems without per-action human approval.
- **No undisclosed AI in customer-facing contexts** — if you use AI to respond to customers, you must disclose that AI is involved when asked or where required by law (e.g., California SB 1001).
- **No biometric inference** — using AI to infer protected characteristics (race, religion, sexual orientation, health status) from photos or behavioural data without informed consent.
- **No emotion or vulnerability exploitation** — using AI specifically to detect and exploit emotional states or cognitive vulnerabilities (e.g., loneliness, grief) for commercial purposes.
- **No social scoring** — using AI to score individuals' "trustworthiness" or similar in ways that determine access to services, in jurisdictions where this is prohibited (e.g., EU AI Act).

5. Use of Personal Data

If you process personal data through the Services:

- You are the Data Controller; DCS is the Data Processor. The DPA applies.
- You must have a lawful basis for processing under GDPR Art. 6 (or equivalent) before submitting personal data.
- You must inform data subjects about the processing as required by Art. 13/14 (or equivalent).
- You must respond to data subject rights requests within the legal timeframe (typically 30 days under GDPR).
- You must not submit special-category personal data (health, biometrics, sexual orientation, religion, etc.) unless your use case is permitted under Art. 9 and you have the additional safeguards in place.

6. Channel-Specific Rules

Different channels have specific compliance requirements that the AUP enforces:

6.1 WhatsApp Business Platform

You must comply with Meta's WhatsApp Business Policy and Commerce Policy. Notably: no broadcasts to non-opted-in users, no use of templates outside their approved category, no sale of regulated goods (firearms, alcohol in restricted jurisdictions, gambling without a licence).

6.2 Voice / SMS

You must comply with TCPA (US), CRTC rules (Canada), CSL (China), and equivalents. Provable opt-in consent is required for marketing calls / texts. STIR/SHAKEN attestation is required for US-originated voice traffic.

6.3 Email

You must comply with CAN-SPAM (US), CASL (Canada), and PECR/GDPR (EU). Each outbound email must include a working unsubscribe mechanism and accurate sender identification.

7. Enforcement

We respond to suspected AUP violations as follows:

Severity	Typical first response	Possible escalation
Minor	Written warning · 14 days to remediate	If unremediated: feature restriction
Moderate	Immediate suspension of affected feature · investigation	Account suspension if pattern continues
Serious	Immediate account suspension · investigation	Termination + forfeiture of prepaid fees
Egregious (CSAM, fraud, etc.)	Immediate termination · law enforcement notification	And/or criminal action

We reserve the right to take any action we believe appropriate to protect our users, third parties, and the integrity of the Services, including taking down content, suspending accounts, and reporting unlawful activity to authorities.

8. Reporting Violations

To report suspected AUP violations: abuse@dc sai.ai. For CSAM specifically: csam-report@dc sai.ai (monitored 24/7). Reports may be made anonymously; we respond to all reports within 24 hours.

9. Bug Bounty

Security researchers may probe DCS infrastructure under our public bug bounty program, published at dcsai.ai/security. Probing outside the bounty scope is a violation of this AUP. Good-faith security research within scope is welcomed and rewarded.

10. Changes to This AUP

We may update this AUP from time to time. Material changes will be announced at least 30 days in advance via email and the dashboard. The current version is always available at dcsai.ai/aup. Continued use of the Services after a change constitutes acceptance of the updated AUP.

This AUP is published under CC BY 4.0. Effective from 1 June 2026. Questions or interpretation requests: legal@dcsai.ai.