ChariyHost.org Acceptable Use Policy (AUP)

Effective January 2026

Posted January 6, 2026

For questions or feedback, create a ***support*** ticket via the client portal. To report suspected abuse or violations of this policy, create an ***abuse*** ticket via the client portal. See section 14.

---

1. Scope of This Policy

What: Where This Policy Applies

This Policy applies to all use of CharityHost.org ("CharityHost," "we," "us," "our") Services, including VPS hosting, web hosting, network services, and any related systems. This includes all customers, resellers, and their end users.

Why: Ensures Clear Service Expectations

Clear boundaries ensure consistent expectations for all customers and allow us to maintain a stable, secure, and predictable hosting environment.

---

2. Accurate Identity Information Required

What: Provide True, Verifiable Identity Information

Customers must provide accurate, complete, and verifiable identity information—including legal name, physical address, and valid contact details. Fictitious, fabricated, placeholder, or unverifiable information is not permitted. Documentation may be requested at any time. Anonymous hosting is not offered. Any detected fraud—including falsified identity information, fraudulent billing activity, unauthorized payment methods, chargeback abuse, or attempts to conceal true identity—may result in immediate service termination and denial of future service.

Why: Protects Against Fraud and Abuse

Accurate identity information protects the network from fraud, abuse, and malicious activity, and ensures compliance with legal, operational, and security requirements.

3. Brand Protection & Harmful Conduct

What: No Harmful or Deceptive Conduct

Customers may not engage in malicious, knowingly false, misleading, or defamatory conduct targeting CharityHost. Impersonation or mimicry of CharityHost.org, or operation of deceptive domains or content that could confuse or mislead others, is prohibited. Repeat offenses may result in termination and denial of future service.

Why: Maintains Trust and Platform Integrity

Brand impersonation and harmful conduct undermine customer trust, create security risks, and can damage the reputation and stability of the hosting operation.

---

4. Prohibited Content & Activities

What: No Harmful or Illegal Usage

Customers may not use the Services to store, host, process, transmit, or engage in any content or activity that is harmful, abusive, illegal, or disruptive. Repeat offenses may result in termination and denial of future service.

These activities include, but are not limited to:

- Malware, viruses, trojans, worms, or malicious code
- Phishing pages, fake login portals, or credential-harvesting tools
- Command-and-control (C2) infrastructure, botnet components, or remote-access trojans
- Spamming or unsolicited email, including hosting spam tools or lists
- Torrent software, trackers, or distribution nodes
- Unauthorized bots, scrapers, crawlers, or automation tools
- Open proxies, open mail relays, or anonymization services
- Hacking tools, scanners, brute-force utilities, or intrusion frameworks

- Harassment, abuse, or targeted harm toward individuals or groups
- Impersonation or deceptive content, including fake business identities
- Adult content or pornography, including storage or distribution
- Cryptomining
- Using Web Hosting for backups, archives, or general file storage
- Any content or activity that violates applicable law
- Child sexual abuse material (CSAM) or related illegal content (zero tolerance; immediate termination and reporting
- Any content or activity that is objectionable or likely to cause reputational harm to CharityHost.org, as determined at our sole discretion

Why: Protects Network Safety and Stability

Harmful or abusive content and behavior can disrupt service for other customers, create security risks, and violate upstream provider requirements. CharityHost.org maintains a zero-tolerance policy for CSAM; any instance results in immediate termination and reporting to authorities.

---

5. Fair Share Resource Use

What: Use Server Resources Responsibly

Customers must use server resources responsibly to maintain a stable and responsive environment for all. Occasional peak usage is permitted, but sustained or excessive consumption that degrades performance for others is not allowed. Customers must remain within reasonable usage expectations for CPU, network, bandwidth, memory, disk, IO, and swap. Repeat offenses may result in termination and denial of future service. Guidelines include:

- CPU
  - Short bursts up to 100% are acceptable
  - Sustained average usage above ~50% average may be limited

- Network (Public)
  - May burst up to 1 Gbps
  - Sustained high-volume traffic may be rate-limited

- Network (Private)
  - May burst up to 10 Gbps
  - Excessive east-west traffic may be shaped

- Bandwidth
  - Monthly allocation applies per plan
  - After allocation is exhausted, speeds may be reduced to 1024 Kbps

- Memory (RAM)
  - Up to 100% of assigned RAM may be used
  - Excessive swapping or ballooning may trigger controls

- Disk Usage
  - Up to 100% of assigned disk space may be used
  - Excessive inode usage or abnormal activity may be restricted

- Disk IO
  - Short bursts are acceptable
  - Continuous high IO may be throttled

- Swap
  - Available for temporary load
  - Sustained usage may trigger throttling

Why: Ensures Fair Performance for Everyone

Shared environments depend on fair usage. These limits ensure predictable performance and prevent resource monopolization.

---

6. DMCA & Copyright Complaints

What: Copyright Infringement Process

CharityHost.org responds to valid Digital Millennium Copyright Act (DMCA) notices and other applicable copyright complaints. Upon receipt of a valid notice:

- Service associated with the allegedly infringing content may be suspended or terminated while the matter is reviewed

- Repeat offenses may result in termination and denial of future service

Why: Ensures Legal Compliance and Content Protection

Compliance with copyright law protects intellectual property rights and maintains a lawful hosting environment.

---

7. SMTP Passlist Access & Abuse Policy

What: Controlled Access to Email Ports

Access to outbound email ports (25, 465, 587, 2525) is restricted by default. Enabling SMTP passlist access is governed by the following:

- A $25 fee (subject to change) must be paid per VPS to enable SMTP passlist access
- The passlist covers all IPs assigned to that VPS

If SMTP abuse occurs:

- Violations may be assessed based on third-party reports or internal review.
- Service is immediately suspended.
- An abuse ticket is submitted to the customer, requiring an outline of remediation efforts.
- An abuse mitigation fee may be assessed per occurrence (see Section 10: Consequences of Violations) to cover the costs of delisting IP addresses from blacklists and restoring service.

Restoring SMTP access requires:

- Compliance with abuse mitigation steps including abuse mitigation fee
- Verified external SMTP relay credentials, at staff discretion

Repeat offenses may result in termination and denial of future service.

Why: Prevents IP Blacklisting and Abuse

SMTP abuse can blacklist IP ranges, harm deliverability, and jeopardize the hosting environment. Quick action and remediation are required to ensure the viability of the shared hosting environment. Utilizing third-party mail services helps ensure safe, verified email delivery and reduces the risk of spam-related issues.

8. Compromised VPS & Security Incidents

What: Handling Compromised or Breached VPS Instances

If a customer's VPS is found to be compromised—through unauthorized access, malware, malicious code, or any other security breach:

- Suspension or termination may occur to protect the network and customers
- Notification and remediation opportunities may be provided where possible
- Repeat offenses may result in termination and denial of future service

Why: Protects Customers From Security Threats

A compromised VPS can be used to launch attacks, send spam, spread malware, or disrupt service for others. Therefore, immediate action is required to protect the platform and all customers.

---

9. Customer Data Responsibility & Backups

What: Customer Data Responsibility

Customers are responsible for all data stored on their services, as well as operating system management and backup management. CharityHost.org does not provide VPS duplication for redundancy or load balancing, nor does it provide OS management or backup services unless explicitly stated. Customers are strongly encouraged to implement a redundant backup strategy, including multi-region, off-site, and/or cloud backups.

Why: Prevents Data Loss and Downtime

Redundant, multi-location backups help prevent data loss and ensure services can be restored quickly and reliably.

---

10. Consequences of Violations

What: Actions for Violations

Violations may result in anyall of the following:

- Warnings

- Rate limiting
- Suspension
- Termination
- Administrative fees
- Forfeiture of any prepaid fees, credits, or refundable balances

Abuse reports require:

- Response to abuse ticket within 12 hours
- Resolution within 24 hours

CharityHost.org may assess an abuse mitigation fee for violations of this policy, including but not limited to SMTP abuse, network abuse, or other prohibited activities. The amount and application of such fees will be determined at discretion of CharityHost.org and may vary depending on the nature and severity of the violation. Service restoration (including unsuspension of a VPS or restoration of features such as SMTP access) will only occur after all mitigation steps, fees, and verification requirements are satisfied. Repeat offenses may result in termination and denial of future service.

Why: Protects Network and Service Stability

Timely and decisive action helps maintain service quality and ensure security and reliability for all customers.

---

11. Right to Refuse Service

What: When Service May Be Refused

Service may be refused, suspended, or discontinued at any time, at CharityHost's discretion, for any reason including but not limited to:

- Abuse
- Fraud
- Identity falsification
- Security risk
- Objectionable conduct
- Reputational harm
- Other activity that may negatively impact the network, other customers, or the business

Why: Protects the Network and Business

This ensures the ability to act quickly to prevent harm, maintain service quality, and protect the safety and stability of the hosting environment.

---

12. Law Enforcement Compliance

What: CharityHost.org complies with valid, lawful requests from US-based law enforcement, including subpoenas, warrants, and court orders.

Why: Fulfilling these legal obligations is necessary to ensure the safety, legality, and integrity of all services.

---

13. Policy Updates

CharityHost.org reserves the right to modify or update this Acceptable Use Policy at any time, at its sole discretion. Any such changes become effective immediately upon being posted on the CharityHost.org website, including but not limited to changes required by law, security needs, or operational requirements. Continued use of CharityHost.org services following the posting of an updated policy constitutes acceptance of those changes. Public posting on the CharityHost.org website is considered sufficient notice; no additional notification is required.

For additional legal terms, disclaimers, and limitations of liability, see our Terms of Service.

---

14. Contact Information

Support Portal: https://charityhost.org/account/submitticket.php

Support Email: support@charityhost.org
Abuse Email: abuse@charityhost.org