

GRAVUN ACCEPTABLE USE POLICY

Effective Date: September 20, 2026

This Acceptable Use Policy (“**Policy**”) governs use of the Gravun platform and its associated services, including communications, AI, electronic signatures, payment integrations, and customer-facing pages.

It forms part of the agreement between **Gravun Inc.** (“**Gravun**”) and the subscribing business (“**Customer**”), including the applicable Terms of Service and any executed Master Services Agreement (“**Agreement**”). Capitalized terms not defined here have the meanings given in the Agreement.

1. Application and Responsibility

1.1 Permitted Purpose. Customer may use the Service for lawful business activities within its purchased subscription and the permissions granted under the Agreement.

1.2 Authorized Users. Customer must ensure that its Authorized Users and persons acting on its behalf comply with this Policy. Customer must not direct, authorize, or knowingly facilitate conduct that it could not undertake itself.

1.3 Customer-Facing Activities. Customer is responsible for the content, instructions, and configurations it supplies for booking pages, campaigns, calls, signing requests, invoices, and other interactions with its clients. Customer is not automatically responsible for independent misconduct by an unrelated person merely because that person interacts with a Customer-facing page.

1.4 Legal and Contractual Standards. This Policy establishes conditions for using Gravun. It does not exhaust every legal requirement applicable to Customer’s business. Some restrictions are platform requirements even where the underlying activity might otherwise be lawful.

1.5 No Compliance Approval. Successful delivery of a message, processing of a payment, completion of a signature, or acceptance of an uploaded file does not establish that the activity is lawful or approved by Gravun.

2. Unlawful, Deceptive, and Harmful Conduct

2.1 Prohibited Conduct. Customer must not use the Service to:

(a) commit or facilitate fraud, theft, extortion, money laundering, or another unlawful activity;

(b) impersonate another person or business, misrepresent authority, or create misleading accounts, invoices, records, or communications;

(c) threaten, harass, stalk, unlawfully discriminate against, or deliberately expose another person to harm;

(d) distribute unlawful content or material that infringes intellectual property, confidentiality, privacy, or other legally protected rights;

(e) collect credentials, payment information, or personal information through phishing, deceptive interfaces, or other dishonest means; or

(f) conceal the source, destination, purpose, or beneficiary of an activity to evade a lawful restriction or a restriction under the Agreement.

2.2 Business Representations. Customer must accurately describe its identity, goods, services, prices, and material transaction terms. It must not misrepresent licensing, accreditation, insurance, affiliation, or approval by Gravun or another organization.

2.3 Fabricated Evidence. Customer must not manufacture or manipulate records to falsely establish consent, delivery, acceptance, payment, work completion, or another material event.

3. Accounts, Access, and System Integrity

3.1 Authorized Access Only. Customer must not access another workspace, account, system, or information without authorization or exceed the permissions assigned to it.

3.2 Credentials. Customer must not sell, transfer, or expose access credentials contrary to the Agreement, use another person's credentials without permission, or permit access through an account after the relevant authority has ended.

3.3 Interference. Customer must not introduce malware, exploit vulnerabilities, interfere with security controls, overwhelm the Service, or deliberately impair another customer's access.

3.4 Circumvention. Customer must not bypass subscription limits, usage metering, authentication controls, communication restrictions, suppression lists, or an enforcement measure. Creating another account or changing an identifier to continue a restricted activity is prohibited.

3.5 Automated Access. Customer may use supported APIs and authorized automation within the applicable permissions and published limits. It must not use automated extraction, excessive polling, or another technique that obtains unauthorized information or materially disrupts the Service.

3.6 Security Testing. Intrusive testing, vulnerability exploitation, and access to production information require Gravun's prior written authorization. A person who inadvertently discovers a vulnerability should stop the affected activity, avoid accessing additional information, and report the issue under Section 12.

3.7 Subscription Misuse. Customer must not use the Service to operate an unauthorized resale, hosted service, or competing access service contrary to the Agreement.

4. Personal Information and Confidential Materials

4.1 Lawful Authority. Customer must have the rights and permissions required to collect, upload, use, and disclose information through the Service.

4.2 Necessary Information. Customer must limit submitted information to what is reasonably needed for its permitted business activities. It must not use ordinary notes, messages, recordings, or uploads as a repository for unnecessary credentials or highly sensitive information.

4.3 Restricted Information. Unless expressly approved in writing under appropriate technical and contractual arrangements, Customer must not use the Service to:

- (a) store payment-card security codes, full magnetic-stripe data, PINs, or similar payment authentication data;
- (b) submit protected health information where doing so requires a business associate agreement or equivalent arrangement that has not been executed;
- (c) establish biometric identification or authentication using voiceprints, facial templates, or similar identifiers; or
- (d) process information subject to specialized legal, residency, or security requirements that the purchased Service has not expressly agreed to support.

Ordinary payment processing through the designated payment interface is not prohibited by paragraph (a). A recording or drawn signature does not, by itself, authorize biometric identification.

4.4 Privacy Choices. Customer must not suppress, falsify, or evade a valid privacy request, consent withdrawal, or communication preference. A lawful retention exception may be applied only to the relevant information and purpose.

4.5 Confidential Information. Customer must not upload another person's trade secrets or confidential materials without authority or instruct an AI feature or integration to disclose them improperly.

5. Email, SMS, and Marketing Campaigns

5.1 Lawful Basis for Contact. Before initiating a communication, Customer must establish the permission or other lawful basis applicable to the recipient, channel, content, and location. A business address, previous transaction, public listing, or acquired contact list does not automatically establish permission for every communication.

5.2 Contact Lists. Customer must not use unlawfully harvested or generated contact details. Purchased, rented, or third-party lists may be used only where Customer can demonstrate the rights required for the intended communication and their use is permitted by the relevant delivery provider.

5.3 Accurate Identification. Customer must not falsify sender details, caller identification, routing information, subject lines, or the purpose of a communication. Required business identification, contact details, and disclosures must remain clear and accessible.

5.4 Opt-Outs. Customer must provide legally required opt-out methods and honour requests within the applicable period. It must also comply with any stricter provider requirement disclosed for the selected service.

5.5 Suppression Records. Customer must not remove suppression entries, re-import opted-out contacts, switch numbers or domains, or use another workspace to continue communications contrary to a valid opt-out. Any renewed contact must rest on a lawful basis consistent with the scope of that opt-out.

5.6 Transactional Messages. Customer must not label a promotional message as a booking confirmation, invoice notice, signing request, or other transactional communication to evade marketing requirements.

5.7 Consent Evidence. Where consent or an exemption is relied upon, Customer must retain appropriate evidence of its source, scope, date, and relevant conditions. A consent field entered by Customer is not independent verification by Gravun.

5.8 Delivery Integrity. Customer must investigate material complaint, bounce, or abuse patterns and cooperate with reasonable remediation requests. It must not rotate senders or alter message content merely to evade filters, carrier review, or restrictions.

5.9 Provider Registration. Customer must provide accurate information for applicable sender, campaign, number, or business registration processes. Registration or approval by a provider does not replace the required permission to contact an individual.

6. Calling, Recording, and Voice Features

6.1 Calling Requirements. Customer must comply with applicable calling restrictions, including required permissions, calling hours, do-not-call rules, identification obligations, and rules governing automated or artificial-voice communications.

6.2 Recording and Transcription. Before recording or transcribing a communication, Customer must provide required notice and obtain required consent. It must not assume that a rule applicable in its own location necessarily governs every participant.

6.3 AI Receptionist Disclosures. Customer must accurately configure any required AI, recording, and transcription disclosures. It must not instruct a voice feature to conceal its automated nature where disclosure is required or falsely claim to be a particular human.

6.4 Voice Impersonation. Customer must not clone or imitate another person's voice without the necessary rights and permissions or use synthetic speech for deceptive impersonation.

6.5 Emergency Use. Unless a particular service is expressly documented as supporting emergency calling, Customer must not present Gravun as an emergency communications service or rely on its AI receptionist as the sole route for reporting an emergency.

6.6 Access to Recordings. Customer must restrict recordings and transcripts to appropriate personnel and recipients. Recording a call does not authorize unrestricted publication, training use, or disclosure.

7. AI and Automated Workflows

7.1 Authorized Use. Customer may use AI and automation only within the purchased functionality, granted permissions, and applicable law.

7.2 Review. Customer must apply review proportionate to the consequences of an output or action. It must not knowingly distribute materially false AI-generated statements or rely on unsupported outputs for consequential factual assertions.

7.3 Prohibited Uses. Customer must not use AI features to generate or facilitate:

- (a) fraudulent invoices, fabricated records, false testimonials, or deceptive impersonations;
- (b) unlawful discrimination, exploitation, harassment, or privacy intrusion;
- (c) instructions intended to obtain unauthorized access to information or defeat security controls; or
- (d) decisions or activities prohibited elsewhere in this Policy.

7.4 Consequential Decisions. Customer must not use Gravun AI as the sole basis for a decision producing legal or similarly significant effects where applicable law requires additional safeguards, explanation, consent, or human review that have not been established.

7.5 Permissions and Limits. Customer must not attempt to induce an AI feature to reveal another workspace's information, expose credentials, ignore access restrictions, or perform actions outside its authorized scope.

7.6 External AI Connections. Customer must assess the permissions granted to external AI tools and revoke access that is no longer appropriate. Connecting a tool does not authorize processing prohibited by the Agreement or restrictions applying to the source data.

8. Gravun Sign

8.1 Eligible Documents. Customer must use Gravun Sign only where electronic execution and the available signing process are appropriate for the document and relevant jurisdiction. Customer must comply with the applicable Document Eligibility Matrix and restrictions presented for the feature.

8.2 Restricted Categories. Where the eligibility guidance blocks a document category or requires additional formalities, Customer must not bypass that restriction. A document involving witnessing, notarization, registration, or enhanced identity verification must not be presented as satisfying those requirements unless the actual process does so.

8.3 Signer Authority. Customer must not sign for another person without lawful authority, misuse a signing link, or represent that a signature establishes authority that has not been verified.

8.4 Consent and Intent. Customer must not bypass, obscure, or pre-complete a signer's required consent or intention-to-sign step. Customer must not substitute its own acceptance for the signer's required action.

8.5 Document Integrity. Customer must not alter a completed document or certificate and present the altered copy as the original completed record. Any legitimate amendment must be clearly identified and executed or acknowledged as appropriate.

8.6 Certificate Claims. Customer must not describe a Gravun certificate as notarization, independent identity verification, government certification, or a guarantee of enforceability where the signing process does not establish that fact.

8.7 Signing Links and Copies. Customer must use accurate recipient details, protect signing links, and take reasonable steps to prevent unauthorized disclosure of documents and certificates.

9. Invoices, Payments, and Customer Transactions

9.1 Genuine Transactions. Customer must use payment features only for genuine, lawful transactions it is authorized to conduct.

9.2 Prohibited Payment Conduct. Customer must not use the Service to process fictitious sales, test stolen payment credentials, conceal the true merchant or beneficiary, or circumvent a payment-provider restriction.

9.3 Transaction Information. Prices, descriptions, payment authorizations, cancellation terms, and refund representations must be accurate and consistent with Customer's agreement with its client.

9.4 Provider Rules. Customer must comply with the applicable payment-provider terms, including restrictions on prohibited goods or services and required verification. Customer must not disguise a restricted transaction through an inaccurate description or invoice.

9.5 Disputes. Customer must not fabricate transaction evidence, obstruct a lawful refund or dispute process, or falsely attribute its own goods, services, or payment obligations to Gravun.

10. Resource Use and Third-Party Restrictions

10.1 Service Capacity. Customer must observe agreed usage limits and reasonable technical controls. A high volume of legitimate activity does not, by itself, constitute abuse.

10.2 Material Disruption. Gravun may require Customer to modify a workflow that demonstrably causes material instability or interferes with other customers, using proportionate measures under the Agreement.

10.3 External Requirements. Customer must comply with provider conditions applicable to a feature where those conditions have been identified or made available to Customer. Mandatory legal or provider restrictions may require an affected feature to be limited or withdrawn under the Agreement.

10.4 No Unrelated Fee Changes. This Policy does not create undisclosed overage fees or amend negotiated subscription quantities, rates, or service commitments.

11. Investigation and Enforcement

11.1 Grounds for Review. Gravun may investigate credible reports, provider notices, technical indicators, or other reasonable evidence of a violation. A complaint alone does not establish that Customer has breached this Policy.

11.2 Customer Cooperation. Customer must reasonably cooperate with an investigation and provide relevant information within a reasonable period, which may be shorter where urgency requires. Requests may include evidence of consent, authority to use a list, transaction legitimacy, or steps taken to address a compromised account.

11.3 Access Restrictions. Investigative access to Customer Content remains subject to the Agreement, DPA, and applicable law. This Policy does not authorize unrestricted inspection or use of Customer information.

11.4 Corrective Measures. Depending on the seriousness and urgency of the issue, Gravun may require corrective action, restrict an affected campaign or feature, block harmful content, revoke compromised credentials, or suspend affected access.

11.5 Notice and Cure. Where reasonably practicable and consistent with the Agreement, Gravun will explain the issue and allow an opportunity to correct it. Immediate protective action may be taken where necessary to address serious security risks, unlawful activity, material harm, or a binding legal or provider requirement.

11.6 Proportionality. Gravun will reasonably seek to confine restrictions to the affected activity, feature, or account. Suspension or termination of the wider subscription remains subject to the grounds and procedures in the Agreement.

11.7 Evasion and Repetition. Deliberate circumvention, repeated material violations, or failure to remedy a material breach may support suspension or termination under the Agreement.

11.8 Evidence and Disclosure. Gravun may preserve relevant evidence and disclose information where lawfully required or permitted, subject to the DPA and applicable privacy obligations. It will not promise confidentiality to a complainant where disclosure is legally required.

11.9 Review of a Restriction. Customer may request review by providing the relevant account details, disputed restriction, and supporting explanation. Gravun will consider the request in good faith. Review does not require a protective restriction to be lifted while its grounds remain unresolved.

11.10 Financial Consequences. Charges, refunds, indemnification, and liability arising from enforcement are governed by the Agreement. This Policy creates no separate penalty, automatic forfeiture, or additional uncapped indemnity.

12. Reporting Misuse

12.1 Reports. Suspected misuse or security concerns may be reported to:

Gravun Inc.

Abuse reporting: Hello@gravun.com

Security reporting: Hello@gravun.com

12.2 Relevant Details. Reports should identify the affected page, message, document reference, or account where known and explain the concern. Reporters should provide only information reasonably necessary to assess the issue and should not circulate signing links, credentials, or sensitive records unnecessarily.

12.3 False Reports. Knowingly false or malicious reports, including reports intended to disrupt another business without a proper basis, are prohibited.

13. Relationship to the Agreement and Updates

13.1 Consistent Enforcement. This Policy supplements the Agreement. It does not override negotiated protections concerning notice, suspension, termination, data handling, or liability.

13.2 Updates. Gravun may update this Policy using the notice and amendment procedures in the Agreement. Changes addressing urgent legal, security, or abuse risks may take effect sooner only to the extent permitted by the Agreement.

13.3 Continuing Obligations. Compliance with this Policy does not reduce Gravun's own contractual or statutory obligations or waive a right that cannot lawfully be waived.