WTC Acceptable Use Policy

WTC Communications' AUP (Acceptable Usage Policy") is provided to give our customers and users a clear understanding of what WTC Communications expects of them while using the service. All users of WTC Communications' Internet services: including those who access any of our Services but do not have accounts, as well as those who pay a service fee to subscribe to the Services, must comply with this AUP and our TOS (Terms of Service).

Use of WTC Communications Service constitutes acceptance and agreement to WTC Communications' AUP as well as WTC Communications' TOS (Terms of Service).

WTC Communications strives to provide its customers with the highest quality Internet service available and at the same time respect the standards that have been created within the Internet community. To that end, WTC Communications believes that certain activities and conduct is inappropriate or abusive and will not be tolerated on the WTC Communications network.

WTC Communications supports the uncensored flow of information and ideas over the Internet and does not actively monitor subscriber activity under normal circumstances. Similarly, we do not exercise editorial control over the content of any web site, e-mail transmission, newsgroups, or other material created or accessible over or through the services. However, in accordance with our TOS (Terms of Service), we may remove any materials that, in our sole discretion, may be considered or thought to be illegal, may subject us to liability, or which may violate this AUP. WTC Communications will cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrongdoing. Your violation of this AUP may result in the suspension or immediate termination of either your WTC Communications account or other actions as detailed in this AUP WITHOUT PRIOR NOTICE.

VIOLATIONS OF WTC COMMUNICATIONS ACCEPTABLE USE POLICY

The following activities constitute violations of this AUP:

Dialup Access: WTC Communications works hard to provide our dialup users with the best possible access across traditional POTs and ISDN lines. To that end, users are expected to use the service in a reasonable manner including but not limited to e-mail, newsgroups, file transfers, Internet chat, online games, and browsing the World Wide Web. High volume or commercial use including but not limited running a server of any sort is strictly prohibited.

WTC Communications will periodically review connections and terminate those connections which have not been actively passing traffic for a period of time. Any attempt by the user to circumvent this policy may result in a significant upcharge on the user's bill. A dialup account is intended for use by one user, simultaneous login attempts from multiple users is not allowed.

Inappropriate Use of Software: Use of software or any device that would facilitate a continued connection on a dialup service, i.e. automated ping programs, while using WTC Communications services could result in suspension of service.

Your FREE Personal Web Page: Most residential WTC Communications access accounts include

FREE personal web space. WTC Communications does not routinely monitor the contents of your personal web page(s) or the network transfer that originates from such. You are solely responsible for any information contained on your personal web page(s). However, if complaints are received regarding language, content or graphics contained on your personal web page(s), WTC Communications may, at its sole discretion, remove the personal web page(s) hosted on WTC Communications servers and revoke your access to that space.

You may not use your personal web site to publish material, which WTC Communications determines, at its sole discretion, to be unlawful, indecent or objectionable. For purposes of this policy, "material" refers to all forms of communications including narrative descriptions, graphics (including photographs, illustrations, images, drawings, logos), executable programs, video recordings, and audio recordings. NO ADULT orientated material may be stored in your personal web space or displayed on your personal web page(s).

This space is not to be used for commercial activities. Client side scripting may be used at your discretion, however, WTC Communications' phone support will not provide in-depth support for any of the above listed services. If you feel you need additional services such as administrative control over your domain, greater scripting capabilities, and your own domain name then please consider our hosting packages starting at just $20/month.

Note: We want you to get the best possible use out of your FREE web space. If your traffic becomes problematic or excessive, we will ask that it be removed or that you purchase a domain hosting account to better suit your needs. As always, your site will be subject to all other provisions of this AUP and TOS.

Hosted Domain Account: You may not use your hosted domain site to publish material, which WTC Communications determines, at its sole discretion, to be unlawful, indecent or objectionable. For purposes of this policy, "material" refers to all forms of communications including narrative descriptions, graphics (including photographs, illustrations, images, drawings, logos), executable programs, video recordings, and audio recordings. NO ADULT orientated material may be stored in your hosted domain site or displayed on your hosted domain pages.

If you feel your site is of a questionable nature, please contact us before you sign up and we can discuss your intentions.

Illegal use: Use of the WTC Communications service to transmit any material (by e-mail, uploading, posting or otherwise) that, intentionally or unintentionally, violates any applicable local, provincial, federal, or international law, or any rules or regulations promulgated thereunder. Examples of such activities, includes but is not limited to, posting illegal copies of software on our news server or providing such software from your web space.

Threats: Use of the WTC Communications service to transmit any material (by e-mail, uploading, posting or otherwise) that threatens or encourages bodily harm, encourages destruction of property or promotes senseless hatred toward other groups of people in society is not permitted. This also includes communications or transmissions of any sort to others intended for the purpose of planning unspeakable acts against society.

Harassment: Use of the WTC Communications service to transmit any material (by e-mail, uploading, posting or otherwise) that harasses another user or member of society is not permitted.

Harm to minors: Use of the WTC Communications service to harm, or attempt to harm, minors in any way, including, but not limited to child pornography or sexual solicitation is not permitted and may result in criminal charges.

Forgery or impersonation: Adding, removing or modifying identifying network header information in any manner in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames is discouraged but does not constitute impersonation.

E-mail / News Bombing: Malicious intent to impede another person's use of electronic mail services or news media will result in the immediate termination of the offending WTC Communications account.
E-mail / Message Forging: Forging any message header, in part or whole, of any electronic transmission, originating or passing through the WTC Communications service is in violation of this AUP and may result in account termination.

Unsolicited commercial e-mail / Unsolicited bulk e-mail (SPAM): Use of the WTC Communications service to transmit any unsolicited commercial or unsolicited bulk e-mail is expressly prohibited. Violations of this type will result in the immediate suspension and possible termination of the offending WTC Communications account. Each report of SPAM by another user or third party will incur a fee according to the TOS. Accounts found sending virus after notification by WTC Communications will be considered SPAMMING and result in service distruption and fees outlined in section 3 of the **TOS**.

Persons and or Businesses using WTC Communications' network to propagate e-mail lists are not exempt from this policy or the fees. Such e-mail lists, commonly called list servers, must present the user with a verification of their subscription prior to sending e-mail to the recipient. This verification process must also be able to provide proof of the recipient's approval to prevent account termination. WTC Communications, at its sole discretion, may terminate any account if complaints regarding the e-mail list(s) become excessive

Usenet SPAMing: WTC Communications has a zero tolerance policy for the use of its network for the posting of messages or commercial advertisements, which violate the rules, regulations, FAQ or charter of any newsgroups or mailing list. Commercial messages that are appropriate under the rules of a newsgroup or mailing list or that are solicited by the recipients are permitted.

Unauthorized access: Use of the WTC Communications service to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of WTC Communications' or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is expressly prohibited and the offending WTC Communications account is subject to immediate termination.

Infringement of Copyright, Patent, Trademark, Trade Secret, or Intellectual Property Right: Use of the WTC Communications service to transmit any material (by e-mail, uploading, posting, peer to peer or otherwise) that infringes any copyright, trademark, patent, trade secret or other proprietary rights of any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or

other copyrighted sources, and the unauthorized transmittal of copyrighted software. In accordance with Canadian Copyright laws, all notifications regrading Copyright Infringement will be passed along to the Subscriber and assessed an Investigation Fee of $50.00 that will be applied against the Subscribers account.

Collection of personal data: Use of the WTC Communications service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is not permitted. Any user found in violation of this policy may be reported to the appropriate authorities.

Network disruptions and unfriendly activity: Use of the WTC Communications service for any activity which affects the ability of other people or systems to use WTC Communications Services or the Internet. This includes, but is not limited to, "denial of service" (DOS) and "distributed denial of service" (DDOS) attacks against another network host or individual user. Interference with or disruption of other network users, services or equipment is prohibited. It is the Subscriber's responsibility to ensure that their network is configured in a secure manner. A Subscriber may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A Subscriber may not permit their network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner. Unauthorized entry and/or use of another company and/or individual's computer system will result in immediate account suspension or termination. WTC Communications will not tolerate any subscriber attempting to access the accounts of others, or penetrate security measures of other systems, whether or not the intrusion results in corruption or loss of data. Ignorance of such activity originating from a Subscriber's equipment is no excuse and service will be suspended until such time that the offense is rectified.

Network Security: It is the responsibility of the individual to ensure the security of their connected computers or devices. This includes but is not limited to virus protection, firewalls, correct configuration of services, etc.

WTC Communications reserves the right to periodically scan its IP address base for security reasons. Any security violation will result in a notification to the customers kingston.net address and access to the un-secured service will be disabled until the individual notifies WTC Communications that the problem has been rectified.

Repeat violations will result in fees levied according to the TOS. Violations of this type may result in the immediate suspension and possible termination of the offending WTC Communications account.

Fraud: Involves a knowingly misrepresentation or misleading statement, writing or activity made with the intent that the person receiving it will act upon it.

Fraudulent activity: Use of WTC Communications service to make fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "ponzi schemes," and "chain letters."

Distribution of Viruses or Hostile software: Intentional distributions of software that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems are prohibited. Such an offense will result in the immediate termination of the offending account.

Reselling the services: Reselling of WTC Communications service without our express written

authorization is prohibited.

Third Party Accountability: WTC Communications subscribers will be held responsible and accountable for any activity by third parties, using their account, that violates guidelines created within the Acceptable Use Policy. This includes but is not limited to DSL and other dedicated customers who are running servers connected through WTC Communications access. Applicable fines may apply.

Mail Box usage: As the primary account holder, you are responsible for all account activity. All provisions of the Acceptable Use Policy apply to your use of all e-mail boxes. Misuse of Extra E-mail Boxes services may result in termination of your account. If a secondary mailbox is involved in a violation of the Acceptable Use Policy, your account, including all secondary mailboxes may be terminated. A terminated account will result in lost e-mail and Internet access for all users of your account. Therefore, it is important that your make sure everyone you will allow to use your account or a secondary mailbox understands all terms of this Acceptable Use Policy and the consequences of violations.

Security: You are responsible for any misuse of your account, even if the inappropriate activity was committed by a friend, family member, guest or employee. You must adopt adequate security measures to prevent or minimize unauthorized use of your account by taking steps to ensure that others do not gain unauthorized access to your account. In addition, you may not use your account to breach security of another account or attempt to gain unauthorized access to another network or server.

Password Privacy and Protection: Your password provides access to your account. It is your responsibility to keep your password secure. Sharing your password and account access with unauthorized users is prohibited. You should take care to prevent others from using your account since you will be held responsible for such use. User accounts will be terminated immediately if WTC Communications feels your password has been compromised.

Network and Personal Security: Users who violate systems or network security may incur criminal and/or civil liability. WTC Communications will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations. Attempting to obtain another user's account password is strictly prohibited, and may result in termination of service. You may not attempt to circumvent user authentication or security of any host, network or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks. Use or distribution of tools designed for compromising security is prohibited. Examples of these tools include, but are not limited to, password guessing programs, cracking tools or network probing tools.

Network Performance: WTC Communications accounts operate on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited by this policy and may result in termination of your account.

a) You are prohibited from excessive consumption of resources, including CPU time, memory, disk space and session time. You may not use resource-intensive programs which negatively impact

other customers or the performances of WTC Communications systems or networks. WTC Communications reserves the right to terminate or limit such activities. This includes, but is not limited to, unattended processes running on our web server.

b) You may not establish more than one connection to our network from your account at any one time, unless your account is permitted to do so.

c) You may not provide network services from your account (for example, you may not use your account to operate an ftp, mail or a web server), unless your account type specifically provides for it. Currently DSL with static IP addresses and Dedicated accounts have the ability to provide these services. Subscribers with Wireless Internet accounts are not permitted to run servers from their connection. Any account(s) found in violation will incur an investigation fee as per section 4 of the **ToS**

d) Each customer account will be provided 20 MB of total disk storage for e-mail boxes. Messages left on WTC Communications' mail servers for more than thirty days (30 days) are subject to immediate deletion read or unread. Total mailbox storage is limited to 20MB per account without regard to the age of the messages in any of the mailboxes. Once the 20MB limit is exceeded, any incoming messages will be returned to the sender until the subscriber reduces mailbox size by removing mail from the server. Additional capacity may be purchased in some of the packages, please contact **sales@wtccommunications.ca**.

e) You may not employ automated electronic or mechanical processes designed to defeat network inactivity time-outs. Such tools include, but are not limited to, use of an auto-dialer and repetitive pinging of a host.

Internet Relay Chat: Although WTC Communications does not offer technical support for Internet Relay Chat (IRC), you may use your account to connect to IRC; servers and networks maintained by WTC Communications or third parties. Please remember that you are a guest when you make use of these facilities. It is particularly important that you do not engage in activities which might interfere with other customers' access to IRC.

a) You may not use IRC scripts or programs that interfere with or deny service to other users on any other server, host, network or channel.

b) You may not engage in activities which harass other users. This includes, but is not limited to, "flooding" (rapidly entering text with the intent to disrupt service), "flashing" (disrupting terminal emulation), "takeovers" (improper seizure and abuse of operator privileges), attempting to send private messages to those who do not wish to receive them, attempting to return to a channel after being banned from it, and other disruptive behaviors.

c) You may not attempt to impersonate other users. The use of nicknames does not constitute impersonation.

d) You may not run "clones" (multiple simultaneous IRC connections).

e) You may not attempt to run IRC bots on our servers at any time.
Applications Expressly Banned on WTC

Communications Servers: The following applications and any of their derivatives are banned from our servers:

- Eggdrop
- Bitchx
- ircd
- linsniff

The servers are monitored for the presence of these applications and their existence on the filesystem. Any user found in possession of these programs will be warned once, further infractions will be viewed as a disregard for the AUP and service will be terminated. Attempts to store or run these programs under different names will result in the same actions being taken against the user.

REPORTING VIOLATIONS OF WTC COMMUNICATIONS' AUP

WTC Communications requests that anyone who believes that there is a violation of this AUP direct the information to the Abuse Department at **abuse@wtccommunications.ca**.

If available, please provide the following information:

- The IP address used to commit the alleged violation
- The date and time of the alleged voilation, including the time zone or offset from GMT
- Evidence of the alleged violation

Failure to provide sufficient information, as deemed by WTC Communications, will result in a dismissal of the complaint. WTC Communications regards reports of abuse with the utmost seriousness and require legitimate information as to avoid falsely accusing users. False accusations will result in reports filed against the reporting party to the appropriate contacts.

- Issue written or verbal warnings
- Suspend the Subscriber's newsgroups posting privileges
- Suspend the Subscriber's account
- Terminate the Subscriber's account
- Bill the Member for administrative costs and/or reactivation charges
- Bring legal action to enjoin violations and/or to collect damages, if any, cause by violations

REVISIONS TO THIS ACCEPTABLE USE POLICY

WTC Communications reserves the right to revise, amend, or modify this AUP, our TOS (Terms of Service) and our other policies and agreements at any time and in any manner. Notice of any revision, amendment, or modification will be posted in accordance with our TOS (Terms of Service).