Comcast Acceptable Use Policy for Comcast Business Services

Effective date: April 1, 2026

This Acceptable Use Policy (this "Policy") applies to all users of Comcast Business connectivity or internet services (including but not limited to Comcast-provided Wi-Fi Internet service and Ethernet services) (collectively, "Internet"); Comcast Business Mobile cellular phone services ("Mobile"); and any other Comcast Business service which terms indicate this Policy applies (collectively, the "Services"). This Policy explains how you may use the Services and is in addition to any other service-specific customer agreements that apply. For the avoidance of doubt, all references in this Policy to "Comcast" and "Comcast Business" refer to the subsidiary or affiliate of Comcast Cable Communications Management, LLC that provides the Services to your business, and such subsidiary or affiliate may provide the Services under the Comcast Business, Masergy, or Nitel brand. The specific entity providing Services to you is identified in your service agreement with Comcast.

Who Must Follow This Policy

All Comcast customers are responsible for complying with this Policy and for the actions of anyone who uses your Services, devices, or network with or without your permission.

Commercial, Non-Residential Use Only

The Services are intended only for commercial, non-residential use. Except as expressly permitted in your service agreement with Comcast, you may not (i) resell the Services to any other person; (ii) offer, share, provide access to, sell, resell, sublease, assign, license, or sublicense any of the Services or otherwise make available to anyone outside your service location(s) the ability to use the Services, in whole or in part, directly or indirectly; or (iii) make the Service available to any person or third party for use within a residential unit at the service location(s) at which you receive the Services. It is not a violation of this Policy for you to make the Services available to your authorized employees, contractors or to other users (i.e., the public, customers of an establishment or hotel or motel guests and patrons) in the common or public areas of the site at which you receive the Services, so long as such use does not violate the terms and conditions of your service agreement with Comcast.

Prohibited Uses

The following are examples of prohibited uses of the Services (each, a "Prohibited Use" and collectively, the "Prohibited Uses"), which may lead to suspension and/or termination of your Services with or without prior notice. Comcast may, in its sole discretion, determine whether any activity is a Prohibited Use.

- Conducting illegal, harmful, or infringing activities (for example, breaking or encouraging breaking the law; infringing copyrights or other intellectual property, privacy or other rights of Comcast or third parties; impersonating other persons or entities; posting, storing, sending, transmitting, disseminating, soliciting or sharing unlawful, defamatory, obscene, fraudulent, exploitative, harassing or threatening information, content, or other material or that incites violence, bigotry or hatred or which a reasonable person could deem to be unlawful).

- Engaging in security violations or network interference (for example, accessing accounts or devices without permission; bypassing authentication; vulnerability scanning; use of hacking tools or other tools used to compromise security; distributing malware; falsifying message headers or network references; denial-of-service or similar attacks; other activities that diminish the use or enjoyment of the Services by others).
- Sending or facilitating unsolicited, bulk, deceptive, or automated communications (for example, spam emails or messages; auto-dialers or robocalls; "blast" messaging; falsified headers or sender information; phishing or other fraudulent schemes; harvesting addresses or identifiers without consent; or engaging in impersonation, phishing, or signature forgery).
- Misusing voice Services (for example, operating call centers, conference bridges, or chat lines; telemarketing (including for charitable, political, or polling solicitation), advertising or commercial solicitation to a person in violation of applicable law; extensive call forwarding; hosting a conference line service for purchase by third parties; transmitting or receiving of communications which do not consist of SMS messages; transmitting or receiving broadcasts over teleconferencing facilities or other means; or transmitting or receiving communications which do not consist of voice messages or standard voice calling involving live dialogue between individuals).
- Conducting excessive calling or messaging (for example, completing excessively long calls to a single number or calls to the same destination telephone number, indicative of an automated call-forwarding device; receiving excessive inbound calls; completing a high volume of calls terminated and re-initiated consecutively, completing or receiving excessive text messages; or conducting any other unusual or atypical calling or usage patterns indicative of an attempt to evade Comcast's enforcement of this Policy).
- Misusing plans, devices, or features (for example, tethering when your plan does not allow it; using, allowing, or facilitating the use of any Services restricted by location or geography outside of the permitted location; activating devices on plans not intended for them; using static IP or non-DHCP configurations without an eligible Internet plan; transmitting traffic that degrades performance or disproportionately contributes to congestion; transmitting or receiving broadcasts or recorded materials (other than standard, commercial voicemail greetings) or other communications which do not consist of standard commercial voice or fax over voice services; physically modifying Comcast-owned hardware; engaging in activities which may generate payments to a subscriber due to their use of the Services).
- Violating third-party terms or service rules (for example, the terms of websites, apps, systems, or networks you access).
- Tampering with Comcast equipment or permitting unauthorized service work.

Intellectual Property Infringement

Your business is solely responsible for preventing your users from using the Services in any manner that constitutes an infringement of a third party's intellectual property rights, and for complying with all notices and requests pursuant to the Digital Millennium Copyright Act, 17 U.S.C. §512(c)(3) ("DMCA"). Your business shall have a process for expeditiously complying with and responding to DMCA take-down notices. Upon reasonable request by Comcast, your business shall furnish to Comcast information that reasonably demonstrates your policies, procedures and practices for addressing DMCA violations in connection with your Services.

Comcast has adopted a policy (the Comcast Digital Millennium Copyright Act (DMCA) Policy at https://www.xfinity.com/dmca) to address notifications of alleged copyright infringement and repeat infringers, which may include suspension or termination of Services.

Policy Updates and Reporting Issues

We may update this Policy by posting a new version on our website at https://business.comcast.com/customer-notifications/acceptable-use-policy or any successor URL(s) (the "Website"). Comcast will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending bill messages or posting information on the Website. Revised versions of this Policy are effective immediately upon posting. Continued use of the Services after an update of this Policy constitutes acceptance.

You can report violations of this Policy at https://business.comcast.com/contact. Please include any relevant details that could assist Comcast in investigating and resolving the reported violation(s).

To report a child exploitation or another child-related incident involving the Internet, go to https://internetsecurity.xfinity.com/help/report-abuse.

Network Management and Enforcement

Comcast may, but is not required to, monitor your compliance, or the compliance of other users, with the terms and conditions of this Policy. You acknowledge and agree that Comcast shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Services, including but not limited to content that violates the law or this Policy.

If we believe your use violates this Policy or your service agreement(s), we may take action with or without notice. Actions may include:

- Temporary or permanent removal or blocking of content or transmissions;
- Filtering or blocking of calling, messaging, or data activity that violates this Policy;
- Suspending or terminating some or all Services or downgrading service tiers;
- Deleting email, voicemail, and other messages or other data associated with terminated accounts; and/or
- Suspending and/or terminating your Services.

We prefer to notify customers and allow time to correct issues except in severe cases. Our failure to enforce this Policy at any time does not waive our rights to enforce it later.

We may cooperate with law enforcement and other network or facilities providers to investigate suspected violations and to protect the network, Services, and customers. You expressly authorize and consent to Comcast and its agents cooperating with law enforcement authorities and system administrators from other internet service providers in such investigations. Please also refer to our Privacy Policy.

Global Application and Legal Compliance

This Policy applies globally. Users must comply with all applicable laws and regulations where they access or use the Services, including telecommunications, data protection, consumer protection, cybersecurity, intellectual property, anti-spam, and record-keeping laws. Users must comply with trade controls, sanctions, and export laws, including the United States, United Kingdom, European Union, and other applicable jurisdictions. Services may not be used from, by, or for the benefit of sanctioned persons or entities or embargoed destinations. Comcast reserves the right to screen transactions, block access, or suspend Services as necessary to comply with applicable sanctions and export control requirements. Where local law requires stricter standards than this Policy, all users must follow the stricter standard.