You.com API

Acceptable Use Policy

For API Integrations & Developer Use · Effective May 15, 2026

Overview

This Acceptable Use Policy ("AUP") governs all programmatic and API-based access to You.com Services. It applies to developers, organizations, and any application or automated system that queries, integrates with, or redistributes You.com outputs.

By calling the You.com API or embedding You.com Services in your application, you agree, and you agree to ensure, that all end users in your organization abide by this policy. Continued use of the Services after review of this AUP will assume acknowledgement of adherence to these terms.

Developer Responsibility

You are responsible for your application's compliance with this AUP, including misuse by your end users.

You must implement safeguards (input filtering, output moderation, rate limiting) appropriate to your use-case.

If You.com identifies a violation originating from your integration, your API access may be suspended.

Prohibited Uses - Summary

Category	Prohibited Activities
Privacy & Data	• Unauthorised access to user data, networks, or systems • Collecting/processing sensitive PII (health, SSNs, biometrics) without consent • Misusing API outputs to harvest or infer private information
Illegal Activity	• Generating or distributing CSAM or child-exploitative content • Facilitating counterfeit goods, illegal substances, or unlicensed professional advice • IP infringement, harassment, hate speech, violence, or trafficking • Researching the application, development, or construction of hazardous materials, weapons, or other harmful instruments
Platform Abuse	• Generating malware, viruses, or disruptive code via the API • Automated spam or email campaigns using API output • Bypassing rate limits, safety filters, or other API restrictions • Scraping, prompt-injection attacks, or resource exhaustion

Harm to Persons	• Discriminatory outputs including those related to employment, housing, credit, or essential services • Content promoting self-harm, eating disorders, or violence • Defamatory, humiliating, or non-consensual intimate imagery
Misinformation & Fraud	• Generating or amplifying disinformation at scale • Impersonating individuals or organizations • Academic dishonesty tools or fake-engagement services

Detailed Policy Requirements

1. Privacy & Data Protection

Your API integration must not:

- Attempt to gain unauthorised access to or exploit vulnerabilities in any user, network, device, or communications system, including via spoofing or social engineering.
- Collect, process, infer, or share sensitive personal data (health records, government IDs, biometrics, financial credentials, API keys, passwords) without user consent and applicable legal authority or a contract that includes appropriate regulatory agreements.
- Use API outputs to build profiles on individuals or to re-identify anonymised data.
- Submit photos, audio, or other biometric data for identification without explicit, informed consent.

2. Illegal Activity & Harmful Content

Your API integration must not generate, facilitate, or distribute:

- Child sexual abuse material (CSAM) or any content that sexualises or exploits minors.
- Counterfeit goods, illicit drugs, or services that circumvent legal frameworks.
- Content that facilitates harassment, stalking, bullying, or threats against any individual or group.
- Discriminatory outputs affecting employment, housing, credit, or access to essential services.
- Unauthorised professional advice (legal, medical, financial) presented as authoritative.
- Content infringing third-party intellectual property, trade secrets, or privacy rights.
- Material that promotes violence, terrorism, extremism, harassment or trafficking.

3. Platform Integrity & API Misuse

Programmatic access imposes additional obligations beyond standard uses:

- Do not use the API to generate malware, ransomware, exploits, or any code intended to compromise systems.
- Do not use API output to power automated spam, phishing, or unsolicited bulk messaging or run Listserv, Maillist or auto-responders on our outputs.
- Do not attempt to circumvent rate limits, safety classifiers, content filters, or any access controls built into the API.
- Do not run bots, scrapers, “spiders” or load-testing tools against You.com infrastructure without explicit written authorization to do so.
- Do not use prompt injection, jailbreaking techniques, or adversarial inputs to manipulate model behavior.

- Do not copy or store for re-use significant portions of the Content of our API without contractual authorization to do so.

Examples of Prohibited Conduct: Rate Limits

Excessive API calls that degrade service quality for other users constitute abuse regardless of intent. Implement exponential back-off and caching in your integration. Repeatedly ignoring 429 responses may result in suspension.

4. Harm to Individuals & Communities

Do not use the API to produce or distribute:

- Content that discriminates against protected classes in consequential decisions (hiring, lending, housing).
- Material that promotes, normalises, or provides instruction for self-harm, suicide, eating disorders, or substance abuse or other actions harmful to human beings.
- Content inciting violence, abuse, or physical harm against any person or group or system.
- Gratuitous depictions of violence, gore, or non-consensual sexual content.
- Content inappropriate for minors if your application may be accessed by users under 18.
- Defamatory, humiliating, abusive or shaming content targeting real individuals.

5. Misinformation, Deception & Fraud

Do not use the API to:

- Generate disinformation, fabricated news, or synthetic media designed to deceive.
- Power fake-engagement services (fake reviews, social media manipulation, astroturfing).
- Create tools that facilitate plagiarism, contract cheating, or academic fraud.
- Impersonate real individuals, brands, or organizations without authorisation.
- Falsely attribute AI-generated content to human authors to mislead recipients.

Enforcement

You.com reserves the right to:

- Suspend or terminate API access immediately upon detection of a policy violation.
- Rate-limit or throttle integrations that generate unusual or potentially harmful traffic patterns.
- Report violations to relevant authorities where legally required.

Reporting Violations

If you discover a vulnerability, material misuse pattern, or significant AUP violation in your own integration or another's please report it to: legal@you.com. Responsible disclosure of security issues will not be treated as a policy violation. If you specifically wish to disclose a found security issue, please email security@you.com, or a privacy issue email privacy@you.com.