Privacy policy options for Chrome:

•        Privacy Sandbox policies:- It addresses the controversial Third Party tracking cookies which collects the sensitive Data. There are different policies listed as follows:

**-- Blocked in Incognito mode**

•        PrivacySandboxAdMeasurementEnabled :- It prevents tracking behavior of a user across different websites.

--Currently enabled

<https://chromeenterprise.google/policies/#PrivacySandboxAdMeasurementEnabled>

•        PrivacySandboxAdTopicsEnabled :- It blocks third-party cookies tracking but still delivers relatable content

--Currently enabled

<https://chromeenterprise.google/policies/#PrivacySandboxAdTopicsEnabled>

•        PrivacySandboxPromptEnabled:- This policy allows or denies the usage of specific Privacy Sandbox features on a web page.

<https://chromeenterprise.google/policies/#PrivacySandboxPromptEnabled>

When set to Enabled, it permits the use of certain Privacy Sandbox APIs (such as Attribution Reporting, Federated Credential Management, Private Aggregation, and Protected Audience) within the browser context and when set to Disabled, it restricts access to these features, enhancing user privacy by preventing certain data-sharing mechanisms.

•        PrivacySandboxSiteEnabledAdsEnabled: A policy to control whether the Privacy Sandbox Site-suggested ads setting can be disabled for your users. If you set this policy to Disabled, then the Site-suggested ads setting will be turned off for your users. If you set this policy to Enabled or keep it unset, your users will be able to turn on or off the Privacy Sandbox Site-suggested ads setting on their device. Setting this policy requires setting the PrivacySandboxPromptEnabled policy to Disabled.

-- Currently enabled

<https://chromeenterprise.google/policies/#PrivacySandboxSiteEnabledAdsEnabled>

•        AutofillAddressEnabled :- Setting the policy to True or leaving it unset gives users control of Autofill for addresses in the UI.Setting the policy to False means Autofill never suggests or fills address information, nor does it save additional address information that users submit while browsing the web.(For more Details :- <https://chromeenterprise.google/policies/#AutofillAddressEnabled>)

•        AutofillCreditCardEnabled :- Setting the policy to True or leaving it unset means users can control autofill suggestions for credit cards in the UI.(For how to implement :- <https://chromeenterprise.google/policies/#AutofillCreditCardEnabled>)

•        BrowsingDataLifetime :- This policy allows admins to configure (per data-type) when data is deleted by the browser. This is useful for customers that work with sensitive customer data.

(For more details :- <https://chromeenterprise.google/policies/#BrowsingDataLifetime>)

•        MetricsReportingEnabled :- When this policy is Disabled, anonymous reporting is disabled and no usage or crash data is sent to Google. Users won't be able to change this setting.On Microsoft® Windows®, this policy is only available on instances that are joined to a Microsoft Active Directory domain, joined to Microsoft Azure Active Directory or enrolled in Chrome Browser Cloud Management.

(For more details :- <https://chromeenterprise.google/policies/?policy=MetricsReportingEnabled>)

•        PasswordManagerEnabled :- Disable this policy to prevent Chrome from saving users’ passwords.

(For more Details :- <https://chromeenterprise.google/policies/?policy=PasswordManagerEnabled>)

•        SearchSuggestEnabled :- Disable this policy to prevent Chrome from using a prediction service to help complete web addresses or search terms, when users type in the address bar. Suggestions based on bookmarks or history are unaffected by the policy.

( For more Details :- <https://chromeenterprise.google/policies/?policy=SearchSuggestEnabled>)

•        SpellCheckServiceEnabled :- Disable this policy to prevent Chrome from using Google's online spell-checking service to suggest spelling corrections on managed devices. This policy only controls the use of the online service. Setting the policy to Disabled means this service is never used.

(For more Details :- <https://chromeenterprise.google/policies/?policy=SpellCheckServiceEnabled>)

•        TranslateEnabled :- By using Chrome’s built-in translation features, users avoid relying on external translation services that might collect data.Google’s Cloud Translation API service (used by Chrome) has separate terms that prioritize data privacy more than the publicly available version of Google Translate.

For more Details (<https://chromeenterprise.google/policies/?policy=TranslateEnabled>)

•        BlockThirdPartyCookies :- Blocking third-party cookies prevents advertisers and other entities from tracking users across different websites. Blocking third-party cookies prevents advertisers and other entities from tracking users across different websites. It helps in Mitigating Data Leakage.

( For More Information :- <https://chromeenterprise.google/policies/#BlockThirdPartyCookies>)

•        DataLeakPreventionClipboardCheckSizeLimit :- This policy sets a minimal data size (in bytes) for the content in the clipboard. When users paste content from the clipboard, Chrome checks it against the configured DataLeakPreventionRulesList policy. It ensures that only substantial data undergoes privacy checks, improving efficiency and user experience. It also helps in striking a good balance between Privacy and Performance.

(For more information :- <https://chromeenterprise.google/policies/#DataLeakPreventionClipboardCheckSizeLimit>)

•        DataLeakPreventionReportingEnabled :- This policy is a general switch for all rules defined in the DataLeakPreventionRulesList policy. Setting this policy to True will switch on real-time reporting of data leak prevention events.

( For more Information :- <https://chromeenterprise.google/policies/#DataLeakPreventionReportingEnabled>)

•        ClearBrowsingDataOnExitList :- Ensures that sensitive data (such as browsing history and saved passwords) is wiped out as soon as Chrome is closed. Prevents unauthorized users from accessing saved credentials or browsing history.It also Reduces the chances of accidental data leaks.( For more information :- <https://chromeenterprise.google/policies/#ClearBrowsingDataOnExitList>)

-- Currently active

**Additional Policies discovered:**

BookmarkBarEnabled: Sets bookmark bar in Chrome

--Currently Active

DefaultBrowserSettingsEnabled: Setting this policy to True has chrome always check whether it’s the default browser on startup and auto register itself. Setting to False stops it from ever checking if it’s the default and turns user controls off.

-- Currently set to False

ExtensionInstallForcelist: Specifies a list of apps and extensions that install silently, without user interaction, and which user cannot uninstall or turn off

--Currently active

InsecureContentAllowedForUrls: Allows you to set a list of url patterns that specify sited which are allowed to display blockablable (i.e active) mixed content (i.e HTTP content on HTTPS sites) and for which optionally blockable mixed content upgrades will be disabled.

--Active value set

JavaScriptBlockedForUrls: This policy lets you set a list of Url patterns that specify the sites that can’t run JavaScript. Eg mobile.twitter.com

Managed Bookmarks: Sets up a list of bookmarks where each one is a dictionary with the keys name & url. These hold the bookmarks name and target. Admins can setup subfolders by defining bookmarks without a url with an additional child key.

--Active values set

PopupsAllowedForUrls: Setting this policy lets you set a list of url patterns that specify the sites that can open pop-ups

--Active values set

ProxySettings: Setting this policy configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified.

--Active values set

ShowAppsShortcutInBookmarkBar: Setting policy to true displays the apps shortcut and setting it to False means this shortcut never appears:

-- Currently set to False

UserDataDir: Configues the directory that chrome will use for storing user data

--Active values set