



## Acceptable Use Policy for Internet Service

The Acceptable Use Policy (AUP) has been created by Lightpath to promote the integrity, security, reliability and privacy of Lightpath's network. The AUP works in conjunction with the Internet Terms & Conditions and specifies actions that are prohibited by users of the Lightpath network. Lightpath reserves the right to modify the AUP at any time and any such modification shall be automatically effective as to all users when adopted by Lightpath.

Use of the Service is subject to the following rules and guidelines as well as product specific Terms & Conditions included with this Agreement. Each Customer of the Service is responsible for ensuring that the use of all Services provided complies with this AUP and associated Terms & Conditions. Any user who does not agree to be bound by these terms should immediately stop their use of the Service and notify their Customer Service Department to terminate the account.

### 1. Illegal Use

The Service may be used only for lawful purposes. Transmission 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.

### 2. 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 limitations, 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 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 of the system or network.
- Interference with Service by any user, host or network including, without limitation, mail bombing, flooding, or denial of service attacks.
- Forging the header of any transmitted information packet, email or Usenet posting.
- Modifying or tampering with any hardware, software, or configuration provided by Lightpath including but not limited to routers, switches, and cable modem configuration files.
- Disrupting any aspect of the Lightpath Internet Network through any means.
- Excessive use of bandwidth, that in Lightpath's sole opinion, goes above normal usage or goes beyond the limit allocated to the user.
- Assuming or assigning a Lightpath IP address that was not allocated to the user by Lightpath or its network. All residential users must use DHCP to acquire an IP address. Business users should refer to the specific product Terms & Conditions for further clarification.

### 3. Electronic Mail

**Spam** – Lightpath defines Spam ("SPAM") as any email 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 email 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 contract for further clarification of this issue.

Lightpath maintains a zero-tolerance policy on SPAM for all of its internet products and will take immediate action against users violating this policy.

Lightpath's Internet Service may not be used to collect responses from unsolicited email regardless of the email's origination. Moreover, unsolicited email 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 email even if that email is not sent through the Service or its infrastructure.

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 email messages to anyone that has expressly requested not to receive email from you is considered to be harassment.

#### **4. 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 – Lightpath’s sole opinion
- Post binary files to non-binary groups
- Flood or disrupt a group

#### **5. Abusable Resources**

Customers shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abusable resources include but are not limited to open news servers, open SMTP servers, insecure routers, wireless access and insecure proxy servers. Upon notification from Lightpath, 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 products permit use of these types of services, please refer to your product specific Terms & Conditions for further clarification.

#### **6. User Responsibility**

The user is solely responsible for the security and misuse of any device that is connected to the Service. Lightpath 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.

#### **7. Viruses**

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

#### **8. Enforcement**

Lightpath 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 Lightpath’s servers and network. Lightpath prefers to advise customers of AUP violations and any necessary corrective action but if Lightpath, in its sole discretion, determines that a user has violated the AUP, Lightpath 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. Lightpath is not liable for any such responsive action and these actions are not exclusive. Lightpath may take any other legal or technical action it deems appropriate.

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