

Acceptable Use Policy

Last updated: September 25, 2026

1. Introduction

This Acceptable Use Policy ("AUP") governs the use of all services provided by the Core Fiber company whose network serves the Service Location, as identified on your order or invoice ("Company," "we," "us," or "our"). All customers, users, and any persons accessing or using Company services ("you" or "your") must comply with this AUP. This AUP is incorporated by reference into the Agreement described in Section 1 of the Core Fiber General Terms & Conditions (the "General Terms"). Capitalized terms not defined in this AUP have the meanings given to them in the General Terms.

2. Network and Usage Restrictions

You may not use Company services in any manner that interferes with, disrupts, or degrades the performance of Company's network, services, or infrastructure, or the use and enjoyment of services by other customers. Prohibited activities include but are not limited to:

- Conducting or participating in denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, or any activity designed to overwhelm, flood, or render unavailable any network, server, or service.
- Reselling, redistributing, or sharing your internet service with third parties, except as expressly permitted by your Subscriber Agreement & Service Order or with prior written authorization from the Company.
- Using any IP addressing or network configuration other than that assigned by the Company via DHCP or as otherwise authorized.
- Operating public-facing servers (web servers, mail servers, game servers, etc.) on residential service plans, EXCEPT that home automation systems, personal media servers, and similar personal-use applications are permitted provided they do not consume excessive bandwidth or degrade network performance for other users.
- Sharing your internet connection with neighboring residences, businesses, or other locations outside the Service Location, except as expressly permitted by your Subscriber Agreement & Service Order or with prior written authorization from the Company.

Excessive use. Our residential and small business plans don't have data caps, but they're built for normal home and small business use. We may treat use as excessive if it is sustained and far beyond typical use of the same plan, burdens our network or other customers' service, or shows signs of commercial hosting, resale, or other use the plan doesn't cover. If we see excessive use, we'll contact you first and work with you on a fix, which may include

moving to a commercial plan. If it continues after notice, we may suspend or terminate the affected Service under Section 6 of the General Terms.

Permitted uses. Using remote access tools (VPN, development servers, remote desktop applications, and similar remote work technologies) is permitted on all service plans provided such use does not degrade network performance or violate other provisions of this AUP. Home businesses requiring higher bandwidth, static IP addresses, or server hosting capabilities should contact the Company about business-class service tiers.

3. Conduct and Information Restrictions

You may not use Company services to engage in any of the following activities:

- Any activity that violates applicable local, state, federal, or international law or regulation.
- Creating, transmitting, storing, or accessing child sexual abuse material, or otherwise using Company services to exploit or endanger minors.
- Harassment, threats, stalking, defamation, or any communication intended to intimidate, abuse, or harm any person or entity.
- Transmitting unsolicited bulk email, commercial messages, or spam in any form.
- Phishing, social engineering, or any attempt to fraudulently obtain personal information, credentials, or financial information from any person.
- Spoofing or forging email headers, IP addresses, or any other identifying information, or causing any caller identification service to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.
- Harvesting, collecting, or scraping email addresses, personal information, or other data from Company systems or third-party systems without authorization.
- Impersonating any person, entity, or organization, or falsely claiming an affiliation with any person, entity, or organization.
- Using AI or automated systems to conduct large-scale scraping, data collection, or model training activities that violate the terms of service of target websites or services, or that infringe upon intellectual property rights. Operating botnets, credential-stuffing tools, or automated attack infrastructure is strictly prohibited.

4. Technical Restrictions

You may not use Company services to engage in any of the following technical activities:

- Unauthorized access or attempted access to any computer, network, system, or data (commonly known as "hacking"), regardless of whether damage occurs.
- Port scanning, network probing, or vulnerability scanning of any system or network without explicit written authorization from the owner of the target system.

- Distributing, installing, or using malicious software, including viruses, worms, trojans, ransomware, spyware, adware, keyloggers, or any other harmful code.
- Reverse engineering, decompiling, or disassembling any Company software, firmware, or network equipment.
- Circumventing, disabling, or interfering with any security features, access controls, or usage limits implemented by the Company.

5. Customer Obligations

You are responsible for all activity that occurs through your account and on your network, whether or not you authorized or had knowledge of such activity. You agree to:

- Secure your account credentials, including usernames and passwords, and not share them with unauthorized persons.
- Maintain reasonable security measures on your own network and devices, including keeping software and firmware updated and using appropriate firewall and antivirus protections.
- Notify the Company promptly if you become aware of any unauthorized use of your account, or if any Company-provided equipment is lost, stolen, or compromised.

6. Company Rights and IoT Security

The Company reserves the right to monitor network traffic for the purposes of network management and security, to the extent necessary to the rendition of the Services or to protect the rights or property of the Company. The Company does not engage in routine or random monitoring of the content of Customer communications. Company's handling of Customer information is governed by the Privacy Policy and the CPNI Policy. The Company may block, filter, or throttle traffic that violates this AUP or threatens network integrity. Any such action will be consistent with the reasonable network management practices described in the Company's Network Management and Open Internet Disclosure and with applicable law. The Company will cooperate with law enforcement agencies as required by applicable law. The Company may suspend or terminate service in accordance with Section 6 of the General Terms and your Subscriber Agreement & Service Order for violations of this AUP.

IoT Device Quarantine: The Company may quarantine or restrict network access for Internet of Things (IoT) devices that pose a security risk to the network or other customers. The following procedures apply:

- (a) Non-Emergency Quarantine: For non-emergency security concerns, the Company will provide advance notice before quarantining an IoT device where reasonably practicable, allowing the customer to remediate the issue.
- (b) Emergency Quarantine: For active security threats, the Company may act immediately to quarantine a device and will notify the customer promptly after taking action.

- (c) Expedited Review: Customers may request expedited review of any quarantine action by contacting the Company's Network Operations Center.
- (d) Service Restoration: Upon confirmation that the security concern has been remediated, the Company will restore full network access as soon as reasonably practicable.
- (e) Agricultural and Medical IoT Devices: The quarantine and restriction procedures described in this Section may affect agricultural monitoring, medical monitoring, and other critical IoT devices. Customers relying on such devices are responsible for maintaining appropriate backup or redundant measures.

7. Email

The Company's email services, where provided, are subject to the following additional rules:

- You may not use Company email services to send unsolicited bulk email or spam, or to relay email through Company servers for the purpose of sending spam.
- You may not forge, spoof, or alter email headers or sender information.
- Email storage is subject to reasonable limits as established by the Company. The Company reserves the right to limit mailbox sizes and delete emails that exceed storage quotas after providing reasonable notice.

8. Network Management

The Company's network management practices are described in the Company's Network Management and Open Internet Disclosure, available at corefiber.com/legal, and the Company's related rights are stated in Section 7 of the General Terms.

9. Violations and Enforcement

The Company prefers to notify customers of AUP violations and work cooperatively to resolve issues. However, the Company reserves the right to suspend or terminate service immediately in cases of severe or repeated violations, or where continued service poses a risk to the network or other customers. The Company may investigate suspected violations of this AUP, including by gathering information from the users involved and any complaining party and examining material on the Company's network, and may cooperate with law enforcement authorities and with other network operators in doing so. The Company reports apparent child sexual abuse material as required by 18 U.S.C. § 2258A. The Company's liability for actions taken under this AUP is limited as provided in Section 11 of the General Terms. The Company has adopted and will reasonably implement a policy providing for the termination, in appropriate circumstances, of subscribers and account holders who are repeat infringers of copyright. The Company applies a graduated response: notices of claimed infringement are forwarded to the subscriber, further notices result in escalating warnings and may result in temporary suspension or other interim measures, and continued infringement may result

in termination. That policy is described in the Company's Copyright/DMCA Policy, which is incorporated herein by reference.

This Acceptable Use Policy should be read in conjunction with the General Terms, Privacy Policy, CPNI Policy, Network Management and Open Internet Disclosure, and Copyright/DMCA Policy, all of which are available at corefiber.com/legal.

Contact Information

Core Fiber
4015 S Lincoln Ave, Suite 500
Loveland, CO 80537
Email: help@corefiber.com
Phone: 855-267-3342
Website: corefiber.com
Report AUP violations or abuse: abuse@corefiber.com
Privacy Inquiries: privacy@corefiber.com
DMCA/Copyright: dmca@corefiber.com
Accessibility: accessibility@corefiber.com

Effective Date: This AUP takes effect as provided in Section 20 of the General Terms.