

LEGAL

Acceptable Use Policy

Fiber Stream Communications Inc. · d/b/a Fiber Stream

Internet access, property-wide Wi-Fi, managed networks, and related services

Effective Date: September 3, 2026 · Version 4.3

This AUP replaces prior acceptable use policies.

This Acceptable Use Policy (“AUP”) applies to every person and entity that uses products or services of Fiber Stream Communications Inc. (“Fiber Stream,” “we,” “us,” or “our”), including property-wide Wi-Fi, managed internet, portals, Resident Included Plans, Upgrades, and related managed services. It protects the security, integrity, reliability, and privacy of the Fiber Stream Network and of other users.

By using the Services you agree to this AUP, our Terms of Service, and our Privacy Policy. We may revise this AUP by posting an updated version. Continued use after the revised AUP is posted is acceptance of the changes.

Property Partners are responsible for informing on-site staff of this AUP. End Users and Property Partners are both “Customers” for purposes of this AUP. Each Customer is responsible for determining which laws apply to that Customer’s use of the Services. This AUP applies whether access is a lease-billed Resident Included Plan or a Fiber Stream-billed Upgrade.

1. Guiding Rule

You may not use the Services in any way that is unlawful; that harms or interferes with our Network, another provider’s network, or another person’s use of the Services; that infringes intellectual property or privacy rights; that is threatening, harassing, or exploitative; or that creates an unreasonable security risk.

2. Illegal, Infringing, and Harmful Content

You may not post, transmit, store, host, or distribute material on or through the Services if, in Fiber Stream’s reasonable judgment, the material:

- violates any local, state, federal, or non-U.S. law or regulation, including copyright, trademark, trade-secret, patent, or other intellectual-property law;
- is threatening, abusive, harassing, or intended to intimidate;
- is obscene or otherwise unlawful;
- is defamatory; or
- constitutes child sexual abuse material or any sexual content involving minors—this is strictly prohibited and will be reported to the National Center for Missing & Exploited Children and to law enforcement as required.

3. Network Abuse and Fair Use

The Network is a shared resource, especially on multifamily and campus properties. You may not:

- restrict or inhibit anyone’s use or enjoyment of the Services;
- generate traffic through automated or manual routines that is unrelated to ordinary personal, household, or authorized business use;

- operate servers, high-volume distribution, or continuous seeding that consumes a disproportionate share of property or upstream capacity, except where your plan and Order expressly allow it;
- use peer-to-peer or similar protocols to distribute infringing or unlawful content (unlawful file sharing is prohibited);
- run open mail, proxy, DNS, or similar relays;
- resell, timeshare, or provide service to premises or users outside the subscribed household, unit, or authorized location without a written agreement with us;
- attempt to jump from your isolated account segment onto another resident's devices, printers, cameras, or storage.

We may use reasonable network management during congestion, including temporary rate-limiting of classes of traffic that degrade the shared Network. Lawful applications are not banned merely because they use a particular protocol, but we may manage or restrict activity that threatens capacity, security, or other users. Advertised speeds are not a license to monopolize a shared property uplink.

4. Security, Malware, and Unauthorized Access

You may not:

- knowingly upload or distribute malware, ransomware, viruses, trojans, worms, time bombs, cancelbots, spyware, or similar code;
- hijack or attempt to hijack modems, routers, access points, cameras, controllers, or other systems;
- cause or attempt security breaches or disruptions of internet communications;
- scan, probe, or monitor networks to intercept data or harvest credentials or email addresses without authorization;
- circumvent user authentication, account isolation, VLANs, or security of any host, network, or account;
- interfere with or deny service to any user or system (including denial-of-service or distributed denial-of-service attacks);
- use any program, script, command, or message designed to interfere with or disable another user's session or device;
- attempt to bypass measurement of time, bandwidth, authentication, captive portals, or other use-recording systems;
- forge packet headers, MAC addresses, or email headers, or otherwise misrepresent the origin of traffic.

If your devices are compromised and used to attack others, we may quarantine or suspend the affected account until the issue is remediated, even if you did not intend the abuse. Quarantine of an Upgrade or of a single account for security reasons is separate from property billing of a Resident Included Plan.

5. Email, Messaging, and Spam

You may not:

- send unsolicited bulk or commercial messages (spam), junk mail, or other advertising to people who did not request it, are not prior customers or contacts of yours, and with whom you have no existing business relationship;
- distribute, advertise, or promote tools whose primary purpose is to facilitate spam;
- use the Fiber Stream Network, or another provider's network, to send unsolicited email advertising a service hosted on or connected through Fiber Stream;
- harvest or solicit email addresses with intent to harass or collect replies;
- use our Services for phishing, smishing, pretexting, or social-engineering schemes.

6. Fraud, Account Integrity, and Property Rules

You may not:

- furnish false or incorrect data on an order, portal, or contract, including fraudulent payment information;
- fail to comply with Fiber Stream procedures for activity on Fiber Stream-managed facilities;
- remove, relocate, or tamper with property-wide access points, switches, or pathways;
- share portal credentials in a way that defeats per-account security or billing;
- use the Services to traffic in stolen credentials, payment data, or pirated software.

7. Export, Interception, and Other Restricted Activity

- Do not export, re-export, or permit download of content in violation of U.S. export or import law, or without required licenses.
- Do not use, distribute, or advertise any tool designed to violate this AUP or another ISP's AUP.
- Do not use the Services to commit wiretapping or unauthorized interception of communications.

8. Customer Security Duties

Customers must use reasonable care to secure their accounts, Wi-Fi passwords, in-unit equipment, and connected devices (including IoT and cameras). Default passwords should be changed. You must promptly notify us of suspected unauthorized use, and take corrective action when we notify you of an AUP or security issue. Network-level isolation and firewalling are aids; they do not replace device hygiene.

9. Intellectual Property and Repeat Infringers

Copyright-infringing distribution—including unauthorized movies, software, and music—is prohibited. We comply with the DMCA. Copyright owners may send notices to info@fiberstreamwifi.com as described in our Terms of Service. We may suspend or terminate repeat infringers and may pass infringement notices to the responsible account holder.

10. Enforcement

Failure to observe this AUP may result in a warning, throttling, quarantine, suspension, termination, reporting to a Property Partner, or reporting to law enforcement. When feasible, we will notify the Customer by email or account notice and allow a reasonable chance to correct the issue. An AUP suspension can affect Network access even if the Resident Included Plan remains on the lease. Non-payment of an Upgrade, by itself, is billed and enforced under the Terms of Service and does not automatically cancel included access. We may act immediately and without prior notice when we reasonably determine that the conduct:

- is the subject of a court order or government notice requiring that it stop;
- may expose Fiber Stream to sanctions, prosecution, civil action, or other liability;
- harms or interferes with the integrity or normal operation of our Network or interconnected networks;
- interferes with another Customer's use of the Services;
- violates applicable law; or
- presents an imminent risk of harm to Fiber Stream, Customers, or the public.

We have no general obligation to monitor content. We may monitor traffic metadata and, where necessary, content or payload information to comply with law, respond to legal process, protect the Network, or investigate a specific AUP violation.

11. Cooperation with Law Enforcement

We may respond to valid subpoenas, court orders, and other lawful process. Nothing in this AUP creates a duty to retain logs beyond our ordinary retention practices except when we have received a valid preservation request.

12. Customer Responsibility for Content

Customers remain solely responsible for material they post, host, download, upload, create, access, or transmit using the Services. Fiber Stream has no responsibility for material created on the Network by Customers. Customers must take prompt corrective action to remedy an AUP violation and to help prevent recurrence.

13. Reporting Abuse

To report spam, network abuse, child-exploitation material, or other AUP violations:

Fiber Stream Communications Inc. d/b/a Fiber Stream

Abuse / AUP: info@fiberstreamwifi.com · Support: support@fiberstreamwifi.com

Phone: 1-888-644-WiFi (9434) · Text: 214-799-0608

Web: <https://www.fiberstreamwifi.com>

Reports of child sexual abuse material should also be made to NCMEC (report.cybertip.org) and local law enforcement. Do not transmit illegal images to us in order to report them; provide URLs, timestamps, and account identifiers instead.