

CLEARPATH OPERATIONS, LLC
ACCEPTABLE USE POLICY
(February 2018)

1. As a provider of Internet access, web site hosting, and other Internet-related services, Clearpath Operations, LLC offers its Customers, and their customers and users, the means to acquire and disseminate public, private, commercial, and non-commercial information. Clearpath respects that the Internet provides a forum for free and open discussion and dissemination of information, however, when there are competing interests at issue, Clearpath reserves the right to take certain preventative or corrective actions. In order to protect these competing interests, Clearpath has developed an Acceptable Use Policy ("AUP"), which supplements and explains certain terms of each Customer's respective service agreement and is intended as a guide to the Customer's rights and obligations when utilizing Clearpath's services. This AUP will be revised from time to time.

2. One important aspect of the Internet is that no one party owns or controls it. This fact accounts for much of the Internet's openness and value, but it also places a high premium on the judgment and responsibility of those who use the Internet, both in the information they acquire and in the information they disseminate to others. When Customers obtain information through the Internet, they must keep in mind that Clearpath cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that Customers may acquire. For this reason, the Customer must exercise his or her best judgment in relying on information obtained from the Internet, and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Because Clearpath cannot monitor or censor the Internet, and will not attempt to do so, Clearpath cannot accept any responsibility for injury to its Customers that results from inaccurate, unsuitable, offensive, or illegal Internet communications.

3. When Customers disseminate information through the Internet, they also must keep in mind that Clearpath does not review, edit, censor, or take responsibility for any information its Customers may create. When users place information on the Internet, they have the same liability as other authors for copyright infringement, defamation, and other harmful speech. Also, because the information they create is carried over Clearpath's network and may reach a large number of people, including both Customers and non-Customers of Clearpath, Customers' postings to the Internet may affect other Customers and may harm Clearpath's goodwill, business reputation, and operations. For these reasons, Customers violate the Acceptable Use Policy when they, their end users, affiliates, or subsidiaries engage in the following prohibited activities:

3.1 Spamming -- Sending unsolicited bulk and/or commercial messages over the Internet (known as "spamming"). It is not only harmful because of its negative impact on consumer attitudes toward Clearpath, but also because it can overload Clearpath's network and disrupt service to Clearpath customers. In addition, maintaining an open SMTP relay is prohibited.

3.2 Intellectual Property Violations -- Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities. Engaging in activity that violates privacy, publicity, or other personal rights of others.

3.3 Obscene Materials -- Using Clearpath's network to advertise, transmit, store, post, display, or otherwise make available child pornography or obscene material. Clearpath is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through Clearpath's network.

3.4 Defamatory or Abusive Language -- Using Clearpath's network as a means to transmit or post defamatory, harassing, abusive, or threatening language.

3.5 Forging of Headers -- Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message. Illegal or unauthorized access to other computers or networks -- Accessing illegally, or without authorization, computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). In addition, any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity).

3.6 Denial Of Service Attacks -- Clearpath reserves the right to null-route any IP address on our network that is under a DoS or DDoS attack that is deemed disruptive to neighboring customers.

3.7 Distribution of Internet Viruses, Worms, Trojan Horses, or Other Destructive Activities -- Distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, ping, flooding, mailbombing, or denial of service attacks. In addition, activities that disrupt the use of or interfere with the ability of other Clearpath customers to effectively use the network or any connected network, system, service, or equipment.

3.8 Internet Relay Chat (IRC) Service -- Clearpath does not support the hosting of IRC servers or bots.

3.9 Export Control Violations -- Exporting encryption software over the Internet or otherwise, to points outside the United States in violation of US Federal Regulations

3.10 Facilitating a Violation of this AUP -- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to spam, initiation of ping, flooding, mailbombing, denial of service attacks, and piracy of software.

3.11 Usenet Groups -- Clearpath reserves the right not to accept postings from newsgroups where we have actual knowledge that the content of the newsgroup violates the AUP.

3.12 Other Illegal Activities -- Engaging in activities that are determined to be illegal, including advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

3.13 Other Activities -- Engaging in activities, whether lawful or unlawful, that Clearpath determines to be harmful to its customers, operations, reputation, goodwill, or customer relations.

4. The responsibility for avoiding the harmful activities described in Section 3 of this AUP rests with the Customer. Clearpath will not, as an ordinary practice, monitor the communications of its Customers to ensure that they comply with the Acceptable Use Policy or applicable law.

5. DMCA -- For information on how to file a DMCA please see the following link and PDF. When sending a DMCA into Clearpath, please use these guidelines and send your completed request into abuse@clearpathsg.com. This e-mail address is being protected from spambots.

Download Example: DMCA.pdf from www.copyright.gov

6. Clearpath is aware that many of its Customers are, themselves, providers of Internet services, and that information reaching Clearpath's facilities from Customers may have originated from an end user of the Customer or from another third-party. Clearpath does not require its Customers who offer Internet services to monitor or censor transmissions or web sites created by end users. Clearpath has the right to directly take action against an end user of a Customer. Also, Clearpath may take action against the Customer because of activities of an end user of the Customer, even though the action may affect other end users of the Customer. Similarly, Clearpath anticipates that Customers who offer Internet services will cooperate with Clearpath in any corrective or preventive action that Clearpath deems necessary and is reasonable. Failure to cooperate with such corrective or preventive measures is a violation of this Acceptable Use Policy. Clearpath also is concerned with the privacy of on-line communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, Clearpath urges its Customers to assume that all of their on-line communications are insecure. Clearpath cannot take any responsibility for the security of information transmitted over Clearpath's facilities.

7. Clearpath will not intentionally monitor private electronic mail messages sent or received by its Customers unless required to do so by law, governmental authority, or when public safety is at stake. Clearpath may, however, monitor its service electronically to determine that its facilities are operating satisfactorily. Also, Clearpath may disclose information, including but not limited to, information concerning a Customer, a transmission made using our network, or a web site, in order to comply with a court order, subpoena, summons, discovery request, warrant, statute, regulation, or governmental request. Clearpath will inform the Customer that Customer information has been provided except in those cases where they may be prohibited by law from giving such notice. Finally, Clearpath, upon notice to the Customer, may disclose Customer information or information transmitted over its network where necessary to protect Clearpath and others from harm, or where such disclosure is necessary to the proper operation of the system.

8. Clearpath expects that its Customers who provide Internet services to others will comply fully with all applicable laws concerning the privacy of on-line communications. A Customer's failure to comply with those laws will violate the Acceptable Use Policy.

9. Any complaints about a customer's violation of this AUP should be sent to abuse@clearpathsg.com. This e-mail address is being protected from spambots.