

ACCEPTABLE USE POLICY



Effective Date: October 1, 2026

This Acceptable Use Policy ("Policy") describes acceptable and prohibited uses of Internet access and related services provided by Allband Communications Cooperative and its affiliates ("Allband").

This Policy applies to Allband Internet access services, related features and applications, Allband-provided equipment, network resources, email or communications services, and any other Internet-related services Allband may provide (collectively, the "Service").

This Policy is incorporated into and forms part of the applicable Allband service agreement, Terms and Conditions, or other agreement governing the Service. If there is a conflict between this Policy and another applicable Allband agreement, the applicable agreement will control unless otherwise stated.

The examples in this Policy are intended to explain prohibited conduct but cannot identify every possible misuse of the Service. Allband may determine that conduct not specifically listed in this Policy violates the Policy when the conduct is unlawful, fraudulent, abusive, harmful to Allband or others, threatens network or information security, materially interferes with the Service, or is inconsistent with the intended use of the Service.

By using the Service, the subscriber and anyone the subscriber permits to use the Service ("User") agrees to comply with this Policy.

1. RESPONSIBILITY FOR USE OF THE SERVICE

The subscriber is responsible for use of the Service through the subscriber's account, connection, premises, or Allband-provided equipment, including use by household members, employees, guests, contractors, or other authorized users.

Subscribers should take reasonable precautions to prevent unauthorized access to their accounts, devices, networks, and wireless connections.

The Service may be used only in accordance with the service plan and agreement under which it is provided.

Unless expressly authorized by Allband, a User may not:

- resell, sublicense, or commercially redistribute the Service;
- make the Service generally available to the public;
- use a residential Service as an Internet service for another residence, business, property, or unrelated third party;
- bypass technical restrictions associated with the subscribed service plan; or
- alter or manipulate Allband provisioning, authentication, addressing, or configuration systems to obtain a level or type of Service not purchased by the subscriber.

ACCEPTABLE USE POLICY



Nothing in this section prohibits ordinary use of a private home or business Wi-Fi network by authorized users.

2. COMPLIANCE WITH LAW

Users may not use the Service to engage in, facilitate, solicit, promote, or knowingly assist activity that violates applicable federal, state, local, or international law or regulation.

Prohibited activity includes, without limitation:

- fraud, scams, identity theft, or financial crime;
- unauthorized access to computers, accounts, networks, or data;
- distribution or solicitation of child sexual abuse material or other unlawful exploitation of minors;
- trafficking in unlawful goods or services;
- unlawful threats, extortion, stalking, or harassment;
- unlawful gambling;
- unlawful distribution of controlled substances;
- violations of applicable export-control or sanctions laws;
- infringement of intellectual property rights; and
- using the Service to plan, facilitate, or materially support criminal activity.

Allband does not undertake to determine the legality of every communication or activity transmitted through its network. Users remain responsible for ensuring that their use of the Service complies with applicable law.

3. INTELLECTUAL PROPERTY

Users may not use the Service to infringe or misappropriate copyrights, trademarks, patents, trade secrets, rights of publicity, or other intellectual property or proprietary rights.

Users are responsible for obtaining any licenses, permissions, or other authorization necessary to copy, distribute, publish, transmit, display, download, upload, or otherwise use protected material.

Copyright and DMCA

Allband responds to valid notifications of claimed copyright infringement in accordance with applicable provisions of the Digital Millennium Copyright Act ("DMCA").

Allband maintains and reasonably implements a policy for addressing repeat copyright infringement and may suspend or terminate Service when appropriate under applicable law and Allband policy.

Information concerning Allband's designated DMCA agent and procedures for submitting copyright notices may be published separately on Allband's website.

ACCEPTABLE USE POLICY



4. SECURITY AND UNAUTHORIZED ACCESS

Users may not use the Service to gain or attempt to gain unauthorized access to any computer, account, device, application, system, service, network, or data.

Prohibited activities include, without limitation:

- password cracking or unauthorized password guessing;
- credential stuffing;
- theft, harvesting, or unauthorized use of authentication credentials;
- exploiting or attempting to exploit security vulnerabilities without authorization;
- unauthorized network scanning or probing;
- bypassing access controls or authentication systems;
- intercepting communications or data without authorization;
- spoofing or impersonating network devices or users for fraudulent or malicious purposes;
- accessing data without authorization; or
- assisting another person in engaging in unauthorized access.

The use of legitimate security, diagnostic, vulnerability-testing, or network-management tools is permitted when the User is authorized to test or manage the affected systems and the activity does not interfere with Allband's network or other users.

5. MALWARE AND MALICIOUS ACTIVITY

Users may not knowingly create, transmit, distribute, operate, or facilitate malware or other malicious code through the Service.

This includes, without limitation:

- viruses;
- worms;
- ransomware;
- Trojan horses;
- spyware;
- malicious scripts;
- botnets;
- logic bombs;
- destructive code; or
- software intended to compromise, damage, disable, encrypt, disrupt, or obtain unauthorized access to systems or data.

Users may not use the Service to operate command-and-control infrastructure, participate in distributed denial-of-service attacks, or knowingly allow compromised equipment under their control to materially harm Allband's network or others.

ACCEPTABLE USE POLICY



6. NETWORK DISRUPTION AND ABUSE

Users may not use the Service in a manner that intentionally or materially interferes with the operation, security, reliability, or availability of Allband's network or the networks, systems, services, or equipment of others.

Prohibited activities include, without limitation:

- denial-of-service or distributed denial-of-service attacks;
- packet flooding or similar disruptive traffic;
- deliberate network congestion;
- unauthorized manipulation of routing, addressing, DNS, DHCP, or other network services;
- IP address spoofing or unauthorized use of an IP address;
- attempts to evade Allband network-security controls;
- operation of malicious or abusive servers or services;
- use of compromised devices to generate harmful network traffic; or
- automated activity that materially degrades network performance or interferes with other customers.

Users may not alter, modify, service, tamper with, or reconfigure Allband-owned equipment except as authorized by Allband.

7. EMAIL, MESSAGING, AND SPAM

Users may not use the Service to send spam or facilitate unlawful or abusive electronic messaging.

Prohibited activities include, without limitation:

- sending unsolicited bulk messages in violation of applicable law;
- sending commercial email in violation of the CAN-SPAM Act or other applicable requirements;
- using false, deceptive, or materially misleading sender information, routing information, or subject lines;
- using harvested, purchased, or generated addresses in a manner that violates applicable law or the rights of recipients;
- continuing to send messages to recipients after a legally valid opt-out request when applicable;
- operating an open mail relay or similar system that facilitates abuse;
- phishing or other deceptive attempts to obtain credentials, financial information, or personal information; or
- using Allband's name, trademarks, domains, network, or identity in a manner intended to deceive a recipient.

Allband may use reasonable technical measures to identify, block, limit, or mitigate spam, phishing, malware, and other abusive traffic.

ACCEPTABLE USE POLICY



8. IMPERSONATION, FRAUD, AND DECEPTIVE ACTIVITY

Users may not use the Service to impersonate another person or organization or to misrepresent identity when doing so is fraudulent, deceptive, unlawful, or intended to cause harm.

Users may not knowingly falsify, manipulate, or conceal electronic communications information, including headers, routing information, caller or sender information, account information, digital signatures, or other identifiers, for an unlawful, fraudulent, or malicious purpose.

This provision does not prohibit lawful privacy tools, anonymous or pseudonymous communications, virtual private networks, security technologies, or other legitimate methods of protecting a User's identity or communications.

9. THREATS, HARASSMENT, AND HARMFUL CONDUCT

Users may not use the Service to engage in conduct that violates applicable laws concerning threats, stalking, harassment, defamation, extortion, intimidation, or similar harmful conduct.

Users may not use the Service to make credible threats of violence or intentionally facilitate unlawful harm to another person or property.

Users may not use the Service to unlawfully publish or distribute another person's private or sensitive information for purposes of harassment, intimidation, fraud, or harm.

10. PROTECTION OF MINORS

Users may not use the Service to exploit, abuse, endanger, groom, traffic, or otherwise unlawfully harm a minor.

The Service may not be used to create, possess, solicit, access, advertise, distribute, or facilitate child sexual abuse material or other material prohibited by law.

Allband may report suspected exploitation of minors to appropriate authorities as required or permitted by law.

11. CUSTOMER SECURITY RESPONSIBILITIES

Users are responsible for taking reasonable steps to secure devices, accounts, applications, and networks connected to the Service.

Recommended measures include:

- using strong and unique passwords;
- enabling multifactor authentication when available;
- securing Wi-Fi networks;

ACCEPTABLE USE POLICY



- keeping operating systems, applications, and device firmware reasonably current;
- applying security updates;
- using appropriate malware protection;
- protecting account credentials; and
- promptly addressing known compromises or security vulnerabilities.

If Allband reasonably determines that a compromised customer device or network is creating a significant security or operational risk, Allband may take reasonable measures to protect its network and other users, including temporarily restricting affected traffic or Service.

12. AUTOMATED SYSTEMS, BOTS, AND RESOURCE-INTENSIVE ACTIVITY

Users may operate automated systems, servers, bots, cloud applications, peer-to-peer applications, Internet-of-Things devices, and similar technologies when permitted by the User's service plan and when their operation complies with this Policy.

Users may not operate automated systems in a manner that:

- violates applicable law;
- facilitates fraud, spam, credential attacks, scraping prohibited by law, or malicious activity;
- attempts to bypass rate limits, security systems, or access controls;
- generates abusive or disruptive traffic; or
- materially interferes with the availability or performance of Allband's network or services.

13. BANDWIDTH AND NETWORK MANAGEMENT

Allband Internet services are intended to provide customers with access consistent with the service plan they purchase.

Normal high-bandwidth activities—including streaming, gaming, cloud backup, video conferencing, software downloads, and other lawful Internet uses—are not prohibited merely because they consume substantial bandwidth.

Users may not intentionally use the Service in a manner designed to damage, disable, overload, or materially impair Allband's network or interfere with the Service provided to other customers.

Allband may engage in reasonable network-management practices to protect network security, mitigate congestion, respond to harmful or abusive traffic, maintain service quality and reliability, comply with legal obligations, and manage the network consistent with applicable law.

Current information regarding Allband service performance, network-management practices, commercial terms, and other required broadband disclosures may be provided separately through Allband's website and applicable broadband consumer disclosures.

ACCEPTABLE USE POLICY



14. IP ADDRESSES AND NETWORK CONFIGURATION

IP addresses and other network resources provided by Allband remain subject to Allband's network-management and provisioning practices.

Unless specifically authorized by Allband, Users may not:

- configure or use IP addresses not assigned or authorized for their connection;
- impersonate or clone another customer's assigned network identity;
- interfere with Allband's address-assignment systems;
- circumvent provisioning or service controls; or
- manipulate network configuration to obtain unauthorized Service.

The availability of static IP addresses, public IP addresses, IPv4 addresses, IPv6 addresses, port configurations, or similar features depends on the applicable service offering.

15. PRIVACY AND NETWORK MONITORING

Allband does not undertake a general obligation to monitor the content of customer communications.

Allband may, however, collect, process, analyze, or retain network, account, device, security, traffic, and other information as reasonably necessary to:

- provide and maintain the Service;
- authenticate users and devices;
- diagnose technical problems;
- protect the security and integrity of Allband's network;
- identify or mitigate spam, malware, denial-of-service attacks, fraud, and other abuse;
- investigate violations of this Policy;
- respond to customer support requests;
- comply with applicable law, regulation, subpoena, court order, or lawful governmental request; and
- enforce Allband's agreements and legal rights.

Any such activity is subject to applicable law and Allband's privacy policies and notices.

Allband may disclose information concerning use of the Service when required or permitted by law.

16. THIRD-PARTY SERVICES

The Internet provides access to networks, applications, websites, platforms, and services that are not owned or controlled by Allband.

ACCEPTABLE USE POLICY



When using third-party services, Users may also be subject to the terms, policies, and rules established by those third parties.

Allband is not responsible for establishing or enforcing the acceptable-use policies of independent third-party services.

17. ENFORCEMENT

Allband may investigate suspected violations of this Policy and take reasonable action when necessary to protect customers, the public, Allband's network, or other networks and services.

Depending on the nature, severity, and frequency of the violation, Allband may:

- contact the subscriber and request corrective action;
- issue a warning;
- block or restrict malicious or abusive traffic;
- temporarily limit access to affected network functions;
- quarantine or isolate a compromised connection when technically appropriate;
- suspend the Service;
- terminate the Service in accordance with applicable agreements and law;
- remove or disable access to material hosted or controlled by Allband when legally permitted or required;
- preserve relevant information;
- cooperate with other network operators, rights holders, or security organizations as permitted by law; or
- report suspected unlawful activity to appropriate authorities.

Where practical and appropriate, Allband may provide notice and an opportunity to correct a violation before suspending or terminating Service. However, advance notice may not be provided when immediate action is reasonably necessary to address a security threat, network disruption, unlawful activity, fraud, harm to others, legal requirement, or other serious violation.

Allband's decision not to take action regarding one violation does not waive its right to take action regarding that or another violation in the future.

18. REPORTING SECURITY OR ABUSE ISSUES

Customers and third parties may report suspected violations of this Policy, network abuse, security concerns, or other misuse involving Allband services to Allband using the contact information published on Allband's website.

Reports should contain enough information for Allband to reasonably identify and investigate the activity, such as relevant IP addresses, timestamps and time zones, message headers, logs, URLs, or other supporting information when available.

ACCEPTABLE USE POLICY



Copyright infringement notices should be submitted using Allband's published DMCA process.

19. CHANGES TO THIS POLICY

Allband may modify this Policy from time to time to reflect changes in its services, technology, security practices, legal requirements, or network operations.

The current version of this Policy will be made available on Allband's website. When required by applicable law or agreement, Allband will provide additional notice of material changes.

Continued use of the Service after a revised Policy becomes effective constitutes acceptance of the revised Policy to the extent permitted by applicable law.

Customers should periodically review the current Policy.

20. CONTACT INFORMATION

Questions concerning this Acceptable Use Policy or reports of suspected abuse may be directed to:

Allband Communications Cooperative

Website: **www.allband.org**

Email: **info@allband.org**

Additional contact information for security incidents, abuse reports, copyright notices, or customer support may be published on Allband's website.