Carr Acceptable Use Policy

This Acceptable Use Policy ("AUP") has been created to promote the integrity, security, reliability and privacy of Carr DSL Broadband Internet Service ('Service'). The AUP works in conjunction with the Terms of Service Agreement ("Agreement") of each particular Service, and specifies actions that are prohibited by users of the Service. Carr reserves the right to modify the AUP at any time, and any such modifications shall be automatically effective to all users when adopted by Carr. The End User recognizes and agrees that the online AUP to be maintained by Carr will supersede all previous versions of this document.

Use of the Service is subject to the following rules and guidelines as well as service- specific Agreements. Each End User of the Service is responsible for ensuring that the use of all services provided complies with this AUP and associated Terms of Service Agreement. Any user who does not agree to be bound by these terms should immediately stop their use of the Service and notify Carr Customer Service to terminate the account.

Illegal Use

The Service may be used only for lawful purposes. Transmission, reception, storage and/or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat or violates export control laws. Furthermore, use of the Service to impersonate a person or entity is not permitted.

System and Network Security

Violations of system or network security are prohibited and may result in criminal and civil liability Examples of system or network security violations include, without limitation, the following:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network, relay communication through a resource or to breach security or authentication measures without express authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network.
- Interference with service to any user, host or network, including but not limited to mail bombing, flooding or denial of service attacks.
- Forging the header of any transmitted information packet, e-mail or Usenet posting.
- Modifying or tampering with any hardware, software or configuration provided by Carr including but not limited to routers, switched, and cable modem configuration files.
- Disrupting any aspect of the Carr Internet Network through any means.
- Excessive use of bandwidth, that in Carr's sole opinion, goes above normal usage or goes beyond the limit allocated to the End User.
- Assuming or assigning an Carr IP address that was not allocated to the user by Carr or its network-all residential users must use DHCP to acquire an IP address, business users should refer to the specific product TOS for further clarification.

Electronic Mail

Spam- Carr defines "spam" as any e-mail or electronic communication including, but not limited to, instant messenger programs, IRC, Usenet, etc. that promotes or advertises a service, product, cause, opinion, money making opportunity or the like that the recipient did not specifically request from the sender. The communication does not necessarily have to pass through the Service's e-mail infrastructure – it only needs to originate from a service user. Residential service users may not send any communication meeting the definition above regardless of whether the recipient requested it or not. Business users should refer to their Terms of Service Agreement for further clarification of this issue.

Carr maintains a zero-tolerance policy on spam for all of its internet services and will take immediate action against users violating this policy.

Carr internet services may not be used to collect responses from unsolicited email regardless of the e-mail's origination. Moreover, unsolicited e-mail may not direct the recipient to any Web site or other resource that uses the Service and the user may not reference the Service in the header or by listing an IP address that belongs to the Service in any unsolicited e-mail even if that e-mail is not sent through the Service of its infrastructure.

End Users may not send any type of communication to any individual who has indicated that he/she does not wish to receive messages from them. Continuing to send e-mail messages to anyone that has expressly requested not to receive e-mail from you is considered to be harassment.

USENET/Internet Chat

Users may not spam newsgroups or chat rooms and must comply with the written charters, FAQs, rules or terms of service for those forums the user chooses to participate. The user is responsible for determining the policies of a given group/room before posting to it. Additionally, users are not permitted to:

- Cross-post the same or substantially similar message excessively-in Carr's sole opinion.
- Post binary files to non-binary groups.
- Flood or disrupt a group

Abuse Resources

End User shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abuse resources include but are not limited to: open news servers, open SMTP servers, insecure routers, wireless access and insecure proxy servers. Upon notification from Carr, users are required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this AUP. Not all services permit use of these types of services, please refer to your Terms of Service Agreement for further clarification.

End User Responsibility

The End User is solely responsible for the security and misuse of any device that is connected to the Service. Carr recommends that users implement appropriate measures to secure their systems, and these measures may include installation of firewalls, antivirus protection with regular updates, regularly checking for and applying security patches for software and operating systems and general security conscience use of the Service.

Viruses

Service users must take appropriate action to prevent their systems from becoming infected with and/or distributing computer viruses. Carr will take appropriate (as decided by Carr) action against users infected with computer viruses or worms to prevent further spread.

Enforcement

Carr reserves the right to investigate violations of this AUP, including the gathering of information from the user or users involved and the complaining party, if any, and the examination of material on Carr's servers and network. Carr prefers to advise customers of AUP violations and any necessary corrective action but, if Carr, in its sole discretion, determines that a user has violated the AUP, Carr will take any responsive action that is deemed appropriate without prior notification. Such action includes but is not limited to temporary suspension of service, reduction of service resources, and termination of service. Carr is not liable for any such responsive action and these actions are not exclusive. Carr may take any other legal to technical action it deems appropriate.

The failure of Carr to enforce this policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time.