

(855) 407-2075

Acceptable Use Policy

for High-Speed Internet Services

FAQ



Why is Comcast providing this Policy to my business?

Comcast's goal is to provide its customers with the best commercial Internet service possible. In order to help accomplish this, Comcast has adopted this Acceptable Use Policy (the "Policy"). This Policy outlines acceptable use of Comcast Business Services Internet service, including Comcast-provided Wi-Fi Internet service, Ethernet services, other Internet-based communications services and any other Comcast Business service that links to or references this Policy (each and collectively, the "Service"). This Policy is in addition to any other restrictions contained in any applicable terms and conditions or other agreements for [Small Business](#) or [Enterprise services](#). All capitalized terms used in this Policy that are not defined here have the meanings given to them in the applicable Small Business and Enterprise Services agreements (each and collectively, "Business Services Agreements").

All Comcast Business Services customers and all others who use the Service (the "customer," "user," "you," or "your") must comply with this Policy. Your business's or your user's failure to comply with this Policy could result in the suspension or termination

of its Service account. In these cases, termination or other charges may apply. Therefore, you should take steps to ensure that end users who use the Service are aware of this Policy and agree to abide by it. If your business does not agree to comply with this Policy, it must immediately stop all use of the Service and notify Comcast so that it can close your business's account.

Does this Policy apply to my use of Comcast Business Services WiFi-identified services inside and outside of my premises and in public places?

This Policy applies to your use of the Service if you are a Comcast Business Services customer who accesses Comcast-provided Business Services Wi-Fi-identified services inside or outside of your premises or in public places using a Comcast Business Services login and password. You can learn more about Comcast-provided Wi-Fi services by going to <http://business.comcast.com/learn/internet/business-internet>.

How will my business know when Comcast changes this Policy and how will it report violations of this Policy?

Comcast may revise this Policy from time to time by posting a new version on the website at <https://business.comcast.com/customer-notifications/acceptable-use-policy> or any successor URL(s) (the "Website") or by communicating it in another manner as described below. For a copy of this document, please call 800-391-3000 or go to [the website](#). Comcast will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending email announcements or posting information on the Comcast Business Services website. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Service should read any Comcast announcements

they receive and regularly visit the Comcast Business Services website and review this Policy to ensure that their activities conform to the most recent version. Your business can send questions regarding this Policy to, and report violations of it at <https://business.comcast.com/contact>.

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

Prohibited Uses and Activities

What uses and activities does Comcast prohibit?

In general, the Policy prohibits uses and activities involving the Service that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Service by others. For example, these prohibited uses and activities include, but are not limited to, using the Service, Customer-Provided Equipment, or the Comcast Equipment, either individually or in combination with one another, to:

Conduct and information restrictions

- undertake or accomplish any unlawful purpose. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation;
- post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be unlawful;
- upload, post, publish, transmit,

reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner;

- transmit unsolicited bulk or commercial messages commonly known as “spam;”
- send large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send large messages or files that disrupts a server, account, blog, newsgroup, chat, or similar service;
- initiate, perpetuate, or in any way participate in any

pyramid or other
illegal scheme;

- participate in the collection of large numbers of email addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including “spyware”) designed to facilitate this activity;
- collect responses from unsolicited bulk messages;
- use IRC (Internet Relay Chat) or other chat services or tools to flood chats, or use unattended clones, bots, or other automated programs to engage in chats;
- falsify, alter, or remove message headers;
- falsify references to Comcast or its

network, by name
or other identifier,
in messages;

- impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (e.g., "phishing");
- violate the rules, regulations, terms of service, or policies applicable to any network, server, computer database, service, application, system, or website that you access or use;

Technical restrictions

- access any other person's computer or computer system, device, sensor, camera, network, software, or data without his, her or their knowledge and consent; breach the security of another user or system; or attempt to

circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for your business, logging into or making use of a server or account your business is not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so;

- use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port

scanning is strictly prohibited;

- copy, distribute, or sublicense any proprietary software provided in connection with the Service by Comcast or any third party, except that your business may make one copy of each software program for back-up purposes only;
- distribute programs that make unauthorized changes to software (cracks);
- service, alter, modify, or tamper with the Comcast Equipment or Service or permit any other person to do the same who is not authorized by Comcast;

Network and usage restrictions

- use the Service for operation as an Internet service provider or for any other business, legal entity, or organizational

purpose (whether or not for profit); restrict, inhibit, compromise, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the Service (except for tools for safety and security functions such as parental controls, for example), including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature;

- restrict, inhibit, compromise, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any Comcast (or Comcast supplier) host, server, backbone network, node or service, or otherwise cause a

performance
degradation to any
Comcast (or
Comcast supplier)
facilities used to
deliver the Service;

- make the Service (i)
available to any
third party unless
done with
Comcast's written
approval in
accordance with an
applicable Business
Services Agreement
or (ii) available to
any person or third
party for use within
a residential unit at
the site(s) at which
Customer receives
the Service. It is
not a violation of
this Policy for a
Customer to make
the Service
available to its
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
Customer receives
the Service, so long
as such use does

not violate the
terms and
conditions of
Customer's
Business Services
Agreement;

- resell the Service
or otherwise make
available to anyone
outside the Service
Location(s) the
ability to use the
Service, in whole or
in part, directly or
indirectly, unless
expressly permitted
by the applicable
Business Services
Agreement;
- connect the
Comcast Equipment
to any computer or
device outside of
your business'
Service
Location(s);
- interfere with
computer
networking or
telecommunications
service to any user,
host or network,
including, without
limitation, denial of
service attacks,
flooding of a
network,
overloading a
service, improper
seizing and abusing

operator privileges,
and attempts to
“crash” a host;

- interfere with Comcast’s ability to control or block ports for safety and security purposes and as part of its overall network management;
- interfere with Comcast’s use and control of its domain name server (“DNS”) used in connection with the Service; and
- access and use the Service with anything other than a dynamic Internet Protocol (“IP”) address that adheres to the dynamic host configuration protocol (“DHCP”), unless otherwise expressly permitted by the applicable Business Services Agreement.

Customer Conduct and

Features of the Service

What obligations does my business have under this Policy?

In addition to being responsible for your own compliance with this Policy, your business is also responsible for any use or misuse of the Service that violates this Policy, even if it was committed by an employee, contractor, customer, or guest with access to your Service account. Your business is solely responsible for the security of any device (including data on those devices) it chooses to connect to the Service.

Your business is responsible for securing the Customer-Provided Equipment and any other Service Location(s) equipment or programs not provided by Comcast that connect to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

How does Comcast address inappropriate content and transmissions?

Comcast reserves the right to refuse to transmit or post, and to remove or block, any information or materials, in whole or in part, that it, in its sole

discretion,
deems to be in
violation of
Sections I or II
of this Policy,
or otherwise
harmful to
Comcast's
network or
customers
using the
Service,
regardless of
whether this
material or its
dissemination is
unlawful so
long as it
violates this
Policy. Neither
Comcast nor
any of its
affiliates,
suppliers, or
agents have any
obligation to
monitor
transmissions
or postings
(including, but
not limited to,
email, file
transfer, blog,
newsgroup, and
instant message
transmissions)
made on the
Service.
However,
Comcast and its
affiliates,
suppliers, and
agents have the

right to monitor these transmissions and postings from time to time for violations of this Policy and to disclose, block, or remove them in accordance with this Policy, the Business Services Agreement, and applicable law.

What requirements apply to electronic mail?

The Service may not be used to communicate or distribute email or other forms of communications in violation of Section I of this Policy. As described below in Section III of this Policy, Comcast uses reasonable network

management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer).

Comcast is not responsible for deleting or forwarding any email sent to the wrong email address(es) by your business or by someone else trying to send email to your business or its employees, contractors, or users. Comcast is also not responsible for forwarding email sent to any account that has been suspended or terminated. This email will be returned to the sender, ignored, deleted, or

stored temporarily at Comcast's sole discretion. In the event that a Service account is terminated for any reason, all e-mail associated with that account (and any secondary accounts) that is hosted by or at the direction of Comcast may be permanently deleted as well.

In the event that Comcast believes in its sole discretion that any subscriber name, account name, or email address (collectively, an "identifier") on the Service may be used for, or is being used for, any misleading, fraudulent, or other improper or illegal purpose, Comcast (i) reserves the

right to block access to and prevent the use of any of these identifiers and (ii) may at any time require any customer to change his, her or their identifier. In addition, Comcast may at any time reserve any identifiers on the Service for Comcast's own purposes.

Comcast Service plans limit the storage of messages on Comcast's systems. Neither Comcast nor any of its suppliers shall have any liability for the deletion of, or failure to store, messages or of the mis-delivery of, failure to deliver, or the untimely delivery of messages.

Comcast's email servers and other systems employ various virus detection and prevention tools that it updates frequently to respond to the latest threats on the Internet. These tools will automatically remove viruses and other unwanted material from emails whenever possible. This applies both to emails your business sends as well as to emails your business receives. Comcast's systems also may scan all incoming and outgoing email traffic over the Service using automated tools applying recognized and commonly used techniques for identifying and blocking spam and other

unwanted or
harmful code or
content.

**What
requirements
apply to
instant, video,
and audio
messages?**

Each user is
responsible for
the contents of
his, her or their
instant, video,
and audio
messages and
the
consequences
of any of these
messages.

Comcast
assumes no
responsibility
for the
timeliness, mis-
delivery,
deletion, or
failure to store
these messages.

In the event
that a Service
account is
terminated for
any reason, all
instant, video,
and audio
messages
associated with
that account
(and any

secondary accounts) will be permanently deleted as well.

What requirements apply to my business' Service account Internet reputation?

Comcast provides the Service for use in your business.

Everything your business does using the Service will be directly attributable to your business and affect its reputation.

However, because Comcast provides the systems to deliver the Service, your business can do things using the Service that are directly attributable to Comcast and affect its

reputation.

Most obviously, if your business uses the Service to send spam (or what spam reporting services or recipients classify as spam), this activity may affect Comcast's reputation because of its ownership of the IP addresses associated with the Service. These types of activities also violate this Policy.

Comcast reserves the right to suspend or terminate Service accounts when your business' use of the Service or any of its features negatively impacts Comcast's reputation as determined in its sole

discretion. Any use of the Service or its features that results in your business' Service account, or any associated Comcast information, being listed on spam reporting websites such as Spamhaus, SBL, ROKSO, TrendMicro Maps, or SenderScore Blocklist, or anti-phishing or anti-spyware services, may result in Comcast suspending or terminating your business' Service account.

In these situations, Comcast prefers to work directly with your business to address the problems causing the harm to Comcast's reputation so

that they do
not happen
again.

Network Management

**Why does
Comcast manage
its network?**

Comcast manages
its network with
one goal: to
deliver the best
possible
broadband
Internet
experience to all
of its customers.
High-speed
bandwidth and
network
resources are not
unlimited.
Managing the
network is
essential as
Comcast works to
promote the use
and enjoyment of
the Internet by
all of its
customers.
Comcast uses
reasonable
network
management
practices that are

consistent with industry standards. Comcast tries to use tools and technologies that are minimally intrusive and, in its independent judgment guided by industry experience, among the best in class. Of course, Comcast's network management practices will change and evolve along with the uses of the Internet and the challenges and threats on the Internet.

The need to engage in network management is not limited to Comcast. In fact, all large Internet service providers manage their networks. Many of them use the same or similar tools that Comcast does. If the company did not manage its

network, its customers would be subject to the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of service. By engaging in responsible network management including enforcement of this Policy, Comcast can deliver the best possible broadband Internet experience to all of its customers.

How does Comcast manage its network?

Comcast uses various tools and techniques to manage its network and to deliver the Service. These tools and techniques are dynamic, like the network and its usage, and can

and do change.
For example,
these Network
management
activities
employed by
Comcast may
include (i)
identifying spam
and preventing
its delivery to
customer email
accounts, (ii)
detecting
malicious
Internet traffic
and preventing
the distribution
of viruses or
other harmful
code or content,
and (iii) using
other tools and
techniques that
Comcast may be
required to
implement in
order to meet its
goal of delivering
the best possible
broadband
Internet
experience to all
of its customers.

Data Consumption

Are there

**restrictions on
data consumption
that apply to the
Service?**

The Service is for commercial use only in a small, medium, or large business as determined by the applicable Business Services Agreement.

Therefore, Comcast reserves the right to suspend or terminate Service accounts where data consumption is not characteristic of a typical commercial user of the Service as determined by the company in its sole discretion, or where it exceeds published data consumption limitations.

Common activities that may cause excessive data consumption in violation of this Policy include, but are not limited to,

numerous or continuous bulk transfers of files and other high capacity traffic using (i) file transfer protocol ("FTP"), (ii) peer-to-peer applications, and (iii) user generated content sites.

Your business must also ensure that its use of the Service does not restrict, inhibit, interfere with, or degrade any other person's use of the Service, nor represent (as determined by Comcast in its sole discretion) an overly large burden on the network. In addition, your business must ensure that its use of the Service does not limit or interfere with Comcast's ability to deliver and monitor the Service or any part of its network.

If your business uses the Service in violation of the restrictions referenced above, that is a violation of this Policy and a breach of your Business Services Agreement. Comcast's determination of the data consumption for Service accounts is final.

Violation of this Acceptable Use Policy

**What happens
if your
business
violates this
Policy?**

Comcast reserves the right to immediately suspend or terminate your business's Service account and terminate the Business

Services Agreement if you violate the terms of this Policy or the Business Services Agreement, or if anyone of your end users violates this Policy or the Business Services Agreement.

How does Comcast enforce this Policy?

Comcast has no obligation to monitor and does not routinely monitor the Service and/or the network for violations of this Policy. However, Comcast and its suppliers reserve the right at any time to monitor bandwidth, usage, data consumption, transmissions,

and content in order to, among other things, operate the Service; identify violations of this Policy; and/or protect the network, the Service and Comcast users.

Comcast prefers to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action.

Comcast also prefers to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without Comcast's intervention. However, if the Service is

used in a way that Comcast or its suppliers, in their sole discretion, believe violates this Policy, Comcast or its suppliers may take any responsive actions they deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service. Neither Comcast nor its affiliates, suppliers, or agents will

have any liability for any of these responsive actions. These actions are not Comcast's exclusive remedies and Comcast may take any other legal or technical actions it deems appropriate with or without notice.

Comcast reserves the right to investigate suspected violations of this Policy, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material and data on Comcast's servers and network.

During an investigation, Comcast may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. Your business expressly authorizes and consents to Comcast and its suppliers cooperating with (i) law enforcement authorities in the investigation of suspected legal violations, and (ii) and system administrators at other Internet service providers or other network or computing facilities in order to enforce this Policy. Upon termination of your business's

Service account, Comcast is authorized to delete any files, programs, data, email and other messages associated with your business's account (and any secondary accounts).

The failure of Comcast or its suppliers to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time. Your business agrees that if any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and

the remaining
portions will
remain in full
force and
effect.

Copyright

What is Comcast's DMCA policy?

Users of the Service and
copyright owners should refer
to the Comcast Digital
Millennium Copyright Act
("DMCA") Policy at
<https://www.xfinity.com/dmca>
to learn more about how
Comcast handles notifications
of alleged copyright
infringement and its repeat
infringer policy.

Revised and effective:
October 13, 2022

[CONTACT US](#)
[COMMUNITY](#)
[PRIVACY POLICY](#)
[YOUR PRIVACY CHOICES](#)
[NOTICE AT COLLECTION](#)
[VISITOR AGREEMENT](#)
[TERMS & CONDITIONS](#)
[SITEMAP](#)
[OPEN SOURCE](#)
[COMCAST RISE](#)

©2023 Comcast Corporation. All Rights Reserved



 [Cookie Preferences](#)