ACCEPTABLE USE

Policy

Dividend Portfolio Planner

Document control	Value
Document owner	Dividend Portfolio Planner
Effective date	September 3, 2026
Version	1.0
Review cycle	At least annually and after material legal, product, security, or service changes
Classification	Public

Policy objective: Establish clear rules for lawful, safe, responsible, and authorized use of Dividend Portfolio Planner (DPP), while protecting users, the Platform, DPP information, third-party services, and the integrity and availability of DPP systems.

Trust Center note: This is a public, user-facing policy. It describes prohibited and restricted uses without disclosing confidential security configurations, internal procedures, or personal information.

1. Purpose

This Acceptable Use Policy (AUP) defines the standards that apply when accessing or using Dividend Portfolio Planner (DPP), including its website, applications, accounts, research tools, portfolio-planning features, artificial intelligence features, reports, exports, APIs or integrations made available by DPP, and related services (collectively, the “Platform”).

Use of the Platform must be lawful, authorized, respectful of others, and consistent with the educational, research, and planning purposes of DPP. This policy supplements the DPP Terms & Conditions of Use.

2. Scope

This policy applies to all visitors, registered users, subscribers, authorized representatives, and other persons who access or use the Platform.

It also applies to activity performed through a DPP account, regardless of whether the activity was performed directly by the account holder or by another person using credentials, sessions, tokens, or access provided by the account holder.

3. Acceptable use principles

Users must use DPP in a manner that protects the security, integrity, availability, and lawful operation of the Platform.

Users are expected to:

- Use the Platform only for lawful educational, research, planning, and other authorized purposes.
- Provide accurate account information where required and keep account credentials secure.
- Respect intellectual property, privacy, confidentiality, and other rights of DPP and third parties.
- Use research, market information, calculations, projections, and AI-assisted outputs responsibly and in accordance with the Terms & Conditions of Use.
- Comply with reasonable technical limits, security controls, and instructions presented through the Platform.
- Promptly report suspected unauthorized account access or security concerns through DPP's published support or security channel.

4. Prohibited unlawful or harmful activity

Users may not use, attempt to use, or enable another person to use DPP to engage in unlawful, fraudulent, deceptive, abusive, or harmful activity.

Prohibited activity includes:

- Violating applicable laws, regulations, court orders, or legally binding restrictions.
- Committing or facilitating fraud, theft, identity misuse, impersonation, money laundering, market manipulation, or other unlawful financial activity.
- Using DPP to threaten, harass, exploit, defame, or unlawfully discriminate against another person.
- Uploading, transmitting, or distributing malicious code, malware, ransomware, destructive instructions, or other harmful material.
- Using the Platform to infringe intellectual property, privacy, publicity, contractual, or other legal rights.
- Attempting to use DPP in a manner that creates material risk to DPP, its users, vendors, or third parties.

5. Security and access restrictions

Users may not interfere with, bypass, defeat, probe, or misuse DPP security controls or access mechanisms except where DPP has expressly authorized a security-testing activity in writing.

Without authorization, users may not:

- Access or attempt to access another user's account, data, portfolio information, subscription information, or other nonpublic information.

- Share, sell, transfer, publish, or improperly disclose passwords, authentication codes, tokens, sessions, recovery information, or other account credentials.
- Bypass authentication, authorization, rate limits, access restrictions, subscription controls, or other technical safeguards.
- Probe, scan, test, exploit, or attempt to exploit Platform vulnerabilities outside an expressly authorized security-testing process.
- Interfere with logging, monitoring, security alerts, or protective controls.
- Use automated means to create accounts, generate abusive traffic, or circumvent controls intended to protect Platform availability or security.

6. Platform integrity and availability

Users may not use the Platform in a way that materially degrades, disrupts, overloads, damages, or interferes with DPP services or the experience of other users.

Examples include:

- Launching denial-of-service activity or generating traffic intended to exhaust Platform resources.
- Using bots, scripts, crawlers, scrapers, or other automated processes in a manner not expressly authorized by DPP.
- Repeatedly submitting requests designed to impair performance or evade technical limitations.
- Introducing corrupted data, malicious files, or inputs intended to cause abnormal Platform behavior.
- Attempting to alter, disable, delete, or disrupt Platform systems, data, configurations, integrations, or services without authorization.

7. Data, privacy, and confidential information

Users must respect the privacy and confidentiality of information processed through DPP.

Users may not:

- Submit personal, confidential, proprietary, or regulated information that they do not have the legal right or authority to provide.
- Use DPP to unlawfully collect, identify, track, profile, expose, or disclose information about another person.
- Attempt to extract or reconstruct nonpublic DPP information, another user’s information, authentication secrets, or confidential system information.
- Use information obtained through DPP for unauthorized marketing, spam, harassment, fraud, or other purposes inconsistent with applicable law or DPP policies.
- Publish or distribute nonpublic information obtained through unauthorized access to the Platform.

8. Financial research and market information

DPP is an education, research, and planning tool and is not a financial adviser, broker-dealer, fiduciary, or provider of individualized investment advice.

Users may not misrepresent DPP research, calculations, projections, backtests, AI-assisted outputs, or educational materials as personalized financial advice issued or endorsed by DPP.

Users may not use the Platform to facilitate unlawful securities activity, market manipulation, deceptive investment promotions, or other conduct prohibited by applicable financial laws or regulations.

Users remain responsible for independently evaluating and verifying financial information and for all financial and investment decisions made using information available through the Platform.

9. Artificial intelligence and automated features

Where DPP provides artificial intelligence or automated analysis features, users must use those capabilities consistently with this policy and the Terms & Conditions of Use.

Users may not intentionally use automated features to:

- Generate or facilitate unlawful, fraudulent, malicious, or deceptive activity.
- Attempt to reveal confidential system instructions, credentials, security controls, or another user's nonpublic information.
- Automate abusive requests or evade usage, security, or subscription controls.
- Represent AI-generated output as guaranteed, verified, personalized investment advice from DPP.
- Use generated content in a manner that violates third-party intellectual property, privacy, or other legal rights.

10. Intellectual property and Platform content

DPP and its licensors retain their rights in the Platform, software, designs, branding, reports, educational materials, calculations, methodologies, and other protected content, subject to applicable law and the rights expressly granted in the Terms & Conditions of Use.

Unless expressly authorized, users may not:

- Copy, reproduce, republish, sell, sublicense, or commercially redistribute substantial portions of DPP proprietary content.
- Reverse engineer, decompile, disassemble, or attempt to derive protected source code or proprietary technology except to the extent such restriction is prohibited by law.
- Remove or alter copyright, trademark, attribution, security, or proprietary notices.
- Use DPP branding in a manner that falsely suggests sponsorship, endorsement, partnership, or affiliation.

11. Automated access, scraping, and integrations

Automated access to DPP is permitted only when provided or expressly authorized by DPP and must comply with applicable documentation, technical limits, authentication requirements, and contractual terms.

Unauthorized scraping, bulk extraction, automated copying, credential-based automation, or systematic collection of Platform content or user information is prohibited.

DPP may restrict or disable automated activity that creates security, privacy, intellectual-property, service-availability, or contractual risk.

12. Account responsibility

Users are responsible for maintaining reasonable control of their DPP accounts and for activity performed through their credentials or authorized sessions.

Users should not share account access except where DPP expressly supports and authorizes such access. Suspected compromise, unauthorized use, or loss of control of an account should be reported promptly.

DPP may require additional verification, credential reset, session termination, or other protective measures when account compromise or misuse is suspected.

13. Enforcement

DPP may investigate suspected violations of this policy and take reasonable action to protect users, the Platform, DPP systems, and third parties.

Depending on the nature, severity, and urgency of the activity, DPP may:

- Warn the user or request corrective action.
- Limit, block, or remove particular activity or content where applicable.
- Temporarily restrict or suspend access.
- Terminate an account or subscription in accordance with applicable agreements and law.
- Preserve relevant records when reasonably necessary for security, fraud prevention, dispute resolution, legal obligations, or enforcement.
- Cooperate with service providers, regulators, courts, or law-enforcement authorities when legally required or otherwise permitted by law.

14. Good-faith security reporting

DPP encourages responsible reporting of suspected security vulnerabilities or security concerns through the official security or support contact method published by DPP.

Users must not exploit a suspected vulnerability beyond what is reasonably necessary to identify and report it, access another person’s data, degrade service, destroy or alter information, demand payment, or publicly disclose sensitive vulnerability information in a manner that creates unnecessary risk.

Any security testing must remain within the scope expressly authorized by DPP.

15. Relationship to other DPP policies

This Acceptable Use Policy should be read together with the other public documents made available through the DPP Trust Center.

16. Changes to this policy

DPP may update this policy to reflect changes in Platform functionality, technology, security risks, legal requirements, or business practices.

Material changes may be communicated through the Platform or other reasonable methods. The current version will identify its effective date.

17. Contact and reporting

Questions about this policy, suspected account misuse, or security concerns should be submitted through the official contact methods published on the Dividend Portfolio Planner website or Trust Center.

For security and privacy reasons, users should not include passwords, authentication codes, full payment-card information, or other unnecessary sensitive information in reports or support communications.

Related Trust Center documents

Document	Purpose
Terms & Conditions of Use	Establishes the contractual terms governing use of DPP, including educational-use, investment-risk, subscription, and liability disclosures.
Information Security Overview	Provides a public overview of DPP's information security program and principal safeguards.
Access Control Policy	Describes DPP's approach to authorization, authentication, access management, and access review.
Data Privacy, Retention and Deletion Policy	Describes DPP's approach to privacy, retention, user privacy requests, and secure deletion.

Trust Center Notice

This public policy is intended to communicate DPP's acceptable-use requirements without disclosing confidential security architecture, internal procedures, vulnerabilities, credentials, personal information, or other sensitive operational information.