



ACCEPTABLE USE POLICY FOR LITECAST / BALTICORE

This Acceptable Use Policy applies to all persons and entities (collectively, “customers”) using the products and services of Litecast/Balticore, LLC (“Litecast”) including Internet service. The policy is designed to protect the security, integrity, reliability, and privacy of both the Litecast network and the products and services Litecast offers to its customers. Litecast reserves the right to modify this policy at any time, effective immediately upon posting of the modification. Your use of Litecast’s products and services constitutes your acceptance of the Acceptable Use Policy in effect at the time of your use. You are solely responsible for any and all acts and omissions that occur during or relating to your use of the service, and you agree not to engage in any unacceptable use of the service.

WHAT USES ARE PROHIBITED?

Unacceptable use includes, but is not limited to, any of the following:

1. Posting, transmission, re-transmission, or storing material on or through any of Litecast’s products or services, if in the sole judgment of Litecast such posting, transmission, re-transmission or storage is: (a) in violation of any local, state, federal, or non-United States law or regulation (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations); (b) threatening or abusive; (c) obscene; (d) indecent; or (e) defamatory. Each customer shall be responsible for determining what laws or regulations are applicable to his or her use of the products and services.
2. Installation or distribution of “pirated” or other software products that are not appropriately licensed for use by customer.
3. Deceptive marketing practices.
4. Actions that restrict or inhibit anyone - whether a customer of Litecast or otherwise - in his or her use or enjoyment of Litecast’s products and services, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.
5. Introduction of malicious programs into the Litecast network or servers or other products and services of Litecast (e.g., viruses, trojan horses and worms).
6. Causing or attempting to cause security breaches or disruptions of Internet communications. Examples of security breaches include but are not limited to accessing data of which the customer is not an intended recipient, or logging into a server or account that the customer is not expressly authorized to access. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.
7. Circumventing user authentication or security of any host, network or account.
8. Interfering with or denying service to any user other than the customer’s host (e.g., denial of service attack).
9. Using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable a user’s terminal session.
10. Failing to comply with Litecast’s procedures relating to the activities of customers on Litecast-owned facilities.
11. Furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document “use” of Litecast’s products or services.

12. PURPOSE—This document outlines the requirements for sending bulk e-mails.

INTRODUCTION—Major Internet service providers take a number of steps to protect their members/customers from unsolicited bulk e-mail. These include automated filters which block messages displaying certain characteristics and/or from suspect Internet addresses. Litecast Customer may need to initiate legitimate (i.e., solicited) bulk mailings. To ensure timely delivery of such messages, they must adhere to certain technical and other requirements, listed below.

Failure to comply with these requirements can potentially result in all of Litecast Customer's messaging systems being blocked from delivering messages to major service providers.

RESPONSIBILITIES—The manager of any Litecast Customer system or application used to generate bulk emailings must ensure that the mailings comply with the applicable technical, formatting, and policy and procedural requirements outlined below.

GUIDELINES—Technical Requirements

- All e-mail must be RFC compliant.

E-mail Formatting Requirements:

- E-mail must be compliant with the federal Can Spam Act of 2003, available at <http://www.spamlaws.com/federal/can-spam.shtml>.
- Persons transmitting mail must not do anything that tries to hide, forge or misrepresent the sender of the e-mail and sending site of the e-mail.
- Bulk mailings must specifically state how e-mail addresses were obtained, and must indicate the frequency of the mailing. Such details as the date and time when the e-mail address was obtained along with the IP address of the subscriber and the web site they visited to sign-up must be made available to providers upon request.
- Bulk mailings should contain simple and obvious unsubscribe mechanisms. The preferred method is to provide a working link to a one-click unsubscribe system; however, a valid "reply to:" address may be used instead.
- All subscription based e-mail must have valid, non-electronic, contact information for the sending organization in the text of each e-mail including phone number and a physical mailing address.

Policy and Procedural Requirements:

- All bulk e-mail must be solicited, meaning that the sender has an existing and provable relationship with the e-mail recipient and the recipient has not requested not to receive future mailings from the sender. Documentation of the relationship between the sender and the recipient must be made available to the provider upon request.
- Use of unsolicited E-mail originating from within the Litecast network or networks of other Internet Service Providers on behalf of or to advertise any service hosted by Litecast or connected via the Litecast network.
- Exporting, re-exporting, or permitting downloads of any content in violation of the export or import laws of the United States or without all required approvals, licenses and exemptions.
- No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such a provision shall be disregarded and the balance of the policy shall remain in effect.

13. Enforcement

Litecast may immediately suspend and/or terminate the customer's service for violation of any provision of this policy upon verbal or written notice, which notice may be provided by voicemail or E-mail. Prior to suspension or termination, Litecast attempts to work with our customers to cure violations of this policy and ensure that there is no re-occurrence; however, Litecast reserves the right to suspend or terminate service after a 30 day "cure" to correct the offense.

14. Electronic Communications Privacy Act Notice

Litecast makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Litecast technology, and makes no guarantee that any other entity or group of users will be included or excluded from Litecast's network. In addition, Litecast may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act, P.L. No. 99-508, as amended.