Acceptable Use Policy

Last Updated: January 1, 2026

This Acceptable Use Policy ("**AUP**") governs your use of the Playbook platform and related services (the "**Services**") provided by **PYBK, Inc.**, doing business as **Playbook** ("**Playbook**," "**we**," "**us**," or "**our**").

This AUP is incorporated by reference into the **Terms of Service** and applies to all users, including administrators, members, guest users, and API clients.

1. Permitted Use

You may use the Services solely for lawful, authorized business purposes in accordance with the Terms of Service and applicable law.

2. Prohibited Activities

You may not, directly or indirectly:

A. Unlawful or Harmful Use

- Use the Services in violation of any applicable law or regulation
- Facilitate illegal, fraudulent, deceptive, or harmful activities
- Store or transmit unlawful content

B. Security and Platform Integrity

- Introduce malware, viruses, or malicious code
- Attempt to gain unauthorized access to systems or data
- Interfere with or disrupt the integrity, performance, or availability of the Services
- Conduct security testing or penetration testing without authorization

C. Data and Privacy Misuse

- Access, use, or disclose data without proper authorization
- Scrape, harvest, or bulk export data except as expressly permitted
- Circumvent access controls, rate limits, or usage restrictions

D. AI and Automation Misuse

- Use AI features to generate unlawful, deceptive, or harmful outputs
- Attempt to reverse engineer AI models, prompts, or system behavior
- Circumvent AI safeguards, guardrails, or limitations
- Represent AI-generated content as human-generated where prohibited by law

E. Competitive and Commercial Misuse

- Use the Services to build, benchmark, or support competing products
- Resell, sublicense, or provide service-bureau access to the Services
- Exploit the Services in a manner inconsistent with normal business use

F. API Abuse

- Exceed documented API limits
- Share API credentials improperly
- Use APIs in a manner that degrades service performance or security

3. Guest Users and Third Parties

Customers are responsible for the actions of all users they authorize, including guest users and third parties.

Playbook is not responsible for misuse arising from customer-granted access.

4. Enforcement

Playbook may investigate suspected violations and may, at its discretion:

- Suspend or restrict access to the Services
- Disable specific features, including AI features or APIs
- Terminate accounts in accordance with the Terms of Service

Playbook is not required to provide prior notice before taking enforcement action where necessary to protect the Services, users, or third parties.

5. Changes to This Policy

Playbook may update this AUP from time to time. Continued use of the Services after updates constitutes acceptance of the revised policy.

6. Contact Information

PYBK, Inc.
Email: **contact@pybk.ai**