

Windows® Marketplace for Mobile Application Policies (Updated February 2010)

To protect the Windows® Marketplace for Mobile service and users of the service, and to address mobile operator requirements, Microsoft has established the following policies for applications offered for distribution in the Windows® Marketplace for Mobile. Microsoft reserves the right to update these policies as needed.

1. Applications may contain a static URL for the Application Provider's top-level website. Applications may not promote or link users to a website, or contain functionality within the application itself, which encourages or requires the user to purchase or pay to upgrade the application outside of Windows® Marketplace for Mobile.
2. Applications may not consist of, distribute, link to, incent users to download, or otherwise promote alternate marketplaces for content types (applications, games, themes etc.) that are offered through Windows® Marketplace for Mobile.
3. Applications may not sell, link to, or otherwise promote mobile voice plans.
4. Applications may enable Voice over IP (VoIP) services over WiFi. Applications may also enable VoIP over a mobile operator network unless specifically prohibited by the applicable mobile operator.
5. Applications may include or display advertising, *provided that* the advertising (a) complies with the Microsoft Advertising Creative Acceptance Policy Guide (available at <http://advertising.microsoft.com/creative-specs>), and (b) does not include any downloadable file(s).
6. Applications may include dialing, SMS, or MMS functionality, *provided that* the application does not remove or replace the *default* dialer, SMS, or MMS interface on the device.
7. Applications may include web browsing, online search, or media playback functionality, *provided that* the application does not remove or replace the *default* browser, search client, or media player on the device.
8. The OTA (over the air) installation file for the application must not exceed 10MB.
9. Applications may not run code outside Microsoft runtimes (native, managed, and widgets).
10. Applications that publish a user's location information to any other person must first obtain the user's express permission (opt-in) to do so and must provide a mechanism through which the user can opt out of having location information published.
11. Applications that publish a user's data from the mobile device to any other person must first obtain the user's express permission (opt-in) to do so and must provide a mechanism through which the user can opt out of having data published. A "user's data" includes, without limit, contacts, photos, phone number, SMS or other text communication, browsing history, location information, and other data either stored on the mobile device or stored on a web-based server but accessible from the mobile device.
12. Applications that use SMS, MMS or other mobile services that may result in data or messaging charges for the user must, during the application's first run experience, notify the user that additional charges may apply for use of the application.

13. Applications that enable social networking, chat, instant messaging, or other person-to-person communication must require that each user have a unique ID. If the application allows for ID setup or creation from the mobile device, the application must include a mechanism to verify that the user creating the ID is at least 13 years old.
14. Applications that require the download of significant data (>50MB) to run as described in the product description must, in the application description, disclose the size of the data download required to function. If the data download is initiated by the application, the application must, before the download, notify the user of the size of the download and that additional charges may apply.
15. Applications must not jeopardize the security of (a) the mobile device or (b) the Windows® Marketplace for Mobile.