IntakeClean

Document intake for small law firms
Generated 2026-05-04

# Acceptable Use Policy

Prohibited content and behavior on IntakeClean. Incorporated by reference into the Terms of Service.

# IntakeClean — Acceptable Use Policy

**Last updated:** `[YYYY-MM-DD]`

This Acceptable Use Policy (the "**AUP**") governs your use of the IntakeClean Service. It is incorporated by reference into the Terms of Service. Violation of this AUP is a material breach of the Terms.

## 1. Prohibited content

You shall not use the Service to upload, store, transmit, or otherwise make available any content that:

- (a) is illegal under U.S. federal, state, or local law, or any other law applicable to you;
- (b) you do not have the right to upload (e.g., content that infringes a third party's intellectual property, privacy, publicity, or contractual rights);
- (c) constitutes child sexual abuse material (CSAM) or otherwise sexually exploits minors;
- (d) contains malware, ransomware, viruses, worms, Trojan horses, or other malicious code;
- (e) constitutes credit-card numbers, full Social Security numbers, or other regulated financial or government identifiers, **except** to the extent that such information appears within a client's intake documents and is processed in accordance with the Customer's professional obligations and applicable law;
- (f) contains protected health information ("**PHI**") as defined under HIPAA, **unless** Customer has executed a Business Associate Agreement with IntakeClean (none is included in the standard subscription); or
- (g) is intended to harass, threaten, defame, or impersonate any person.

## 2. Prohibited uses

You shall not, and shall not permit any third party to:

- (a) reverse engineer, decompile, disassemble, or attempt to derive the source code of the Service, except to the limited extent applicable law expressly permits;
- (b) modify, translate, or create derivative works of the Service or any of its components;
- (c) rent, lease, lend, sell, sublicense, or otherwise commercially exploit the Service to any third party other than for the benefit of Customer's own End-Clients in the ordinary course of Customer's

professional-services practice;

- (d) use the Service to develop a competing product or service, or to benchmark performance for any such purpose, without IntakeClean's prior written consent;
- (e) probe, scan, or test the vulnerability of the Service except in accordance with IntakeClean's published responsible disclosure or bug-bounty program (if any);
- (f) interfere with or disrupt the Service, including by exceeding documented rate limits, sending denial-of-service traffic, or attempting to bypass security or access controls;
- (g) access the Service to compile a competing dataset, train an external machine-learning model, or extract documents in bulk other than via the documented export tools;
- (h) circumvent metering, quotas, or billing;
- (i) use the Service to send unsolicited bulk communications ("**spam**") or any communication that violates applicable anti-spam law (e.g., CAN-SPAM, TCPA, CASL, GDPR Article 7);
- (j) impersonate any person or entity, or misrepresent your affiliation with any person or entity;
- (k) misuse the End-Client upload link (e.g., posting it publicly to invite uploads from persons unrelated to Customer's matters); or
- (l) use the Service in violation of any applicable rule of professional responsibility.

## 3. Security and integrity

You are responsible for the security of your account credentials, your API tokens, and any End-Client upload links you generate. Notify `[security@CONTACT EMAIL]` promptly of any actual or suspected unauthorized use. You shall not share login credentials with any person who is not an Authorized User.

## 4. AI integrations

If you enable any optional AI integration:

- (a) you remain responsible for ensuring you have the legal basis to transmit Customer Content to that provider;
- (b) you acknowledge that AI outputs are assistive only and may be inaccurate (see `06-ai-disclaimer.md`);
- (c) you shall not use the Service to develop AI models that compete with IntakeClean.

## 5. Reporting violations

To report a suspected AUP violation, email `[abuse@CONTACT EMAIL]` with relevant details, the affected URL or content, and your contact information. We will investigate and take action as appropriate.

## 6. Enforcement

Without limiting any other remedies, IntakeClean may, in its discretion, after reasonable attempts to notify Customer where practical:

- (a) require corrective action;
- (b) remove or disable access to specific content;
- (c) suspend the affected account or feature; or
- (d) terminate the Agreement under Section 6 of the Terms.

In the case of an active threat to the Service, other customers, or third parties (e.g., active malware distribution, active denial-of-service, CSAM), IntakeClean may take immediate action without prior notice.

---