



PO Box 321 Crowder, OK 74430
918-334-3700 Fax: 918-334-3202

Acceptable Use Policy

As a provider of Internet access, Internet email, web site hosting, and other Internet-related services, Canadian Telephone Co. and cvok.net herein after referred to as "the Provider" offers its subscribers (and their customers, and users), the means to acquire and disseminate a wealth of information. Our network is engineered to provide the highest accessibility available. Factors outside our control may influence that availability. Our staff is on duty 24 hours a day, seven days a week to provide the highest standards of availability in the industry. All service and maintenance related issues are performed strategically to prevent or minimize any interruption of service. The Provider respects that the Internet provides a forum for free and open discussion and dissemination of information. However, there are competing interests at issue. The Provider reserves the right to take certain preventative or corrective actions as deemed necessary. In order to protect these competing interests, the Provider 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 the Provider's services. This AUP will be revised from time to time. A customer's use of the Provider's web site, www.cvok.net, will constitute the customer's acceptance of any new or additional terms of the AUP that result from those changes.

Prohibited Activities

When subscribers disseminate information through the Internet, they also must keep in mind that the Provider does not review, edit, censor, or take responsibility for any information its subscribers 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, information created and carried over the Provider's network may reach a large number of people, including both subscribers and nonsubscribers of the Provider, possibly affecting other subscribers and any harm the Provider's goodwill, business reputation, and operations. For these and other reasons, the Provider has developed an AUP to define prohibited activities:

Spamming—Spamming is sending unsolicited bulk and/or commercial messages over the Internet. It is harmful not only because of its negative impact on consumer attitudes toward the Provider, but also because it can overload the Provider's network and disrupt service to the Provider's subscribers. Such behavior could result in the Provider's mail servers being blacklisted by various anti-spamming organizations subscribed to by other Internet service providers, thus denying the Provider's subscribers access to other parts of the Internet. Also, creating operating or maintaining an open SMTP relay is prohibited. The only acceptable method for creating and maintaining a mailing list for unsolicited commercial email (UCE) or bulk email (UBE) is to have subscribers opt in to the list using secure sockets layer (SSL) authentication, or other means where the user can be positively identified by means of a digital "signature" and the user's choice to receive the bulk or commercial mailings is clear. Opt-out lists, and double negative lists are specifically prohibited. The existence of a "business relationship" between the entity sending and the individual receiving UCE or UBE is not an acceptable justification for the dissemination of UCE or UBE, unless the customer has specifically "opted-in" via verifiable SSL webpage or specific verifiable request via email. When a complaint is received, the Provider has the discretion to determine from all of the evidence whether the email recipients were from an

acceptable “opt-in” email list. Maintainers of such bulk from all of the evidence whether the email recipients were from an acceptable “opt-in” email list. Maintainers of such bulk mailing lists are required to keep verifiable evidence, to include logs for SSL-verified opt-in web pages, or complete headers and text for e-mail requests for a period of 120 days after the addition of each email address to the list. The maintainer of such lists must present this evidence to the Provider upon request. Any domains hosted by the Provider must have working, active mailboxes maintained for “abuse” and “postmaster” aliases. Failure of a responsible party in the company hosted to answer email received by either the postmaster or abuse aliases shall be grounds for termination of the account concerned. The Provider proactively opposes spamming in all forms, and it is the Provider’s policy to immediately interrupt traffic in progress, and terminate subscriber service that may potentially pose harm to the Provider’s business reputation and operations. The Provider reserves the right to terminate, with or without notice, the account of any webhosted service whose website is advertised by or referred to in UCE or UBE. This activity, known as “spamvertising” or the site, known as a “spamadvertised website” is specifically prohibited under the terms of this policy.

Intellectual Property Violations—Intellectual property violations include 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. Also, engaging in activity that violates privacy, publicity, or other personal rights of others is prohibited. The Provider is required by law to remove or block access to customer content upon receipt of a proper notice of copyright infringement. It is also the Provider’s policy to terminate the privileges of subscribers who commit repeat violations of copyright laws. Utilization of services to copy material from third parties (including text, graphics, music, videos or other copyrightable material) without proper authorization is prohibited. See also Other Services.

Obscene Speech or Materials—Obscene speech or materials can include using the Provider’s network to advertise, transmit, store, post, display, or otherwise make available child pornography or obscene speech or material. The Provider is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through the Provider’s network. Using the Provider’s network as a means to transmit or post defamatory, harassing, abusive, or threatening language is also prohibited and grounds for immediate termination of the account concerned, as well as the release of all logs containing such language to the proper investigative government authorities.

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 proper authorization, any computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual’s system (often known as “hacking”). This includes 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). Knowingly engaging in any activities that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any of the Provider customers or end-users whether on the Provider’s network or on another provider’s network is prohibited. Accessing services not included or not paying for: This includes but is not limited to circumventing security, interfering with a service, overloading a service, disabling a host encumbering disk space processors or other system resources. 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. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network,

system, service, or equipment. The Provider may suspend activity of any account whose computer(s) have become infected by a worm or Trojan Horse-type virus, causing the computer to generate unsolicited emails, or where the danger of infecting other users on the Provider's network or any other network is present.

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.

Export Control Violations—Exporting encryption software over the Internet or otherwise, to points outside the United States.

Usenet Groups—The Provider reserves the right not to accept postings or deliver messages from newsgroups where we have actual knowledge that the content of the newsgroup violates the Provider's AUP.

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. Internet connections and all other services provided to the subscriber may only be used for lawful purposes. Transmission or storage of any information, data or material in violation of any U.S. federal or state regulation or law is prohibited.

Other Activities—Engaging in activities, whether lawful or unlawful, that the Provider determines to be harmful to its subscribers, operations, reputation, goodwill, or customer relations.

IRC—The Provider does not allow, maintain, provide, nor support Internet Relay Chat services.

Policy Enforcement—When the Provider becomes aware of an alleged violation of the Acceptable Use Policy, the Provider will initiate an investigation. As the Provider has pointed out, the responsibility for avoiding the harmful activities just described rests primarily with the subscriber. The Provider will not, as an ordinary practice, monitor the communications of its subscribers to ensure that they comply with the Provider's policy or applicable law. When the Provider becomes aware of unauthorized activities, however, it may take any action to stop the unauthorized activity, including but not limited to, removing information, shutting down a website, implementing screening software designed to block offending transmissions, denying access to the Internet, or take any other action it deems appropriate. If such violation is a criminal offense, the Provider will notify the appropriate law enforcement department of such violation.

Third Party—The Provider also is aware that many of its subscribers are, themselves, providers of Internet services, and that information reaching the Provider's facilities from those subscribers may have originated from a customer of the subscriber or from another third party. The Provider does not require its subscribers who offer Internet services to monitor or censor transmissions or web sites created by customers of its subscribers. The Provider has the right to directly take action against a customer of a subscriber. Also, the Provider may take action against the Provider's subscriber because of activities of a customer of the subscriber, even though the action may affect other customers of the subscriber. Similarly, the Provider anticipates that subscribers who offer Internet services will cooperate with the Provider in any corrective or preventive action that the Provider deems necessary. Failure to cooperate with such corrective or preventive measures is a violation of the Provider's policy. The subscriber agrees not to resell products or services without prior written consent from the Provider.

Privacy—The Provider also is concerned with the privacy of online 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, the Provider urges its subscribers to assume that all of their online communications are insecure. The Provider cannot take any responsibility for the security, accuracy, or delivery of information transmitted over the Provider's facilities. The Provider will not intentionally monitor private electronic mail messages sent or received by its subscribers unless required to do so by law, governmental authority, or when public safety is at stake. The Provider may, however, monitor its service electronically to determine that its facilities are operating satisfactorily. Also, the Provider may disclose information, including but not limited to, information concerning a subscriber, a transmission made using our network, or a website, in order to comply with a court order, subpoena, summons, discovery request, warrant, statute, regulation, or governmental request. The Provider assumes no obligation to inform the subscriber that subscriber information has been provided and in some cases may be prohibited by law from giving such notice. Finally, the Provider may disclose subscriber information transmitted over its network where necessary to protect the Provider and others from harm, or where such disclosure is necessary for the proper operation of the system.

Other Services—The Provider may, but is not required to, block incoming or outgoing traffic of any kind, via any protocol. The Provider at its discretion may use Spam filtering and/or virus scanning for both inbound and outbound messages, but instead acts as a secondary safety mechanism and minimizes misuse of network infrastructure and bandwidth. The Provider will not be held responsible for any viruses or emails the subscriber may receive or send via email, nor will the Provider be responsible for lost, misdirected or undeliverable email. The Provider, at its discretion, may apply quality of service (QOS) software and hardware to our network connections which shape bandwidth and transfer of data to best accommodate the needs of the network. This can include prioritizing traffic to insure customers have the optimal opportunity to surf the web and utilize email include but not limited to bandwidth shaping, traffic prioritizing, and caching. The Provider, at its discretion, may apply advertising or banners as deemed necessary.

Legal—The Provider expects that its subscribers who provide Internet services to others will comply fully with all applicable laws concerning the privacy of online communications. A subscriber's failure to comply with those laws will violate the Provider policy. Finally, the Provider wishes to emphasize that in utilizing the Provider's services and network, subscribers indemnify the Provider for any violation of the service agreement, law, or the Provider's policy, that results in loss to the Provider or the bringing of any claim against the Provider is sued because of a subscriber's or customer of a subscriber's activity, the subscriber will pay any damages awarded against the Provider, plus costs and reasonable attorney's fees. 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 subscribers obtain information through the Internet, they must keep in mind that the Provider cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that subscribers may acquire. For this reason, the subscriber 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 the Provider cannot monitor or censor the Internet, and will not attempt to do so, the Provider cannot accept any responsibility for injury to its subscribers that results from inaccurate, unsuitable, offensive, or illegal Internet communications. By utilizing this service the subscriber and the subscriber's customers agree to defend, hold harmless, and expeditiously indemnify the Provider from any and all liability, claim, loss, damage or expense arising out of breach or violation of any covenant contained in this policy, or resulting from use of the service. It is further agreed that the subscriber and the

subscriber's customers agree to waive and hold the Provider harmless for any claims relating to any action taken as part of an investigation into a suspected violation of this Policy or as a result of its conclusion that a violation of this Policy has occurred. Therefore, neither the subscriber nor the subscriber's customers can sue or recover any damages whatsoever from the Provider as a result of the decision to remove material from the Provider's server, or to suspend or terminate any account. The subscriber further agrees to defend, indemnify, and hold harmless the Provider against any claim arising from the subscribers customers. This service(s) is provided "as is". The Provider makes no warranties, expressed or implied, of any kind. This includes but is not limited to business claims, accuracy, security, performance, privacy, or the fitness for any specific purpose.

We hope this AUP is helpful in clarifying the obligations of Internet users, including the Provider and its subscribers, as responsible members of the Internet. Any complaints about a subscriber's violation of this AUP should be sent to cvstaff@cvok.net.