Dealr Acceptable Use & Communications Policy (AUP)

Effective October 1, 2026 · v1.0.0

This Acceptable Use & Communications Policy ("**AUP**") governs use of the Services by Customer and its End Users. Capitalized terms used but not defined in this Policy have the meanings given in Section 2 of the MSA General Terms, including the terms Section 2 identifies as defined in other components of the Agreement. Violations are grounds for suspension under MSA §3.4 (suspension) and termination for cause under MSA §6.4 (termination for cause), and are covered by Customer's indemnity under MSA §12.2 (indemnity by Customer).

Part I — Platform Acceptable Use

1. Lawful use only. Customer will not use the Services to store, transmit, or process material or conduct activity that is unlawful, fraudulent, deceptive, defamatory, or infringing, or that violates any person's privacy or publicity rights.

2. Security of the Services. Customer will not: (a) probe, scan, or test the vulnerability of the Services or circumvent any security or authentication measure; (b) access data of another Dealr customer or any account not its own; (c) introduce malware or harmful code; (d) interfere with the integrity or performance of the Services; or (e) use the Services to attack or overload any system.

3. No misuse of the platform. Customer will not: (a) reverse engineer, decompile, or attempt to derive source code from the Services except as law permits notwithstanding this limit; (b) copy, frame, or mirror the Services; (c) resell, sublicense, rent, or provide the Services to third parties except to End Users as permitted (affiliated entities covered by the Order Form are permitted), or use the Services on a service-bureau, timesharing, or outsourced-processing basis for the benefit of any third party; (d) use the Services to build, or assist anyone in building, or to benchmark, a competing product or service, or publish performance benchmarks without Dealr's consent; (e) scrape or bulk-extract data other than Customer Content via the provided export mechanisms; (f) circumvent usage limits, plan gates, or security controls; or (g) exceed reasonable use of support and shared resources. This Section 3, with MSA §3.5(c) (restrictions), is the Agreement's statement of use restrictions; MSA §3.5(c) carries the license-scope restrictions that survive termination.

4. Credentials. Each End User uses a unique login; credentials may not be shared. Customer promptly deactivates departed personnel and notifies Dealr of suspected compromise.

4A. Connections and tokens. Customer will not, and will not permit any End User to: (a) share, export, or embed an access or refresh token issued for an AI Client Connection (MSA §10.2(d)) or other connection, or use it from any application other than the one it was issued to; (b) use a connection to retrieve data for any person other than Customer, including on a service-bureau basis or to aggregate data across Dealr customers; (c) use a connection to evade usage limits, rate limits, plan gates, or permissions, or run it at volumes designed to replicate the Services' database (bulk export is available through MSA §10.3 (export; deletion)); or (d) connect an AI application or account that Customer has not approved under its own information-security program.

5. Accurate information. Customer will keep account, billing, and licensing information (e.g., dealer or other business licenses, registrations) accurate and current, and will submit only truthful, accurate data in title, registration, tax, and financing workflows.

6. Customer websites. Where Dealr hosts, generates, or syndicates content to Customer's websites, Customer is the operator of its own sites and is solely responsible for their legal compliance. That responsibility includes cookie/tracking-consent requirements, its own website privacy policy and terms, accessibility (ADA/WCAG), and the compliance of content Customer directs Dealr to publish. Dealr will identify Dealr-deployed scripts or pixels on request and offers consent-management tooling as a feature. Deploying and configuring that tooling is Customer's responsibility.

7. DTS program integrity (Schedule B services). Customer will not: submit fraudulent, altered, or unauthorized documents or transactions; misrepresent any Dealr/DTS fee as a government fee; state or imply that any state agency endorses Customer or its services; or attempt to access state systems except through the Services as authorized. Schedule B's suspension and audit provisions apply in addition to this AUP.

Part II — Communications Compliance (calls, texts, email, voicemail)

8. Allocation of responsibility. The Services provide communication tools. As between Customer and Dealr, Customer is the initiator, seller, and (where applicable) telephone solicitor for all communications sent through the Services by or for Customer, to any recipient, and is solely responsible for their legal compliance. Customer alone selects and approves:

(a) the recipients of each campaign;

(b) the consent basis relied upon for each recipient;

(c) the campaign content and scripts, including approving the prompts, templates, and disclosure configurations that govern any AI agent acting on Customer's behalf; and

(d) the decision to launch, and the schedule of, each campaign.

Where an AI Feature composes individual outbound messages, the Services' default mode requires Customer's per-message review and approval before a message is sent; automatic sending applies only where Customer has affirmatively enabled it for the applicable feature or campaign, and that election is a Customer configuration choice recorded by the Services.

Dealr transmits communications only at Customer's direction and acts solely as a technology provider.

As between Customer and Dealr, Dealr provides the communications tools and acts solely within parameters Customer approves: Customer selects recipients, approves campaign content, scripts, prompts, and templates, sets timing and frequency rules, and controls consent classifications; AI composition and dialing/sequencing occur within those Customer-approved parameters; and automated compliance blocking under Section 18 and the AI Addendum (e.g., blocking campaigns lacking qualifying consent classifications) is a safety control, not the exercise of discretion over Customer's campaigns.

Dealr is not the initiator, seller, telemarketer, or telephone solicitor with respect to Customer's communications.

Dealr provides configuration options, consent-storage features, disclosure defaults, and suppression tooling as described in the AI Addendum and product documentation; Customer is responsible for configuring and using them correctly for its consumer base.

8A. Own-business traffic only. Customer may use the communications features only to communicate for Customer's own business with recipients whose consent runs to Customer. For purposes of this Part II, "Customer" includes the Affiliates and rooftops covered by the Order Form. This follows Part I §3(c) (no resale; End Users and covered affiliated entities permitted) and the Order Form's covered-entities list. A communication a group business-development center sends for a sibling rooftop covered by the same Order Form is Customer's own-business traffic, not third-party traffic.

Customer will not use the Services to: (a) send communications for or on behalf of any third party; (b) operate a lead-generation, list-rental, or marketing-bureau service; or (c) send communications whose seller or sender is any person other than Customer. Permitting a third party (including a marketing agency or outsourced BDC vendor) to send its own or another party's campaigns through Customer's account is a violation of this AUP.

9. Compliance with communications laws. Customer warrants that its calls, texts, voicemails (including ringless voicemail), and emails made or sent using the Services will comply with all applicable communications laws, including:

(a) the Telephone Consumer Protection Act (TCPA) and FCC rules and orders (including those treating AI-generated and prerecorded voice as "artificial or prerecorded voice");

(b) the Telemarketing Sales Rule;

(c) the CAN-SPAM Act; and

(d) state telemarketing, telephone-privacy, and text-messaging laws, including the Florida Telephone Solicitation Act, Texas Business & Commerce Code Chapters 302 and 305, Oklahoma's Telephone Solicitation Act, Maryland's Stop the Spam Calls Act, New Jersey's telemarketing statutes (as amended by P.L. 2023, c.108), Washington's telephone-solicitation and commercial-electronic-mail statutes (RCW 80.36.390; RCW ch. 19.190), Virginia's telephone-privacy statutes, and Oregon's telemarketing statutes.

Each law named in (a) through (d) applies as enacted, amended, or superseded from time to time. The statutes named in this policy are examples only. They do not limit, and Customer's obligations extend to, every federal, state, and local statute, regulation, rule, or order that applies to Customer's communications, whether or not named here and whether existing now or adopted later.

10. Consent. Before initiating a communication through the Services, Customer must hold, and on request produce, the level of consumer consent that Applicable Law requires for that communication's channel, content, and technology. This includes prior express written consent for marketing calls or texts using an autodialer, artificial or prerecorded voice, or AI voice. Customer will record consent evidence in the Services' consent store (or maintain equivalent records), including source, disclosure text, timestamp, and scope, and will classify campaigns accurately. Bulk-imported contact lists require Customer's attestation of consent basis; Customer is responsible for the accuracy of that attestation.

11. Do-not-call, opt-outs, and suppression. Customer will: (a) honor opt-out requests within the shortest period Applicable Law requires, using the Services' suppression processing; (b) maintain and honor its internal do-not-call list, with suppression records retained and honored for at least ten (10) years from the request or for such longer period as Applicable Law requires (revoked consent is not time-limited under federal law); (c) scrub against the National Do Not Call Registry and applicable state registries unless a documented exemption (e.g., established business relationship, written consent) applies; and (d) not evade suppression by changing numbers or channels.

12. Calling windows and frequency. Customer will observe the calling-time and frequency limits of the recipient's jurisdiction, including limits stricter than the federal 8 a.m.–9 p.m. (recipient local time) window and state per-day contact caps. Where the Services offer a "strict" default profile, Customer's relaxation of that profile is Customer's own compliance decision. That relaxation is subject to any acknowledgment mechanics the Services provide (AI Addendum §4.1 for AI Features).

13. Caller identity; telephone numbers. Customer will: (a) use only telephone numbers provisioned to it through the Services or that it is otherwise authorized to use; (b) not cause the display of misleading, inaccurate, or unauthorized caller ID or otherwise spoof, mask, or misrepresent the origin of a communication; (c) not rotate, cycle, or acquire numbers to evade frequency limits, suppression, or carrier blocking; (d) identify itself truthfully at the start of solicitation communications; and (e) cooperate promptly with any carrier, registered traceback consortium, or governmental inquiry concerning its communications, including reimbursing Dealr's reasonable costs of responding to legal process concerning Customer's communications.

14. Registration and bonding. Customer warrants that it holds, and will maintain, any telephone-solicitation registration, bond, or filing required of it by the states into which it communicates. Those states include Texas, Oklahoma, and Washington, where applicable, and any state that adopts such a requirement in the future. Customer is responsible for determining whether its campaigns trigger those requirements.

15. Recording and monitoring. Customer is responsible for lawfully recording or monitoring its communications, including obtaining all-party consent where required. Customer is likewise responsible, as the employer, for any employee-monitoring notice, acknowledgment, or consent its jurisdiction requires for workplace recording and activity logging with respect to its End Users' use of the Services. Examples of those requirements include N.Y. Civ. Rights Law §52-c, Conn. Gen. Stat. §31-48d, and 19 Del. C. §705. The Services enforce certain non-configurable safeguards. For example, recording disclosure cannot be disabled for a call, inbound or outbound, in which any party is in an all-party-consent state while recording is on, per the AI Addendum. Those safeguards do not shift responsibility to Dealr. Customer may not attempt to defeat them.

16. AI disclosures. Where Customer uses AI voice or AI-generated messaging, Customer is responsible for the disclosure configuration choices the AI Addendum allocates to it, including state AI-disclosure requirements for chatbots and synthetic voice.

17. Content of communications. Customer's communications must not be deceptive or harassing, must include required disclosures (identity, purpose, opt-out mechanics for texts and email), and must comply with advertising law applicable to vehicle sales and financing (including Truth in Lending and state advertising rules) — which remain Customer's obligations as the advertiser.

Part III — Enforcement

18. Monitoring; enforcement.

- (a) Dealr does not pre-screen Customer communications or content but may investigate suspected violations, may remove or block content or campaigns that violate this AUP or create legal risk, and may suspend affected features or accounts under MSA §3.4 (suspension).
- (b) Dealr will notify Customer of enforcement action where practicable.
- (c) Carrier and platform requirements (e.g., 10DLC registration, carrier content rules) are conditions of the underlying networks. Customer will cooperate with them. Messages violating them may be blocked by carriers regardless of Dealr action.
- (d) Customer will provide accurate and complete information for carrier and messaging-ecosystem registrations made by or through Dealr (including 10DLC brand and campaign registration) and will keep that information current.
- (e) Customer is responsible for, and will reimburse Dealr within thirty (30) days of invoice for, any fine, penalty, or surcharge imposed on Dealr by a carrier, aggregator, or messaging-ecosystem authority that is attributable to Customer's communications, content, or registration information.
- (f) Dealr may suspend affected numbers or campaigns to the extent a carrier or aggregator requires.

19. Reporting. Suspected abuse of the Services may be reported to abuse@dealr.cloud.

20. Changes. This AUP is an operational Incorporated Policy and may be updated per MSA §17.1 (operational policies); provided that any update that expands Customer's warranties, representations, indemnification, or liability obligations, or that materially restricts core use of a purchased Service, takes effect as provided in MSA §17.2 (material terms) (at the start of Customer's next Service Term), except to the extent the change is required by Applicable Law (MSA §17.1(d) (changes that are material in substance)).