FUNDAPPS
Monitor It. Report It.

Acceptable Use Policy

Updated: September 2025
Applies to: All Users of the Service

At FundApps, we are committed to providing a secure, reliable, and high-performing service for all our users. To uphold this commitment and foster a positive environment, this Acceptable Use Policy (**"AUP"**) outlines acceptable and unacceptable conduct for our Services. Violations, especially deliberate, repeated, or harmful ones, may lead to suspension or termination of access. By accessing or using the Service, you agree to comply with this AUP.

This policy may be updated; please check regularly. Capitalised terms not defined here are defined in the latest FundApps General Terms.

1. Fair and Responsible Use

Users may only access the Service in ways that are consistent with its intended purpose, within reasonable usage limits, and in compliance with all applicable agreements.

Specifically, you may not:

- Use high-frequency or automated scripts, bots, or tools that cause excessive load on the platform, degrade performance, or interfere with normal system operation.
- Run continuous polling, crawling, scraping or data harvesting processes without prior written authorisation.
- Create or use unauthorised automation (e.g., headless browsers, custom connectors) that bypass usage limits or fair usage expectations.

2. Abuse of Access and Workarounds

The Service is offered under defined pricing, licensing, and feature models. You must not:

- Attempt to circumvent product or feature restrictions that are intended for separate licensing or subscription tiers.
- Use any undocumented, internal or unsupported APIs, endpoints or methods - whether accessed via reverse-engineering, UI manipulation or other techniques for any purpose, including but not limited to:
    - Automating access to data or exports;
    - Circumventing workflow steps or controls;
    - Integrating with unauthorised systems or scripts; and
    - Extracting information at a scale or frequency not intended for user consumption.

- Modify, instrument, or manipulate the user interface (e.g., via browser automation, injected scripts, headless browsers, or overlays) to extract data, simulate user behaviour, or bypass intended usage patterns.
- Attempt to gain access to features, functionality or data in a manner not explicitly supported by the Service or that undermines billing models, product boundaries or usage controls.
- Share accounts, tokens, or credentials with other parties.

3. Infrastructure & Platform Use

To maintain availability and security for all users, the following activities are strictly prohibited:

- Uploading, transmitting, or executing any code or processes that may disrupt, damage, or interfere with the Service's infrastructure.
- Attempting to probe, scan, or test the vulnerability of any system or network related to the Service.
- Bypassing or attempting to bypass any platform or access controls.
- Hosting or distributing any malware, ransomware, or code intended to disrupt systems.
- Using any artificial intelligence (AI) system, tool, or service to infer, replicate, or approximate our algorithms, models, or methodologies.

4. Security and Account Responsibility

You are responsible for maintaining the confidentiality and security of your access credentials and must not share accounts or credentials.

You must promptly notify security@fundapps.co if you become aware of any unauthorised access or breach related to your use of the Service.

5. Enforcement

FundApps reserves the right to investigate any violation of this AUP and may take appropriate actions including:

- Temporary or permanent account suspension.
- Throttling or restricting API access.
- Fee adjustments or back-charging for unauthorised usage.
- Legal action if warranted.

6. Contact

For questions or to report a suspected violation, please contact us at security@fundapps.co.