

Acceptable Use Policy

Version 2026-10-19-draft - published 2026-10-19

This Acceptable Use Policy ("AUP") lists what you may not do with the C2R.ai (Clientor) platform. It forms part of the Terms of Service and applies to every customer, User, agency client and anyone else who uses the Service through an account. It works together with the Communications & AI Agent Policy, which sets out the rules for calls, texts, messaging and email. Capitalized terms have the meanings given in the Terms of Service.

1. Illegal and unwanted communications

You may not use the Service to:

- place calls using an artificial or AI-generated voice, or send automated texts, to anyone without the prior express consent the law requires, or for telemarketing or advertising without prior express written consent;
- call or text numbers on the National Do Not Call Registry, a state do-not-call list or your own internal do-not-call list, except as the law permits;
- send spam, unsolicited bulk email, or messages to purchased, rented, scraped, appended or shared lists;
- contact people outside the calling hours or more often than the Communications & AI Agent Policy and the law allow;
- spoof or falsify caller ID, sender names, email headers or the origin of a message, or rotate numbers to avoid blocking or identification ("snowshoeing");
- leave artificial-voice voicemails, including "ringless" voicemails, without the required consent;
- continue contacting anyone who has opted out on any channel; or
- send messages with content that carriers or platforms prohibit, including the "SHAFT" categories (sex, hate, alcohol, firearms, tobacco) where not permitted, cannabis and CBD, high-risk financial offers such as payday loans and debt relief, third-party lead generation, gambling, and phishing.

2. Deception, impersonation and AI personas

You may not:

- configure an Agent to claim to be human, deny being an AI when asked, or remove or obscure the AI disclosure or recording disclosure;
- impersonate any person, business, government agency or official, or falsely claim an affiliation;

- clone, or upload or record for cloning, the voice of anyone other than the person giving the recording: a voice may be cloned only from a recording that person makes of their own voice, with their own written consent given in the product (for example, the account owner or a staff member recording themselves in Voice Studio); never from calls, voicemails, videos, recordings or samples of someone else;
- imitate the voice or likeness of a real person (including celebrities and public figures), or create a voice persona designed to be mistaken for a specific real person;
- use a cloned voice to impersonate the person whose voice it is or anyone else, or to deceive a listener about who is speaking; a cloned voice is still an AI voice, and the AI disclosure applies to every call made with it;
- keep using a cloned voice after the person whose voice it is withdraws consent or leaves your organization (delete it in Voice Studio);
- make false or misleading statements about prices, products, results, urgency, emergencies or legal consequences;
- generate or post fake reviews or testimonials, reviews written by an AI presented as a real customer's, or reviews from people without real experience of the business, or suppress negative reviews; or
- use the Service for phishing, social engineering, pretexting, or to obtain passwords, one-time codes, payment card numbers or bank details under false pretenses.

Voice recordings and voice models are handled as described in our Biometric Data Retention and Destruction Policy (clientor.ai/legal/biometric-policy).

3. Political, debt-collection and other restricted uses

3.1 Political and election communications. You may not use the Service for political campaign calls or texts, get-out-the-vote calls, fundraising for candidates or parties, issue advocacy calls to the public, or any communication intended to mislead voters about elections, unless we have agreed in writing in advance and you meet all applicable federal and state requirements.

3.2 Debt collection. You may not use the Service to collect debts, or for communications covered by the Fair Debt Collection Practices Act, Regulation F or state collection laws, unless you have told us in writing before starting and you comply with those laws (including their limits on call frequency, required disclosures and time-of-day restrictions).

3.3 Healthcare, legal and financial services. Agents may provide general information, scheduling, reminders and intake for licensed professionals. They may not diagnose, prescribe, provide medical, mental-health, legal, tax, investment, insurance or credit advice, or make eligibility or underwriting decisions, and you must not present Agent output as professional advice. Protected health information may be processed only under a signed Business Associate Agreement with us.

3.4 Other regulated offers. You must hold every license required for what you offer and comply

with industry-specific rules (for example, insurance, mortgage, real estate, auto sales, solar, home-improvement and timeshare telemarketing rules).

4. Harmful content and conduct

You may not use the Service to:

- harass, threaten, intimidate, stalk, bully or abuse anyone, or send hateful, discriminatory or violent content;
- create or distribute sexual content involving minors, or any non-consensual intimate content;
- promote or facilitate violence, terrorism, self-harm, human trafficking or illegal goods and services;
- discriminate unlawfully against anyone, including in housing, employment, credit, insurance or access to services; or
- distribute malware, ransomware, spyware or any other harmful code.

5. Data misuse, scraping and targeting

You may not:

- scrape, harvest or buy the personal or contact data of third parties' users, followers, members, reviewers or customers (including those of a competitor) to contact them through the Service;
- upload lists of people who did not consent to hear from you, or use the Business Brain or any connector to collect personal data about individuals for outreach;
- target a competitor's customers using data obtained from the competitor or from scraping; use native advertising-platform interest targeting instead, outside the Service;
- process special categories of data, children's data, payment card numbers, biometric identifiers or government identification numbers except as the Terms of Service and a signed addendum allow;
- use the Service to make solely automated decisions with legal or similarly significant effects on individuals;
- copy, download, export or extract the data shown in the dashboard in bulk other than through the export and reporting features the Service provides or the public API with your own API keys, or redistribute, sell, publish or share data obtained through the Service outside your organization except as needed to serve your own Contacts;
- access the dashboard or the Service with scripts, bots, browser automation, scrapers or any other automated means apart from the public API, or share, lend or pool a personal sign-in;

- keep or use data obtained through the Service after leaving the organization or after an Owner or we have deactivated your access; or
- infringe or misappropriate anyone's intellectual property, privacy or publicity rights.

6. Minors

You may not use the Service to communicate with, or knowingly collect personal information from, children under 13, or to market to minors anything that may not lawfully be sold or marketed to them. If your business serves minors (for example, tutoring or pediatric care), Agents must communicate only with parents or guardians.

7. High-risk and life-critical uses

You may not use the Service as an emergency service or to handle emergency calls, to replace 911 or any emergency line, for medical triage, or in any situation where a failure, delay or error could lead to death, personal injury, or serious physical or environmental damage. Agents for businesses that receive urgent calls (for example, plumbing, medical practices or security) must tell callers with an emergency to hang up and call 911 and must transfer urgent matters to a human.

8. Abuse of the platform and its models

You may not:

- attempt to jailbreak, prompt-inject or otherwise make the Service's models or Agents ignore their safety guardrails, or use Agents to generate content that the AI model providers' usage policies prohibit;
- probe, scan or test the vulnerability of the Service, or breach its security or authentication, except under a written security-testing agreement with us;
- access another organization's data, or attempt to get around tenant isolation, rate limits, budget caps or compliance locks;
- use the Service to build training data for, or to distill or copy, a competing AI model or service;
- overload the Service, or run automated access other than through our published APIs within their limits; or
- create multiple accounts to evade suspension, limits, verification or free-credit restrictions.

9. Reselling

You may not resell, sublicense, white-label or provide the Service to third parties, or operate client workspaces for other businesses, unless you have accepted the Agency / White-Label Reseller Addendum and comply with it.

10. Reporting

Report suspected violations, unwanted calls or messages from an agent powered by C2R.ai (Clientor), or security issues to [ABUSE EMAIL]. Include the number or address that contacted you, the date and time, and what happened. We review every report.

11. Enforcement

11.1 We may investigate suspected violations and may review relevant Customer Data and logs to do so, as the Data Processing Addendum allows.

11.2 If we find or reasonably suspect a violation, we may, at our discretion and without liability: warn you; require changes; pause an Agent, flow, channel, number or sender identity; lock outbound calling, texting or email; suspend or terminate your account; release or decline to port numbers used for illegal robocalling where carriers or regulators require it; and report the activity to carriers, platforms, law enforcement or regulators, including by responding to traceback requests from the Industry Traceback Group.

11.3 The response depends on the seriousness of the violation; for illegal robocalls, consent violations, impersonation, fraud, or anything that puts people or the platform at risk, we may act immediately without prior notice.

11.4 You are responsible for fees and Credits consumed before suspension, and for any carrier fines, penalties or costs that your violation causes us, as the Terms of Service describe.

11.5 We may update this AUP as described in the Terms of Service. Changes that respond to new laws, carrier rules or abuse patterns may apply immediately on posting.