BPS Telephone Company Acceptable Use Policy (AUP)

Effective Date: January 1, 2026
Last Updated: February 18, 2026
Version: 2026-v2 (includes Exhibits A–B)

---

1. Introduction and Acceptance

This Acceptable Use Policy ("AUP" or "Agreement") is a legally binding agreement between you ("Customer," "You," "User," or "Account Owner") and BPS Telephone Company, including its assumed business names BPS Networks and BPS Fiber (collectively, "BPS," "we," "us," or "our"), governing your use of BPS's fiber-to-the-premises ("FTTH") broadband Internet services (the "Services").

By establishing an account, accessing, using, or continuing to use the Services, you agree to comply with this AUP and all other BPS policies referenced herein. **Exhibit A (Internet Transparency & Network Management Statement)** and **Exhibit B (DMCA Policy)** are attached to and incorporated into this AUP. If you do not agree to this AUP, you may not access or use the Services.

BPS reserves the right, in its sole discretion, to modify this AUP at any time. Changes become effective upon posting on our website. Continued use of the Services after changes are posted constitutes acceptance of the revised AUP.

---

2. Scope of Services

This AUP applies only to BPS fiber-based broadband Internet services. Voice services, if offered, are governed by separate terms unless expressly stated otherwise.

BPS currently offers the following residential broadband service tiers:

- 100 Mbps download / 100 Mbps upload
- 500 Mbps download / 500 Mbps upload
- 1 Gbps download / 1 Gbps upload

All speeds are up to the subscribed tier and are not guaranteed. Actual performance may vary based on network conditions, customer equipment, inside wiring, device capabilities, and other factors beyond BPS's control.

BPS may modify service tiers, technologies, or network architecture at any time. Continued use of the Services constitutes acceptance of such changes.

---

3. Purpose of This Policy

This AUP is intended to protect:

- The integrity, security, and reliability of the BPS network
- Fair access to network resources for all customers
- BPS, its customers, and the broader Internet community from unlawful, harmful, or disruptive activities

Customers are responsible for ensuring that their use of the Services complies with this AUP and all applicable local, state, and federal laws.

---

4. Prohibited Uses

You may not use, attempt to use, or allow others to use the Services in any manner that is illegal, harmful, abusive, or that interferes with the operation of the BPS network or the use of the Services by others. Prohibited activities include, but are not limited to:

4.1 Network Abuse and Security Violations

- Attempting to gain unauthorized access to any network, system, account, or data
- Circumventing authentication or security measures
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Network flooding, packet injection, spoofing, or scanning
- Operating botnets or command-and-control infrastructure
- Using the Services to develop, distribute, host, or operate malware, spyware, ransomware, or similar malicious software

4.2 Excessive or Harmful Use

- Activities that unreasonably consume bandwidth or network resources in a manner that degrades service for others
- Any use that threatens network stability, performance, or integrity

BPS reserves the right to manage network traffic and take reasonable measures—including rate-limiting, protocol- or destination-based filtering used for security purposes, throttling, suspension, or termination—to protect the network and ensure fair access. For additional detail on our transparency and network management practices, see Exhibit A.

4.3 Servers and Hosting

- Operating servers of any kind (including but not limited to web, email, FTP, file-sharing, game, media, proxy, or IRC servers) without prior written authorization from BPS

4.4 Illegal and Prohibited Content

- Violating copyright, trademark, or intellectual property laws
- Unauthorized downloading, uploading, or distribution of copyrighted material
- Distribution of unlawful, obscene, or otherwise prohibited content

4.5 Email and Messaging Abuse

- Sending unsolicited bulk or commercial messages (spam)
- Email bombing or message flooding
- Forging headers or obscuring message origins
- Harassing, threatening, or abusive communications
- Using purchased, scraped, or third-party mailing lists without verifiable permission (for example, without confirmed opt-in)
- Operating or supporting spam-related services or infrastructure (including list harvesting, open relays/proxies, or similar abusive tools)

4.6 Fraud and Misrepresentation

- Obtaining or attempting to obtain Services through false representations or fraudulent means
- Using the Services to avoid lawful charges or assist others in doing so

4.7 Resale and Redistribution

- Reselling, redistributing, or sharing the Services outside the customer premises (beyond the service address/demarcation) without a separate written agreement with BPS

5. Protection of Minors

BPS has a zero-tolerance policy regarding the use of the Services to exploit, harm, or intimidate minors. Customers may not knowingly collect personal information from minors without verifiable parental consent and must comply with all applicable child protection laws.

---

6. Customer Responsibilities

- You are responsible for all activity conducted through your account, whether authorized or not
- You must safeguard account credentials and prevent unauthorized use
- You are responsible for ensuring that household members and authorized users comply with this AUP
- You are responsible for your customer-owned equipment, including routers, Wi-Fi systems, wiring, and devices
- Violations committed using your connection, account, equipment, or by any user acting on your behalf may be treated as violations by the Account Owner

BPS is not responsible for performance issues caused by customer-owned equipment or inside wiring.

---

7. Network Monitoring and Privacy

BPS does not routinely monitor customer content. However, BPS reserves the right to investigate suspected violations of this AUP, network abuse, or unlawful activity as permitted by law and to comply with lawful requests from governmental or regulatory authorities.

---

8. Enforcement and Remedies

BPS may take any action it deems appropriate in response to violations of this AUP, including but not limited to:

- Temporary or permanent suspension of Services

- Termination of account without refund
- Network traffic management measures
- Referral to law enforcement or regulatory authorities

BPS's failure to enforce any provision of this AUP does not constitute a waiver of its rights.

---

9. Limitation of Liability

BPS provides the Services on an "as is" and "as available" basis. BPS makes no warranties, express or implied, regarding the Services and is not liable for damages arising from delays, interruptions, errors, or inability to use the Services, except as required by law.

---

10. Indemnification

You agree to indemnify and hold harmless BPS from any claims, damages, liabilities, costs, or expenses arising from your use of the Services or violation of this AUP.

---

11. Upstream Provider Policies

Use of the Services is also subject to the acceptable use policies of BPS's upstream network providers. Violations of upstream provider policies may constitute a violation of this AUP.

---

12. Reporting Abuse

Suspected violations of this AUP or abusive activity originating from BPS customers should be reported to:

Email: info@bpstelephone.com
Phone: 800-785-8630

Reports should include sufficient detail and supporting information (such as logs or message headers) to allow investigation.

---

13. Acceptance

Use of the BPS Telephone Company Services constitutes your understanding of and agreement to comply with this Acceptable Use Policy, including Exhibits A and B.

Exhibit A — Internet Transparency & Network Management Statement

This Exhibit is incorporated into the AUP and describes, at a high level, how BPS manages its network to provide reliable service and to protect customers and the network.

A1. Network Security and Congestion Management

BPS uses generally accepted technical measures to provide acceptable service levels to all customers, such as application-neutral bandwidth allocation, as well as measures to address service attacks, illegal content, and other harmful activities to protect network integrity and reliability.

During periods of heavy congestion, BPS may apply neutral and generally accepted technical measures intended to preserve service quality and network stability. These measures may include temporary rate-limiting, traffic shaping, or other reasonable network management practices.

No paid prioritization: BPS does not practice affiliated or paid prioritization of Internet traffic.

BPS may monitor aggregate or account-level usage patterns to efficiently manage the performance of the network and to ensure a sustainable quality broadband service is provided. Congestion due to malfunctioning hardware and/or software is remedied as quickly as reasonably possible after diagnosis.

Congestion or degradation due to malicious activity may be mitigated using techniques available to BPS, including filtering, rate-limiting, blackholing/sinkholing, or blocking specific traffic patterns associated with attacks or malware.

A2. Blocking, Throttling, and Unreasonable Interference

BPS does not block access to lawful content, applications, services, or non-harmful devices, subject to reasonable network management for security and network integrity.

BPS does not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management.

BPS does not unreasonably interfere with or unreasonably disadvantage customers' ability to select, access, and use broadband Internet access service or the lawful Internet

content, applications, services, or devices of their choice, subject to reasonable network management practices.

A3. Factors Affecting Speed and Performance

- Network conditions (including congestion and upstream conditions outside BPS's control)
- Customer equipment (router/Wi-Fi configuration, device capabilities, and Ethernet vs. Wi-Fi performance)
- Inside wiring and in-home network layout
- Destination server performance and general Internet conditions

For questions about performance, contact BPS support at 800-785-8630 or info@bpstelephone.com.

Exhibit B — DMCA Policy

BPS respects the intellectual property rights of others and expects its customers to do the same. Unauthorized copying or distribution of copyrighted material using the Services may violate U.S. copyright law.

B1. Designated DMCA Agent

In accordance with the Digital Millennium Copyright Act (DMCA), BPS has designated an agent to receive notifications of claimed copyright infringement.

DMCA Agent: DMCA Agent, BPS Telephone Company
Address: 120 Stewart Street, P.O. Box 550, Bernie, MO 63822
Email: info@bpstelephone.com
Phone: 800-785-8630

B2. Submitting a DMCA Notice

To be effective, a DMCA notice should include: (1) identification of the copyrighted work claimed to have been infringed; (2) identification of the material that is claimed to be infringing and information reasonably sufficient to permit BPS to locate the material; (3) contact information for the complaining party; (4) a statement that the complaining party has a good faith belief that the use is not authorized; (5) a statement, under penalty of perjury, that the information is accurate and the complaining party is authorized to act; and (6) a physical or electronic signature.

B3. Counter-Notification

If you believe material was removed or disabled by mistake or misidentification, you may submit a counter-notification consistent with the DMCA. BPS may forward a counter-notification to the original complaining party and may restore access as permitted by law.

B4. Repeat Infringers

BPS may suspend or terminate accounts of customers who are determined, in BPS's reasonable discretion, to be repeat infringers or who repeatedly violate this AUP.