Program Policies

The Chrome Web Store is committed to providing a safe and secure environment for users, built on trust and transparency. For these reasons, the Chrome Web Store requires all developers to comply with both the Developer Program Policies listed below, and the Developer Agreement. When your extension is reviewed by Google, these policies act as a guiding principle for those reviews. These policies apply to the entire user experience of your application/extension/theme – including any marketing materials, user generated content, ads, landing pages, etc – unless otherwise noted.

Best Practices and Guidelines

1. Research and understand the Chrome Web Store policies (/docs/webstore/program-policies). Before developing a Chrome extension, it is important to review the Chrome Web Store Developer Program Policies and ensure your extension complies with all guidelines and requirements.
2. Extensions should add value to the Chrome Web Store. If your extension is not particularly useful or unique, it doesn't belong on the Chrome Web Store.
3. No cheating. If you attempt to scam the system (for example, by misleading users, circumventing enforcement, copying the work of other developers, or manipulating your extension's reviews or ratings) you will be banned from the Chrome Web Store.
4. Developers must carefully adhere to strict guidelines (/docs/webstore/program-policies#protecting-user-privacy) regarding the collection, use, and disclosure of user data, and must obtain user consent for any data collection or usage. Apps that access sensitive user data such as financial information, health information, or personal information must comply with additional policies and guidelines.
5. Ensure that all of your extension's information and metadata are up to date and accurate. This also includes information provided in the developer dashboard at the time of publishing, such as data collection certifications, item category, etc.
6. Test your extensions for crashes, broken features, and bugs prior to submission.

7. Verify that your contact information is correct to ensure you receive important communications for the Chrome Web Store. Some of these emails will require action on your part. Failing to respond could result in the removal of your item from the Store.
8. Include detailed information in the single purpose field regarding your extension's primary functionality.
9. Provide meaningful customer support for your extension.
10. Chrome Web Store policies are subject to change. Google may update the policies at any time, and developers are responsible for keeping up-to-date with any changes and complying with the updated policies. Updates to our policies will be announced via email to the address listed in your developer account.

Fostering a Safe Ecosystem

Mature & Sexually Explicit Material

1. We don't allow content that contains nudity, graphic sex acts, sexually explicit material, or content that drives traffic to commercial pornography sites.
2. We also don't allow content that promotes incest, bestiality, necrophilia, or non-consensual sexual acts.
3. Google has a zero-tolerance policy against child pornography. If we become aware of content with child pornography, we will report it to the appropriate authorities and delete the Google accounts of those involved with the distribution.
4. Content which contains non-sexual nudity—such as artistic, educational, scientific, or cultural nudity—is generally allowed, but may impact the visibility of your Product.
5. Products that include content that may not be suitable for all ages should be marked "Mature" on the Developer Dashboard. Items marked as mature will only be available to logged in, adult aged Google Accounts.

Malicious and Prohibited Products

1. Don't transmit viruses, worms, defects, Trojan horses, malware, or any other products of a destructive nature.
2. We don't allow content that harms or interferes with the operation of the networks, servers, or other infrastructure of Google or any third-parties.
3. Spyware, malicious scripts, and phishing scams are also prohibited in the Chrome Web Store.
4. Do not facilitate unauthorized access to content on websites, such as circumventing paywalls or login restrictions.
5. Do not encourage, facilitate, or enable the unauthorized access, download, or streaming of copyrighted content or media.
6. We do not allow the mining of cryptocurrency.

Hate Speech and Violent Behavior

1. Depictions of gratuitous violence are not allowed. Products should not contain materials that threaten, harass, or bully other users.
2. We don't allow content or products that advocating against or inciting hatred towards groups of people based on their race or ethnic origin, religion, disability, gender, age, veteran status, nationality, sexual orientation, gender, gender identity, or any other characteristic that is associated with systematic discrimination or marginalization.
3. We remove products that recruit, fundraise, or promote violence on behalf of extremist groups defined by the US State Department and other international organizations. Violent extremism is defined as the use of violence and intimidation in the pursuit of political aims or goals outside of societal norms.
4. The visibility of your Product may be impacted if it contains generally hateful content not covered by the above definition.

Regulated Goods and Services

1. Don't engage in or promote unlawful activities in your product, such as rape, illegal sex work, or the sale of prescription drugs without a prescription. We will remove content which promotes, glorifies, or encourages dangerous or illegal activity that may result in physical harm to those involved.
2. We don't allow content or services that facilitate or promote real money gambling, including but not limited to online casinos, sports betting, lotteries, or games of skill that offer prizes of cash or other value. Products that simulate gambling but don't offer any opportunity for real money winnings, payouts, or prizes of value may be allowed. However, such products must clearly indicate that no real money is involved and comply with all other applicable policies of the Chrome Web Store.
3. We don't allow the facilitation of the sale of regulated products or services. Regulated goods include pharmaceuticals, alcohol, tobacco, fireworks, weapons, gambling, or health/medical devices.

Protecting User Privacy

Privacy Policy

1. If your Product handles any user data, then you must post an accurate and up to date privacy policy.
2. The privacy policy must, together with any in-Product disclosures, comprehensively disclose:
    a. How your Product collects, uses and shares user data
    b. All parties the user data will be shared with.
3. You must make the policy accessible by providing a link in the designated Chrome Web Store Developer Dashboard field.

For more information on this policy, see the Developer FAQ (/docs/webstore/program-policies/user-data-faq).

Limited Use

1. This policy establishes the Chrome Web Store's minimum user data privacy requirements; you or your Product must comply with applicable laws.
2. You must limit your use of the data to the practices you disclosed.
3. Collection and use of web browsing activity is prohibited, except to the extent required for a user-facing feature described prominently in the Product's Chrome Web Store page and in the Product's user interface.
4. Upon accessing user data for a single purpose, your use of the user data obtained must comply with the below requirements. The requirements apply to both the raw data obtained and the data aggregated, anonymized, de-identified, or derived from the raw data. They also apply to scraped content or otherwise automatically gathered user data.
    a. Limit your use of user data to providing or improving your single purpose
    b. Only transfer user data to third parties
        i. If necessary to providing or improving your single purpose;
        ii. to comply with applicable laws;
        iii. to protect against malware, spam, phishing, or other fraud or abuse; or,
        iv. as part of a merger, acquisition or sale of assets of the developer after obtaining explicit prior consent from the user.
    c. Do not allow humans to read user data, unless:
        i. the user's explicit consent to read specific data (for example, helping a user re-access the product or a service after having lost their password) is obtained;
        ii. The data is aggregated and anonymized and used for internal operations in accordance with applicable privacy and other jurisdictional legal requirements;
        iii. It's necessary for security purposes (e.g., investigating abuse); or,

iv. To comply with applicable laws.

d. All other transfers, uses, or sale of user data is completely prohibited, including:

i. Transferring, using, or selling data for personalized advertisements.

ii. Transferring or selling user data to third parties like advertising platforms, data brokers, or other information resellers.

iii. Transferring, using, or selling user data to determine credit-worthiness or for lending purposes.

5. An affirmative statement that your use of the data complies with the Limited Use restrictions must be disclosed on a website belonging to your extension; e.g., a link on a homepage to a dedicated page or privacy policy noting: "The use of information received from Google APIs will adhere to the Chrome Web Store User Data Policy, including the Limited Use requirements."

Use of Permissions

1. Request access to the narrowest permissions necessary to implement your Product's features or services. If more than one permission could be used to implement a feature, you must request those with the least access to data or functionality. Don't attempt to "future proof" your Product by requesting a permission that might benefit services or features that have not yet been implemented.

Disclosure Requirements

1. You must be transparent in how you handle user data (e.g., information provided by a user or collected about a user or a user's use of the Product or Chrome Browser), including by disclosing the collection, use, and sharing of the data.

2. If your Product handles any user data that is not closely related to the functionality described prominently in the Product's Chrome Web Store page and user interface, then prior to installation, it must:

a. Prominently disclose what user data will be collected and how it will be used

b. Obtain the user's affirmative and informed consent for such use

Handling Requirements

1. If your product is associated with a security vulnerability that could be exploited to compromise another application, service, browser, or system, we may remove your product from the Chrome Web Store and take other measures to protect users. In such an event, you may be contacted about remediation steps required to restore the product. Chrome extension security vulnerabilities can be reported here (https://www.google.com/about/appsecurity/ddprp/).
2. If your product collects any user data, it must handle the user data securely, including transmitting it via modern cryptography.
3. Don't publicly disclose financial or payment information.
4. Keep authentication information secure. Don't publicly disclose authentication information.

Ensuring Responsible Marketing and Monetization

Impersonation & Intellectual Property

1. Don't pretend to be someone else, and don't represent that your product is authorized by, endorsed by, or produced by another company or organization, if that is not the case.
2. Your Product and its user experience also must not mimic functionality or warnings from a user's operating system or browser.
3. Developers should not divert users or provide links to any other site that mimics the Chrome Web Store or passes itself off as the Chrome Web Store.
4. Any metadata that misrepresents the extension's or developer's current status or performance on the Chrome Web Store (e.g. "Editor's Choice" or "Number One") is not

allowed.

5. Don't infringe on the intellectual property rights of others, including patent, trademark, trade secret, copyright, and other proprietary rights. We will respond to clear notices of alleged copyright infringement. For more information or to file a DMCA request, use this tool (http://www.google.com/support/bin/static.py?page=ts.cs&ts=1114905).
6. The visibility of your Product may be impacted if we believe it potentially infringes on intellectual property rights.

Deceptive Installation Tactics

1. Extensions must be marketed responsibly. The set of functionalities promised by the extension must be stated clearly and in a transparent manner. The outcome of any user interaction should match the reasonable expectations that were set with the user. Extensions that use or benefit from deceptive installation tactics will be removed from the Chrome Web Store. Deceptive installation tactics include:
    a. Confusing or deceptive advertisements or marketing materials preceding the installation of your extension. The features of your extension should be clear when marketing your product.
    b. Misleading interactive elements as part of your distribution flow. This includes misleading call-to-action buttons or forms that imply an outcome other than the installation of an extension. Any call-to-action buttons preceding the installation of your extension must state that an extension will be installed.
    c. Adjusting the Chrome Web Store product listing window with the effect of withholding or hiding extension metadata from the user.
    d. Bundling other extensions or offers within the same installation flow.
    e. Requiring unrelated user action to access advertised functionality.

For more information about this policy, see the Developer FAQ (/docs/webstore/program-policies/deceptive-installation-tactics-faq).

Accepting Payment From Users

If you collect sensitive personal information through your Product for sales, you must follow these requirements:

1. You must securely collect, store, and transmit all credit card and other sensitive personal information in accordance with privacy and data security laws and payment card industry rules.
2. You must avoid misleading users. For example, clearly and honestly describe the products or services that you are selling and conspicuously post your terms of sale (including any refund and return policies).
3. If your Product requires the user to pay to obtain basic functionality, you must make that clear in the description that the user sees when choosing whether to install it.
4. You must clearly identify that you, not Google, are the seller of the products or services.
5. Regardless of the method of payment, you may not process payment transactions that are prohibited for Google Checkout under the Google Checkout Seller Terms of Service (http://checkout.google.com/termsOfService?type=Seller). This includes any illegal transaction or the sale or exchange of any illegal or prohibited goods or services, including the prohibited products set forth in the Content Policies for Google Checkout (http://checkout.google.com/seller/content_policies.html).

Misleading or Unexpected Behavior

1. We do not allow products that deceive or mislead users, including in the content, title, description, or screenshots. If any of your product's content, title, icon, description, or screenshots contains false or misleading information, we may remove it.
2. Any changes to device settings must be made with the user's knowledge and consent and be easily reversible by the user.
3. Don't misrepresent the functionality of your product or include non-obvious functionality that doesn't serve the primary purpose of the product. Descriptions of your product must directly state the functionality so that users have a clear

understanding of the product they are adding. For example, products should not contain:

a. Claimed functionalities that are not possible to implement (e.g. "Who has viewed your social media account").

b. Anti-virus, privacy, or security extensions that do not provide any discernible monitoring or protection.

Ads

1. Ads are considered part of your Product for purposes of content review and compliance with developer terms, and therefore must comply with the above content policies.
2. Ads which are inconsistent with the content rating (/docs/webstore/rating) of your products or extension are also in violation of our developer terms.
3. Currently, AdSense may not be used to serve ads in Products, per AdSense policies (https://support.google.com/adsense/bin/answer.py?answer=48182).
4. Ads must be presented in context or clearly state which product they are bundled with.
5. Ads must also be easily removable by either adjusting the settings or uninstalling the product altogether.
6. Ads may not simulate or impersonate system notifications or warnings.
7. Forcing the user to click on ads or submit personal information for advertising purposes in order to fully use an app or extension provides a poor user experience and is prohibited.
8. Ads associated with your product may not interfere with any ads on a third-party website or application. You may show ads alongside a third-party website only if all of the following criteria are met:

    a. This behavior is clearly disclosed to the user.

    b. There is clear attribution of the ads' source wherever those ads appear.

c. The ads do not interfere with any native ads or functionality of the website.

d. The ads do not mimic or impersonate the native ads or content on the third-party website, and the ads adhere to the content policy on impersonation (/docs/webstore/program-policies/impersonation-and-intellectual-property) and misleading behavior (/docs/webstore/program-policies/unexpected-behavior).

Affiliate Ads

1. Any affiliate program must be described prominently in the product's Chrome Web Store page, user interface, and before installation.
2. Affiliate links, codes, or cookies must only be included when the extension provides a direct and transparent user benefit related to the extension's core functionality. It is not permitted to inject affiliate links without related user action and without providing a tangible benefit to users. Some common violations include:
   a. Inserting affiliate links when no discount, cashback, or donation is provided.
   b. An extension that continuously injects affiliate links in the background without related user action.
3. Related user action is required before the inclusion of each affiliate code, link, or cookie. Some example violations include:
   a. An extension that updates a shopping-related cookie without the user's knowledge while the user is browsing shopping sites.
   b. An extension that appends an affiliate code to the URL or replaces an existing affiliate code in the URL without the user's explicit knowledge or related user action.
   c. An extension that applies or replaces affiliate promo codes without the user's explicit knowledge or related user action.

Building Quality Products

Feature Products

1. The Chrome Web Store features products that align with our standards, values, and that we believe will produce valuable user experiences. Certain products that don't meet these standards, but which do not explicitly violate Chrome Web Store policies—such as VPN extensions and video downloaders—may be restricted from feature in the store, but will still be available to users. For example, the following products are currently not featured in the Chrome Web Store:
    a. Religious or political content
    b. VPNs
    c. Video downloaders
    d. Anti-virus tools
    e. Content deemed not family friendly
    f. Bots
    g. Cryptocurrency
    h. Non-production builds
    i. Prohibited products
    j. Gambling content
    k. Extensions whose developers have questionable reputations, such as historically misleading or malicious extensions.

For information about Product ranking, see these FAQs (/docs/webstore/faq#faq-gen-24).

Spam and Abuse

1. We don't allow any developer, related developer accounts, or their affiliates to submit multiple extensions that provide duplicate experiences or functionality on the Chrome Web Store. Extensions should provide value to users through the creation of unique content or services.

2. Developers must not attempt to manipulate the placement of any extensions in the Chrome Web Store. This includes, but is not limited to, inflating product ratings, reviews, or install counts by illegitimate means, such as fraudulent or incentivized downloads, reviews and ratings.
3. We do not allow extensions that abuse, or are associated with abuse, of notifications by sending spam, ads, promotions, phishing attempts, or unwanted messages that harm the user's browsing experience.
4. We don't allow extensions that send messages on behalf of the user without giving the user the ability to confirm the content and intended recipients.
5. In addition to these requirements, all extensions must comply with Google's Webmaster Quality Guidelines (https://support.google.com/webmasters/answer/35769#3).

For additional information about the spam policy, see the Spam FAQ (/docs/webstore/program-policies/spam-faq).

Quality Guidelines

1. An extension must have a single purpose that is narrow and easy to understand. Don't create an extension that requires users to accept bundles of unrelated functionality. If two pieces of functionality are clearly separate, they should be put into two different extensions, and users should have the ability to install and uninstall them separately. Common violations include:
    a. Functionality that displays product ratings and reviews, but also injects ads into web pages.
    b. Toolbars that provide a broad array of functionality or entry points into services are better delivered as separate extensions, so that users can select the services they want.
    c. Email notifiers combined with a news aggregator.
    d. New Tab Page extensions that alter the user's web search experience and don't respect the user's existing search settings.

2. When designing an extension, it's important to ensure it functions as a helpful companion to users' browsing experiences by providing complementary functionality. If utilizing a persistent user interface, extensions should actively enhance the user's current task while causing minimal distractions. Some common violations include:
    a. Side panel extensions which hijack a user's browsing or search experience.
    b. Extensions with the primary purpose of serving ads.

See this FAQ (/docs/webstore/program-policies/quality-guidelines-faq) for more information.

Listing Requirements

1. If your product has a blank description field or is missing an icon or screenshots, it will be rejected.
2. Ensure your product's listing information is up to date, accurate, and comprehensive. We don't allow extensions with misleading, inaccurate, incomplete, improperly formatted, non-descriptive, out of date, or inappropriate metadata, including but not limited to the extension's description, category, developer name, title, icon, screenshots, and promotional images.
3. All information provided in the privacy fields (/docs/webstore/cws-dashboard-privacy) of your extension must be up to date and accurate. If the information listed in your privacy fields contradicts the information provided in your privacy policy, or the behavior of your extension, your extensions may be removed from the Store.
4. Keyword Spam is the practice of including irrelevant or excessive keywords in an extensions description in an attempt to manipulate its ranking, resulting in a spammy, negative user experience. We don't allow extensions with irrelevant or excessive metadata. Developers should focus on providing a clear and well-written description that uses keywords appropriately and in context. Some examples of Keyword Spam include:
    a. Lists of sites/brands/keywords without substantial added value
    b. Lists of regional locations

    c. Unnatural repetition of the same keyword more than 5 times

5. We don’t allow unattributed or anonymous user testimonials in the product's description.

Minimum Functionality

1. Do not post an extension with a single purpose of installing or launching another app, theme, webpage, or extension.
2. Extensions with broken functionality—such as dead sites or non-functioning features—are not allowed.
3. Extensions must provide a basic degree of functionality and utility that provide value to the catalog of the Chrome Web Store. Some examples of common violations include:
    a. Extensions with no functionality or utility.
    b. Extensions with functionality that is not directly provided by the extension (e.g. file converters which only link to other file conversion services).
    c. Click-baity template extensions that only vary slightly in functionality with negligible utility (e.g. a “Word of the Day” extension and a “Daily Inspirational Quotes” extension, which use the same general extension template).

Chrome Apps

To ensure a great user experience, Chrome Apps distributed through the Chrome Web Store must follow the additional quality guidelines listed below. The guidelines in this section apply only to Chrome Apps.

1. Packaged apps should:
    a. Take advantage of the capabilities of the platform and not wrap around existing websites or simply launch a webpage without providing additional functionality.
    b. Detect an offline state and clearly message that state to the user.

c. Recover automatically from loss of internet connectivity, and should resume normal functioning when connectivity is restored without the user having to restart the app.

2. Packaged and hosted apps should not:

   a. Require a local executable, other than the Chrome runtime, to run.

   b. Provide a WebView of a website that is not owned or administered by you.

   c. Download or execute scripts dynamically outside a sandboxed environment such as a WebView or a sandboxed iframe.

   d. Misuse notifications by sending spam, ads, promotions of any kind, phishing attempts, or unwanted messages in general.

Technical Requirements

Code Readability Requirements

1. Developers must not obfuscate code or conceal functionality of their extension. This also applies to any external code or resource fetched by the extension package. Minification is allowed, including the following forms:

   a. Removal of whitespace, newlines, code comments, and block delimiters

   b. Shortening of variable and function names

   c. Collapsing files together

API Use

1. Extensions must use existing Chrome APIs for their designated use case. Use of any other method, for which an API exists, would be considered a violation. For example, overriding the Chrome New Tab Page through any means other than the URL Overrides API is not permitted.

Additional Requirements for Manifest V3

1. Extensions using Manifest V3 must meet additional requirements related to the extension's code. Specifically, the full functionality of an extension must be easily discernible from its submitted code, unless otherwise exempt as noted in Section 2. This means that the logic of how each extension operates should be self contained. The extension may reference and load data and other information sources that are external to the extension, but these external resources must not contain any logic. Some common violations include:

    a. Including a <script> tag that points to a resource that is not within the extension's package

    b. Using JavaScript's `eval()` (https://developer.mozilla.org/docs/Web/JavaScript/Reference/Global_Objects/eval) method or other mechanisms to execute a string fetched from a remote source

    c. Building an interpreter to run complex commands fetched from a remote source, even if those commands are fetched as data

2. Execution of logic from a remote source is permissible only when accomplished through a documented API that explicitly allows this practice and the use is inline with the documented purpose of the API, as detailed in the API Use policy (/docs/webstore/program-policies/api-use). The permitted APIs for such remote execution are:

    a. Debugger API (/docs/extensions/reference/api/debugger)

    b. User Scripts API (/docs/extensions/reference/api/userScripts)

    Note that exemptions apply solely to the specific section of code covered by these APIs. Extensions may still be in violation of this policy if they employ alternative methods to execute logic from remote sources elsewhere in their code.

    Additionally, code run in contexts that are isolated from extension APIs (such as iframes and sandboxed pages) are exempt from the restriction on loading code from remote sources; however, these are treated similarly to our policy on communication with

external servers. That is, it must still be possible to determine the full functionality of your extension and the interaction must still comply with our user data policies, including Limited Use (/docs/webstore/program-policies/limited-use) and the extension's Privacy Policy (/docs/webstore/program-policies/privacy).

3. Communicating with remote servers for certain purposes is still allowed. For instance:
    a. Syncing user account data with a remote server
    b. Fetching a remote configuration file for A/B testing or determining enabled features, where all logic for the functionality is contained within the extension package
    c. Fetching remote resources that are not used to evaluate logic, such as images
    d. Performing server-side operations with data (such as for the purposes of encryption with a private key)
4. If we are unable to determine the full functionality of your extension during the review process, we may reject your submission or remove it from the store.

2-Step Verification

1. To ensure the security of Chrome Web Store accounts, 2-Step Verification is required for all developer accounts prior to publishing an extension or updating an existing extension. Developers can activate 2-Step Verification for their Google accounts here (https://myaccount.google.com/security/signinoptions/two-step-verification/enroll-welcome). More information on Google's 2-Step Verification features can be found here (https://www.google.com/landing/2step/).

Enforcement

Enforcement Circumvention

1. Any attempt to circumvent intended limitations or enforcement actions will result in the immediate termination of your developer account, and possibly related developer accounts.

Notification and Appeals

1. In the event that your Product is removed from the Chrome Web Store, you will receive an email notification to that effect, with further instructions if applicable.
2. Verify that the associated publisher account with your Product can receive emails from external parties and not get flagged as Spam to ensure that you receive all communications in a timely manner.
3. Removals are permanent unless you submit a revision to fix the issue. Enforcement actions are applied globally by default. If your enforcement action is subject to a territorial restriction, you will be notified of that fact.
4. Developers are permitted to appeal a violation decision once. After the appeal has been reviewed and a decision rendered, no further appeals will be accepted for the same violation.
5. Developers are encouraged to submit good faith appeals. Any attempts to submit frivolous appeals or misuse the appeal process may result in further action, including the forfeiture of future appeal rights.

Repeat Abuse

1. Serious or repeated violations of the Chrome Web Store Distribution Agreement or these Program Policies will result in the suspension of your developer account, and possibly related developer accounts. Additionally, you may be banned from using the Chrome Web Store. In extreme cases, this may also result in the suspension of related Google services associated with your Google account.
2. Repeated infringement of intellectual property rights, including copyright, will also result in account termination. For more information on Google's copyright policies, please use this tool (http://www.google.com/support/bin/static.py?page=ts.cs&ts=1114905).

Last updated 2025-05-22 UTC.