

Acceptable Use Policy

EFFECTIVE DATE	LAST UPDATED
July 23, 2026	July 23, 2026

This Acceptable Use Policy (“AUP”) applies to all use of CapConnect OS and related services. Capitalized terms not defined here have the meanings in the Master SaaS Subscription Agreement.

1 1. General Standard

Customer and Authorized Users may use the Services only for lawful, legitimate business purposes and in a manner that does not harm individuals, CapConnect, telecommunications carriers, email providers, data providers, other customers, or the public.

2 2. Prohibited Content and Conduct

Users may not use the Services to create, upload, transmit, facilitate, or promote:

- unlawful, fraudulent, deceptive, misleading, or abusive activity;
- phishing, impersonation, identity theft, credential theft, or social engineering;
- malware, ransomware, malicious code, exploitation, or unauthorized access;
- harassment, threats, hate, discrimination, stalking, or violence;
- sexual exploitation, non-consensual intimate content, or content involving minors;
- trafficking, illegal drugs, illegal gambling, unlawful weapons sales, or other prohibited commerce;
- infringement or misappropriation of intellectual property, privacy, publicity, confidentiality, or other rights;
- false endorsements, fabricated testimonials, deceptive offers, or material misrepresentations;
- do-not-call violations, suppression-list evasion, or outreach to recipients where Customer lacks a lawful basis;
- prerecorded, artificial voice, autodialed, automated, or similar calls or messages to mobile phones, residential lines, or other protected numbers without all legally required consent;
- caller ID spoofing or falsification of caller identification, sender identity, routing information, headers, domains, numbers, or authentication;
- manipulation of caller identification, sender identity, routing, headers, domain records, or authentication;
- attempts to evade opt-outs, suppression lists, spam filters, carrier controls, platform enforcement, or usage limits;
- scraping or acquisition of data in violation of law, contract, website terms, or technical restrictions;
- automated decision-making that produces legal or similarly significant effects without required safeguards; or
- activity likely to create material security, legal, regulatory, reputational, or deliverability risk.

3 3. Outreach Requirements

Customer must:

- have a lawful basis and all required consents or permissions for communications;
- identify the sender accurately;
- use truthful subject lines, caller identification, offers, and message content;
- honor opt-outs and do-not-contact requests promptly;
- maintain and apply suppression lists;
- comply with calling-hour restrictions, frequency limits, and consent requirements;
- provide legally required disclosures;
- obtain all required consent before recording or transcribing calls;
- avoid purchased, scraped, or generated lists that cannot be lawfully used;
- not send messages to emergency numbers, public-safety answering points, or prohibited destinations; and
- comply with carrier, email-provider, and third-party platform policies.

4 4. High-Risk and Restricted Uses

CapConnect may prohibit or require prior written approval for campaigns involving:

- consumer credit, debt relief, lending, mortgage, insurance, or financial products;
- healthcare, medical, genetic, or highly sensitive information;
- political campaigns, advocacy, or fundraising;
- legal services targeting vulnerable consumers;
- sweepstakes, contests, gambling, or prize promotions;
- age-restricted products;
- cryptocurrency, digital assets, investment solicitations, or trading services;
- employment screening, housing eligibility, education admissions, or other regulated decisions;
- public-sector, defense, sanctions-sensitive, or export-controlled activity; or
- any industry with elevated complaint, carrier, legal, or reputational risk.

5 5. Technical Restrictions

Users may not:

- probe, scan, or test system vulnerabilities without written authorization;
- bypass authentication or access controls;
- interfere with other customers;
- introduce excessive traffic or abusive API requests;
- use bots or automation except through approved features and APIs;
- share credentials or permit unauthorized access;
- upload secrets, credentials, or regulated data unnecessary for the Services;
- attempt to extract non-public models, prompts, algorithms, or data; or
- use the Services to benchmark or train a competing system.

6 6. Enforcement

CapConnect may investigate suspected violations and may remove content, limit functionality, block destinations, suspend campaigns, revoke numbers or domains, throttle usage, require remediation, or suspend or terminate access. CapConnect may cooperate with carriers, providers, regulators, and law enforcement where legally permitted or required.

CapConnect may take any enforcement action immediately, without prior notice, without liability, and without refund or credit, where CapConnect reasonably believes the activity may violate law, provider requirements, carrier rules, platform rules, consent obligations, do-not-call restrictions, caller-ID requirements, opt-out obligations, or creates regulatory, security, deliverability, abuse, complaint, carrier, platform, legal, or reputational risk.

Customer remains responsible for fees and obligations arising before or during suspension. CapConnect is not liable for actions taken in good faith to enforce this AUP or protect the Services.

7 7. Reporting

Suspected abuse may be reported to **support@capconnectsolutions.com**. Reports should include relevant account, campaign, sender, number, domain, and message details.

Questions about this document may be sent to legal@capconnectsolutions.com.