

COOKIE POLICY

Policy and User Choices

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 changes to cookies, browser storage, analytics, advertising, privacy requirements, or Platform functionality
Classification	Public

Policy objective: Explain how Dividend Portfolio Planner (DPP) uses cookies and browser storage, the purposes these technologies serve, the choices available to users, and how users can control or remove them.

Trust Center note: This public policy describes DPP's cookie and browser-storage practices at a functional level. Because the currently provided DPP policy materials do not identify the exact production cookie names, storage keys, vendors, or expiration values, this policy does not invent them. DPP should maintain and publish a current cookie inventory or consent-manager list showing the specific technologies actually deployed.

1. Purpose

This Cookie Policy explains how DPP uses cookies and similar browser technologies when users visit or interact with the DPP website and Platform. It also explains how users can manage these technologies through DPP controls, where available, and through browser or device settings.

This policy should be read together with the DPP Data Privacy, Retention and Deletion Policy and Terms & Conditions of Use.

2. Scope

This policy applies to cookies, local browser storage, session storage, and similar client-side technologies used by or on behalf of DPP through supported web experiences.

It does not describe every storage technology that may be used by a user's browser, operating system, or unrelated third-party website.

3. What are cookies and browser storage?

Cookies are small data files that a website can place or read through a user's browser. Cookies may be temporary for a browsing session or may remain for a defined period.

Browser storage is functionality provided by modern browsers that allows a website to store limited information on a user's device. Common forms include local storage and session storage.

These technologies can support functions such as authentication, security, user preferences, consent choices, Platform performance, and analytics.

4. Which cookies and browser storage DPP may set

DPP limits cookies and browser storage to legitimate Platform, security, preference, and analytical purposes. The categories below describe the types of storage that may be used by DPP.

Category	Typical purpose	Examples of information stored	Control
Strictly necessary / essential	Operate the Platform, maintain sessions, authenticate users, protect accounts, process consent choices, prevent abuse, and provide requested functionality.	Session or authentication state, security indicators, consent status, load-balancing or service state. DPP should avoid storing passwords or full payment-card data in browser storage.	Generally required for requested Platform functions and cannot always be disabled through DPP controls.
Preferences / functional	Remember user-selected settings and improve continuity between visits.	Display choices, interface preferences, or other nonessential settings selected by the user.	May be controlled through DPP cookie or privacy settings where offered, or removed through browser settings.
Analytics / performance	Understand aggregate Platform usage, identify errors, evaluate performance, and improve services.	Pseudonymous or device/browser identifiers, page or feature interactions, referral information, and performance events, subject to applicable settings and disclosures.	Where required, used only after appropriate consent. Users may be able to decline through DPP cookie controls or browser/privacy tools.
Advertising / marketing	Measure campaigns or support advertising or marketing activities if DPP activates such technologies.	Campaign identifiers, referral information, or similar identifiers appropriate to the disclosed purpose.	DPP should not activate nonessential advertising cookies where consent is required unless the user has provided the required choice or consent.

5. Browser storage used by the Platform

DPP may use browser storage in addition to traditional cookies. The specific keys and values depend on the production implementation and should be documented in DPP's maintained cookie and storage inventory.

Storage type	How DPP may use it	Typical duration
Session cookies / session storage	Maintain temporary state during a browser session, support authentication flows, security, and requested Platform functions.	Usually ends when the browser session ends, subject to the technology used.
Persistent cookies	Remember permitted settings, consent choices, or other functions across visits.	Remains until its configured expiration or until removed.
Local storage	Store limited client-side preferences, consent state, or other Platform information appropriate for local browser storage.	Remains until removed by DPP logic, the user, or the browser, unless an expiration mechanism is implemented.

6. Current cookie and storage inventory

The policy documents provided for preparation of this Trust Center policy establish that DPP may use cookies and similar identifiers, analytics, authentication information, and security controls, but they do not identify the exact cookie names, local-storage keys, session-storage keys, vendors, domains, or expiration periods currently deployed in production.

Accordingly, DPP should maintain a current implementation-level inventory that identifies, at minimum:

- Cookie or browser-storage name/key.
- Provider or party setting it.
- Domain or service on which it operates.
- Purpose and category.
- Whether it is essential or optional.
- Information stored or collected at an appropriate descriptive level.
- Expiration or retention period.
- Whether information is shared with or processed by a third party.
- Applicable consent or control mechanism.

Where DPP deploys a cookie-consent manager, the current inventory may be presented dynamically through that tool so users can see the specific cookies and browser-storage technologies in use.

7. How DPP uses these technologies

Subject to the user's choices and applicable law, DPP may use cookies and browser storage to:

- Sign users in and maintain authenticated sessions.

- Protect accounts and detect suspicious or abusive activity.
- Remember consent and privacy choices.
- Maintain user-selected Platform preferences.
- Support reliable operation and troubleshooting.
- Measure Platform usage and performance.
- Understand which features are useful and improve the user experience.
- Support marketing measurement or advertising only where DPP has activated those functions and applicable requirements have been satisfied.

8. Third-party technologies

Some DPP functions may depend on third-party providers, such as authentication, payment, analytics, communications, or other technology services. Those providers may set or access cookies or similar technologies when necessary to provide their services.

DPP evaluates third-party processing as part of its privacy and security governance. Third-party technologies remain subject to the provider's applicable terms and privacy practices as well as DPP's contractual and configuration controls.

DPP's existing privacy and security policies contemplate third-party processors and analytics services, but the supplied materials do not identify the specific cookie-setting vendors currently active on the production Platform. The published cookie inventory should be updated whenever such vendors are added, removed, or materially changed.

9. How users can control cookies and browser storage

9.1 DPP cookie or privacy controls

Where DPP provides a cookie banner, preference center, or privacy settings, users can use those controls to accept, reject, or change choices for nonessential categories. Strictly necessary technologies may remain active because they are required to provide requested services, maintain security, or remember privacy choices.

9.2 Browser controls

Most browsers allow users to view, block, delete, or limit cookies and site data. Browser settings may also allow users to clear local storage and session-related site data.

Users should consult the privacy or site-data settings in their browser to manage stored DPP data. Blocking all cookies or deleting essential site data may sign the user out, remove saved preferences, reset consent choices, or prevent portions of the Platform from functioning correctly.

9.3 Private browsing and device controls

Private or incognito browsing modes may limit how long some browser data remains on a device, but they do not necessarily prevent all cookies, browser storage, analytics, or network-level processing.

Device-level privacy controls may provide additional options depending on the browser and operating system.

9.4 Changing a prior choice

Where a DPP preference center is available, users may revisit it to change nonessential cookie choices. Users can also delete existing site data through their browser. A new choice generally applies prospectively and does not automatically erase information already processed under a lawful basis.

10. Retention and expiration

DPP's internal privacy policy establishes that cookies and similar identifiers should follow their disclosed lifespan and that nonessential identifiers generally should not be retained longer than necessary for their purpose.

Exact expiration periods must reflect the technologies actually configured in production. DPP should periodically review cookie and browser-storage durations and remove technologies that are no longer necessary.

Information derived from cookies or browser storage may be retained separately in DPP or provider systems according to the applicable purpose and the DPP Data Privacy, Retention and Deletion Policy.

11. Data minimization and security

DPP seeks to minimize information stored in cookies and browser storage and to avoid placing highly sensitive information in client-side storage when it is not necessary.

DPP's security policies require safeguards appropriate to the sensitivity of information, including access controls, encryption where appropriate, secure authentication practices, monitoring, and retention controls.

DPP does not intend to store full payment-card numbers or card security codes in DPP browser storage. Payment processing is designed to rely on an appropriate hosted payment provider.

12. Do Not Track and similar browser signals

Browsers and devices may provide privacy signals or settings that differ in operation and legal effect. DPP should evaluate and honor legally required browser-based opt-out or preference signals where applicable to DPP's processing activities and jurisdictions.

Because the supplied DPP materials do not establish whether the current production Platform recognizes a particular browser signal, this policy does not represent that any specific signal is currently implemented.

13. Children and cookies

DPP should apply its Terms & Conditions of Use and privacy requirements to determine who may create or use an account. DPP should not knowingly use optional tracking technologies in a manner inconsistent with applicable requirements concerning children or minors.

14. Related Trust Center documents

Document	Purpose
Data Privacy, Retention and Deletion Policy	Describes DPP's approach to collection, retention, privacy requests, processors, and secure deletion.
Information Security Overview	Provides a public overview of DPP's information security safeguards.
Access Control Policy	Describes DPP's approach to authorization, authentication, access management, and access review.
Acceptable Use Policy	Defines permitted and prohibited uses of the DPP Platform.
Terms & Conditions of Use	Establishes the contractual terms governing use of DPP.

15. Changes to this policy

DPP may update this Cookie Policy when cookies, browser-storage practices, service providers, Platform functionality, privacy requirements, or user-control mechanisms materially change.

The current version should identify its effective date. Material changes may be communicated through the Platform or other reasonable means where appropriate.

16. Contact

Questions about this Cookie Policy or DPP privacy practices may be submitted through the official contact methods published on the Dividend Portfolio Planner website or Trust Center.

Users should not include passwords, authentication codes, full payment-card information, or other unnecessary sensitive information in privacy or support communications.

TRUST CENTER NOTICE

This Cookie Policy is intended to provide a clear public description of DPP's use of cookies and browser storage. The implementation-level cookie inventory should be kept current so that users can identify the specific cookies and storage technologies actually deployed on the Platform.