GetPassive Acceptable Use Policy

GetPassive Ltd
Last updated: 2026-05-31
Version: 1.0
Company details: Company No 17245817, registered office London, United Kingdom **Effective date:** 2026-06-01

1. Purpose

1.1 This Acceptable Use Policy (**AUP**) applies to all businesses and individuals who purchase, access, or use GetPassive internet-sharing network services (**Business Partners**).

1.2 The purpose of this AUP is to protect end-users, networks, websites, public services, and GetPassive's platform from unlawful, harmful, abusive, or high-risk activity.

1.3 By using GetPassive, Business Partners agree to this AUP and any product-specific rules shown in the dashboard, order form, or contract.

2. Permitted Uses

2.1 GetPassive may be used for lawful business purposes such as: publicly available web data collection for market research; ad verification; price aggregation; SEO monitoring; brand protection; availability testing; content localisation testing; and other approved data collection activities.

2.2 Business Partners are responsible for ensuring their use complies with all applicable laws, website terms, robots.txt where relevant, intellectual property rights, privacy laws, sanctions rules, and contractual obligations.

3. Prohibited Uses

3.1 Business Partners must not use GetPassive for DDoS attacks, denial-of-service activity, stress testing without written authorisation, port scanning, vulnerability scanning of third-party systems, brute force attacks, or automated exploitation.

3.2 Business Partners must not use GetPassive for credential stuffing, password spraying, account takeover, session hijacking, phishing, social engineering, fake account creation, or attempts to bypass account security.

3.3 Business Partners must not access or attempt to access .gov or .mil domains, government systems, military systems, emergency services, public safety systems, or financial institutions' internal systems.

3.4 Business Partners must not distribute, host, retrieve, transmit, or facilitate malware, spyware, ransomware, spam, botnets, CSAM, terrorist content, hate content where unlawful, or any illegal content.

3.5 Business Partners must not use GetPassive to circumvent fraud detection, risk scoring, device fingerprinting, anti-money-laundering controls, payment limits, ticketing limits, gambling restrictions, sanctions controls, or platform enforcement systems.

3.6 Business Partners must not target entities, infrastructure, users, or services located in sanctioned countries or involving sanctioned persons under OFAC, UK, EU, UN, or other applicable sanctions lists.

3.7 Business Partners must not share credentials, API keys, accounts, sessions, or access tokens with unauthorised third parties, make access available to unapproved third parties without written permission, or allow unvetted customers to use the service.

3.8 Business Partners must not use GetPassive for collecting or processing special category data, children's data, health records, financial account data, government identifiers, or other highly sensitive data unless expressly approved in writing.

3.9 Business Partners must not overload target websites, ignore reasonable rate limits, interfere with services, or continue activity after receiving a cease-and-desist, block notice, or abuse complaint.

3.10 Business Partners must not use GetPassive in any way that could expose End Users, Developers, or GetPassive to legal, reputational, security, or regulatory harm.

4. KYC and Account Verification

4.1 Business Partners must complete identity verification, business verification, sanctions screening, and other Know Your Customer checks before account activation or at any time requested by GetPassive.

4.2 Business Partners must provide accurate, current, and complete information. GetPassive may suspend access if verification is incomplete, outdated, false, or suspicious.

5. Monitoring and Enforcement

5.1 GetPassive monitors for AUP violations using logs, metadata, automated controls, blocklists, destination rules, complaints, and manual review.

5.2 GetPassive may suspend, throttle, block destinations, terminate accounts, revoke credentials, or require additional information without notice where it suspects a violation, security risk, legal risk, or harm to third parties.

5.3 Violations may result in immediate termination and forfeiture of any prepaid balance, credits, or unused service value to the fullest extent permitted by law.

5.4 GetPassive may report unlawful activity to law enforcement, regulators, affected networks, or other parties where appropriate or required.

6. Business Partner Responsibilities

6.1 Business Partners must secure credentials, rotate keys if compromised, supervise employees and contractors, and ensure all activity under their account complies with this AUP.

6.2 Business Partners must maintain accurate contact details and respond promptly to abuse, compliance, or security requests.

7. Reporting Abuse

7.1 Report suspected abuse to **abuse@getpassive.io**. Include timestamps, destination, logs, request samples, and any relevant identifiers where available.

7.2 GetPassive reviews abuse reports and may take action at its discretion.

8. Governing Law

8.1 This AUP is governed by the laws of England and Wales.