Microsoft Store Policies

12/16/2020 • 23 minutes to read •

In this article

Document version: 7.12

Document date: October 1, 2019

> **Note**
>
> For a summary of recent changes to this agreement, see **Change history**.

> **Note**
>
> **Dec 16, 2020 Policy Update Notice**: For game products targeting console developed through the **Xbox Live Creators program** , the requirement to integrate with XBL Services no longer applies. The specific policy (**Policy 10.13.1**) will be updated to reflect this change the next time the Store Policy document is updated, but effective as of this notice, the policy will no longer be enforced for the XBL Creators Program.

Thank you for your interest in developing products for the Microsoft Store[1]. "Product" means content in whatever form submitted including, but not limited to, apps, games, titles, and any additional content sold or offered from within a Product. We're committed to a diverse catalog of products for customers worldwide. Products on the Store must meet our certification standards, offer customers a truly useful and engaging experience, and provide a good fit for the Store.

A few principles to get you started:

- Offer unique and distinct value within your product. Provide a compelling reason to download your product from the Store.
- Don't mislead our joint customers about what your product can do, who is offering it, etc.

- Don't attempt to cheat customers, the system or the ecosystem. There is no place in our Store for any kind of fraud, be it ratings and review manipulation, credit card fraud or other fraudulent activity.

Adhering to these policies should help you make choices that enhance your product's appeal and audience.

Your products are crucial to the experience of hundreds of millions of customers. We can't wait to see what you create and are thrilled to help deliver your products to the world.

If you have feedback on the policies, please let us know by commenting in our forum . We will consider every comment.

Table of Contents

Product Policies:

Content Policies:

Product Policies

10.1 Distinct Function & Value; Accurate Representation

Your product and its associated metadata must accurately and clearly reflect the source, functionality, and features of your product.

10.1.1

All aspects of your product should accurately describe the functions, features and any important limitations of your product, including required or supported input devices. The value proposition of your product must be clear during the first run experience. Your product may not use a name or icon similar to that of other products, and may not claim to be from a company, government body, or other entity if you do not have permission to make that representation. Products submitted as web apps must be published by the domain or website owner.

10.1.2

Your product must be fully functional and must provide appropriate functionality for targeted systems and devices.

10.1.3

Search terms may not exceed seven unique terms and should be relevant to your product.

10.1.4

Your product must have distinct and informative metadata and must provide a valuable and quality user experience. Your product must also have an active presence in the Store.

10.1.5

Your app may promote or distribute software only through the Microsoft Store.

10.2 Security

Your product must not jeopardize or compromise user security, or the security or functionality of the device, system or related systems.

10.2.1

Products that browse the web must use the appropriate HTML and JavaScript engines provided by the Windows Platform.

10.2.2

Your product must not attempt to change or extend its described functionality through any form of dynamic inclusion of code that is in violation of Store Policies. Your product should not, for example, download a remote script and subsequently execute that script in a manner that is not consistent with the described functionality.

10.2.3

Your product must not contain or enable malware as defined by the Microsoft criteria for Unwanted and Malicious Software.

10.2.4

Your product may contain fully integrated middleware (such as third-party cross-platform engines and third-party analytics services), but must not deliver or install non-integrated third-party owned or branded products or modules unless they are fully contained in your package.

Your product may depend on non-integrated software (such as another product, module, or service) to deliver its primary functionality, subject to the following requirements:

- You disclose the dependency at the beginning of the description metadata
- The dependent software is available in the Store

10.2.5

All of your product and in-product offerings that are available to acquire from the Store must be installed and updated only through the Store.

10.2.6

Apps that enable the mining of crypto-currency on device are not allowed. Apps that enable remote management of the mining of cryptocurrency are allowed.

10.3 Product is Testable

The product must be testable. If it is not possible to test your product for any reason, including, but not limited to, the items below, your product may fail this requirement.

10.3.1

If your product requires login credentials, provide us with a working demo account using the **Notes for certification** field.

10.3.2

If your product requires access to a server, the server must be functional to verify that it's working correctly.

10.4 Usability

Your product must meet Store standards for usability, including, but not limited to, those listed in the subsections below.

10.4.1

Products should support the devices and platforms on which they are downloaded, including compatibility with the software, hardware and screen resolution requirements specified by the product. If a product is downloaded on a device with which it is not compatible, it should detect that at launch and display a message to the customer detailing the requirements.

10.4.2

Products must continue to run and remain responsive to user input. Products must shut down gracefully and not close unexpectedly. The product must handle exceptions raised by any of the managed or native system APIs and remain responsive to user input after the exception is handled.

10.4.3

The product must start up promptly and must stay responsive to user input.

10.4.4

Where applicable, pressing the back button should take the user to a previous page/dialog.

10.5 Personal Information

The following requirements apply to products that access Personal Information. Personal Information includes all information or data that identifies or could be used to identify a person, or that is associated with such information or data.

10.5.1

If your product accesses, collects or transmits Personal Information, or if otherwise required by law, you must maintain a privacy policy. You must provide users with access to your privacy policy by entering the privacy policy URL in Partner Center when you submit your product. In addition, you may also include or link to your privacy policy in the product. The privacy policy can be hosted within or directly linked from the product. Your privacy policy must inform users of the Personal Information accessed, collected or transmitted by your product, how that information is used, stored and secured, and indicate the types of parties to whom it is disclosed. It must describe the controls that users have over the use and sharing of their information and how they may access their information, and it must comply with applicable laws and regulations. Your privacy policy must be kept up-to-date as you add new features and functionality to your product.

Product types that inherently have access to Personal Information must always have privacy policies. These include, but are not limited to, Edge Extension and Desktop Bridge products.

10.5.2

You may publish the Personal Information of customers of your product to an outside service or third party through your product or its metadata only after obtaining opt-in consent from those customers. Opt-in consent means the customer gives their express permission in the product user interface for the requested activity, after you have:

- described to the customer how the information will be accessed, used or shared, indicating the types of parties to whom it is disclosed, and
- provided the customer a mechanism in the product user interface through which they can later rescind this permission and opt-out.

10.5.3

If you publish a person's Personal Information to an outside service or third party through your product or its metadata, but the person whose information is being shared is not a customer of your product, you must obtain express written consent to publish that Personal Information, and you must permit the person whose information is shared to

withdraw that consent at any time. If your product provides a customer with access to another person's Personal Information, this requirement would also apply.

10.5.4

If your product collects, stores or transmits Personal Information, it must do so securely, by using modern cryptography methods.

10.5.5

Your product must not collect, store or transmit highly sensitive personal information, such as health or financial data, unless the information is related to the product's functionality. Your product must also obtain express user consent before collecting, storing or transmitting such information. Your product's privacy policy must clearly tell the user when and why you are collecting Personal Information and how you will use it.

10.5.6

If your product supports Microsoft identity authentication it must do so only by using Microsoft-approved methods.

10.5.7

Products that receive device location must provide settings that allow the user to enable and disable the product's access to and use of location from the Location Service API. For Windows Phone 8 and Windows Phone 8.1 products, these settings must be provided in-product. For Windows Mobile 10 products, these settings are provided automatically by Windows within the Settings App (on the **Settings** > **Privacy** > **Location** page). You must respect such settings, and if you choose to collect device location data in another way, such data is Personal Information and collection is subject to the other requirements of section 10.5. You must gain legally sufficient consent for your data practices, and such practices must generally comply with applicable laws and regulations.

10.6 Capabilities

The capabilities you declare must legitimately relate to the functions of your product, and the use of those declarations must comply with our product capability declarations. You must not circumvent operating system checks for capability usage.

10.7 Localization

You must localize your product for all languages that it supports. The text of your product's description must be localized in each language that you declare. If your product is localized such that some features are not available in a localized version, you must clearly state or display the limits of localization in the product description. The experience provided by a product must be reasonably similar in all languages that it supports.

10.8 Financial Transactions

If your product includes in-product purchase, subscriptions, virtual currency, billing functionality or captures financial information, the following requirements apply:

10.8.1

You must use the Microsoft Store in-product purchase API to sell digital items or services that are consumed or used within your product. Your product may enable users to consume previously purchased digital content or services, but must not direct users to a purchase mechanism other than the Microsoft Store in-product purchase API.

In-product offerings sold in your product cannot be converted to any legally valid currency (for example, USD, Euro, etc.) or any physical goods or services.

10.8.2

You must use the Microsoft payment request API or a secure third party purchase API for purchases of physical goods or services, and a secure third party purchase API for payments made in connection with real world gambling or charitable contributions. If your product is used to facilitate or collect charitable contributions or to conduct a promotional sweepstakes or contest, you must do so in compliance with applicable law. You must also state clearly that Microsoft is not the fundraiser or sponsor of the promotion.

You must use the Microsoft payment request API or a secure third party purchase API to receive voluntary donations from users. If the user receives digital goods or services in return, including but not limited to additional features or removal of advertising, you must use the Microsoft Store in-product purchase API instead.

The following requirements apply to your use of a secure third party purchase API:

- At the time of the transaction or when you collect any payment or financial information from the customer, your product must identify the commerce transaction provider, authenticate the user, and obtain user confirmation for the transaction.
- The product can offer the user the ability to save this authentication, but the user must have the ability to either require an authentication on every transaction or to

turn off in-product transactions.
- If your product collects credit card information or uses a third-party payment processor that collects credit card information, the payment processing must meet the current PCI Data Security Standard (PCI DSS).

10.8.3

If your product requires financial account information, you must submit that product from a company account type.

10.8.4

Your product and its associated metadata must provide information about the types of in-product purchases offered and the range of prices. You may not mislead customers and must be clear about the nature of your in-product promotions and offerings including the scope and terms of any trial experiences. If your product restricts access to user-created content during or after a trial, you must notify users in advance. In addition, your product must make it clear to users that they are initiating a purchase option in the product.

If your game offers "loot boxes" or other mechanisms that provide randomized virtual items, then you must disclose the odds of receiving each item to customers prior to purchase. These disclosures may appear: in-product, such as in an in-app store, on the Microsoft Store Product Description Page (PDP), and/or on a developer or publisher website, with a link from the Store Product Description Page (PDP) and/or in-app.

10.8.6

You must use the Microsoft recurring billing API to bill for subscriptions of digital goods or services, and the following guidelines apply:

- You may add value to a subscription but may not remove value for users who have previously purchased it.
- If you discontinue an active subscription, you must continue to provide purchased digital goods or services until the subscription expires.

10.8.7

All pricing, including sales or discounting, for your digital products or services shall comply with all applicable laws, regulations and regulatory guidelines, including without limitation, the Federal Trade Commission Guides Against Deceptive Pricing .

10.9 Notifications

Your product must respect system settings for notifications and remain functional when they are disabled. This includes the presentation of ads and notifications to the customer, which must also be consistent with the customer's preferences, whether the notifications are provided by the Microsoft Push Notification Service (MPNS), Windows Push Notification Service (WNS) or any other service. If the customer disables notifications, either on an product-specific or system-wide basis, your product must remain functional.

If your product uses MPNS or WNS to transmit notifications, it must comply with the following requirements:

10.9.1

Because notifications provided through WNS or MPNS are considered product content, they are subject to all Store Policies.

10.9.2

You may not obscure or try to disguise the source of any notification initiated by your product.

10.9.3

You may not include in a notification any information a customer would reasonably consider to be confidential or sensitive.

10.9.4

Notifications sent from your product must relate to the product or to other products you publish in the Store catalog, may link only to the product or the Store catalog listing of your other products, and may not include promotional messages of any kind that are not related to your products.

10.10 Advertising Conduct and Content

For all advertising related activities, the following requirements apply:

10.10.1

- The primary purpose of your product should not be to get users to click ads.
- Your product may not do anything that interferes with or diminishes the visibility, value, or quality of any ads it displays.
- Your product must respect advertising ID settings that the user has selected.

- All advertising must be truthful, non-misleading and comply with all applicable laws, regulations, and regulatory guidelines.

10.10.2

If you purchase or create promotional ad campaigns to promote your products through the ad campaign functionality in Partner Center, all ad materials you provide to Microsoft, including any associated landing pages, must comply with Microsoft's Creative Specifications Policy and Creative Acceptance Policy .

10.10.3

Any advertising content your product displays must adhere to Microsoft's Creative Acceptance Policy .

If your product displays ads, all content displayed must conform to the advertising requirements of the App Developer Agreement, including the following requirements:

10.10.4

The primary content of your product may not be advertising, and advertising must be clearly distinguishable from other content in your product.

10.10.5

Your privacy statement or terms of use must let users know you will send Personal Information to the ad service provider and must tell users how they can opt-out of interest-based advertising.

10.10.6

If your product is directed at children under the age of 13 (as defined in the Children's Online Privacy Protection Act), you must notify Microsoft of this fact in Partner Center and ensure that all ad content displayed in your product is appropriate for children under the age of 13.

10.11 Mobile Voice Plans

Your product may not sell, link to, or otherwise promote mobile voice plans.

10.12 Edge Extensions

Edge Extensions are subject to these additional requirements:

- Your Extension must have a single purpose with narrowly scoped functionality that is clearly explained in the product description.
- Your Extension may collect Personal Information only as part of a prominently disclosed, user-facing feature.
- If your Extension collects web browsing activity, it must do so only if required by and only for use in a prominently disclosed, user-facing feature.
- The Extension must not programmatically alter, or appear to alter, browser functionality or settings including, but not limited to: the address bar search provider and suggestions, the start or home page, the new tab page, and adding or removing favorites and reading list items.

10.13 Gaming and Xbox

For products that are primarily gaming experiences or target Xbox One, the following requirements apply:

10.13.1

Game products, including products that primarily offer remote game play/control functionality of games running on other devices or platforms, that target Xbox One must use Xbox Live services through either the Xbox Live Creators or ID@Xbox program.

10.13.2

Game products that allow cross-player communication or synchronous network play on Xbox One devices must use Xbox Live and be approved through the ID@Xbox program.

10.13.3

Game products on Xbox One must not present an alternate friends list obtained outside Xbox Live.

10.13.4

Products published to Xbox One must not:

- Include the sale of Xbox game products, Xbox consoles or Xbox console accessories outside the Store.
- Request or store Microsoft Account usernames or passwords.

10.13.5

Game products that use Xbox Live must:

- Automatically sign the user in to Xbox Live, or offer the user the option to sign in, before gameplay begins.
- Display the user's Xbox gamertag as their primary display and profile name.

10.13.6

Game products that use Xbox Live and offer multiplayer gameplay, user generated content or user communication:

- Must not allow gameplay until the user signs in to Xbox Live.
- Must respect parental and service controls.

10.13.7

Game products must gracefully handle errors with or disconnection from the Xbox Live service. When attempting to retry a connection request following a failure, game products must honor the retry policies set by Xbox Games. When they are unable to retrieve configuration information for or communicate with any non-Microsoft service, game products must not direct users to Microsoft support.

10.13.8

Game products must not store user information sourced from Xbox Live, such as profile data, preferences, or display names, beyond a locally stored cache used to support loss of network connectivity. Any such caches must be updated on the next available connection to the service.

10.13.9

Xbox Live game products must comply with the following requirements for service usage:

- Do not link or federate the Xbox Live user account identifier or other user account data with other services or identity providers.
- Do not provide services or user data in a way that it could be included in a search engine or directory.
- Keep your secret key and access tokens private, except if you share them with an agent acting to operate your product and the agent signs a confidentiality agreement.
- Do not duplicate the Xbox Live Friends service.

10.13.10

Products that emulate a game system are not allowed on any device family.

10.13.11

The following privacy requirements apply to Xbox Live user data:

- Services and user data are only for use in your game by you. Don't sell, license, or share any data obtained from us or our services. If you receive personal data of end users through Xbox Live, you are an independent controller of such data and must have a privacy statement (or policy) in place with end users governing your use of personal data, as required by the App Developer Agreement. We recommend you include a link to your privacy statement on your website and on the Microsoft Store pages for your games.
- Services and user data must be used appropriately in games. This data includes (without limitation) usage data, account identifiers and any other personally identifiable data, statistics, scores, ratings, rankings, connections with other users, and any other data relating to a user's social activity.
- Don't store any Xbox Live social graph data (for example, friends lists), except for account identifiers for users who've linked their Xbox Live account with your game.
- Delete all account identifiers, when you remove your game from our service, or when a user unlinks their Xbox Live account from your game. Do not share services or user data (even if anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.
- When Microsoft receives requests from end users to delete their personal data, we will communicate the requests to you by providing a list of end user identifiers. You must check the list at least every 30 days to ensure you receive all delete requests and must use the information provided on the list only to satisfy the delete requests of end users. You can find details about this process at Deleted Account List Tools .

10.14 Account Type

If a reasonable consumer would interpret your publisher account name to be that of a business entity, you must publish from a company account type, not an individual account type.

Content Policies

The following policies apply to content and metadata (including publisher name, product name, product icon, product description, product screenshots, product trailers and trailer

thumbnails, and any other product metadata) offered for distribution in the Store. Content means the product name, publisher name, product icon, product description, the images, sounds, videos and text contained in the product, the tiles, notifications, error messages or ads exposed through your product, and anything that's delivered from a server or that the product connects to. Because product and the Store are used around the world, these requirements will be interpreted and applied in the context of regional and cultural norms.

11.1 General Content Requirements

Metadata and other content you submit to accompany your product may contain only content that would merit a rating of PEGI 12, ESRB EVERYONE 10+, or lower.

11.2 Content Including Names, Logos, Original and Third Party

All content in your product and associated metadata must be either originally created by the application provider, appropriately licensed from the third-party rights holder, used as permitted by the rights holder, or used as otherwise permitted by law.

11.3 Risk of Harm

11.3.1

Your product must not contain any content that facilitates or glamorizes the following real world activities: (a) extreme or gratuitous violence; (b) human rights violations; (c) the creation of illegal weapons; or (d) the use of weapons against a person, animal, or real or personal property.

11.3.2

Your product must not: (a) pose a safety risk to, nor result in discomfort, injury or any other harm to end users or to any other person or animal; or (b) pose a risk of or result in damage to real or personal property. You are solely responsible for all product safety testing, certificate acquisition, and implementation of any appropriate feature safeguards. You will not disable any platform safety or comfort features, and you must include all legally required and industry-standard warnings, notices, and disclaimers in your product.

11.4 Defamatory, Libelous, Slanderous and Threatening

Your product must not contain any content that is defamatory, libelous, slanderous, or threatening.

11.5 Offensive Content

Your product and associated metadata must not contain potentially sensitive or offensive content. Content may be considered sensitive or offensive in certain countries/regions because of local laws or cultural norms. In addition, your product and associated metadata must not contain content that advocates discrimination, hatred, or violence based on considerations of race, ethnicity, national origin, language, gender, age, disability, religion, sexual orientation, status as a veteran, or membership in any other social group.

11.6 Alcohol, Tobacco, Weapons and Drugs

Your product must not contain any content that facilitates or glamorizes excessive or irresponsible use of alcohol or tobacco products, drugs, or weapons.

11.7 Adult Content

Your product must not contain or display content that a reasonable person would consider pornographic or sexually explicit.

11.8 Illegal Activity

Your product must not contain content or functionality that encourages, facilitates or glamorizes illegal activity in the real world.

11.9 Excessive Profanity and Inappropriate Content

- Your product must not contain excessive or gratuitous profanity.
- Your product must not contain or display content that a reasonable person would consider to be obscene.

11.10 Country/Region Specific Requirements

Content that is offensive in any country/region to which your product is targeted is not allowed. Content may be considered offensive in certain countries/regions because of local

laws or cultural norms. Examples of potentially offensive content in certain countries/regions include the following:

China

- Prohibited sexual content
- Disputed territory or region references
- Providing or enabling access to content or services that are illegal under applicable local law

11.11 Age Ratings

You must obtain an age rating for your product when you submit it in Partner Center. You are responsible for accurately completing the rating questionnaire to obtain the appropriate rating.

11.11.3

If your product provides content (such as user-generated, retail or other web-based content) that might be appropriate for a higher age rating than its assigned rating, you must enable users to opt in to receiving such content by using a content filter or by signing in with a pre-existing account.

11.12 User Generated Content

User generated content is content that users contribute to an app or product and which can be viewed or accessed by some or all users. If your product contains UGC, you must

- Publish and make available to users product terms of service and/or content guidelines
- Provide a means for users to report inappropriate content within the product

---

[1]"Store" or "Microsoft Store" means a Microsoft owned or operated platform, however named, through which Apps may be offered to or acquired by Customers. Unless otherwise specified, Store includes the Microsoft Store, the Windows Store, the Xbox Store, Microsoft Store for Business, and Microsoft Store for Education.

See also

- Change history for Microsoft Store Policies

- Microsoft Store Policies and Code of Conduct
- App Developer Agreement

Is this page helpful?

Yes No