



Introduction

This Acceptable Use Policy ("AUP") sets forth the principles that govern the use by customers of the systems ("Customer"), services and products provided by Cast Web Design ("Company"). The AUP has been created to promote the integrity, security, reliability and privacy of Company's systems and networks.

Compliance With Law

Customer shall not post, transmit, re-transmit or store material on or through any of Company's system services or products that: (i) is in violation of any local, state, federal or non-United States law or regulation; (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons"); or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer.

Prohibited Uses of Company's Systems, Services and Products

This AUP identifies the actions that the Company considers to be abusive, and thus, strictly prohibited. In addition to the other requirements of this AUP, Customer may only use the Company's systems, services and products in a manner that, in the Company's sole judgment, is consistent with the purposes of such systems, services and products. If Customer is unsure whether a contemplated use or action is permitted under the AUP, Customer should e-mail Company with a description of the proposed use at info@castwebdesign.com for a determination as to whether the use is permissible under this AUP. The examples identified in the subsections below are non-exclusive and are provided, in part, for guidance purposes.

The following uses of Company's systems, services and products as described in subsections A through E are expressly prohibited:

A. Prohibited Actions: General Conduct

1. Transmitting on or through any of Company's systems, services, or products any material that is, in Company's sole discretion, unlawful, obscene, threatening, abusive, libelous, or hateful, or encourages conduct that may constitute a criminal offense, may give rise to civil liability, or otherwise may violate any local, state, national or international law.
2. Transmission, distribution, or storage of any information, data or material in violation of United States or state regulations or law, or by the common law.
3. Violations of the rights of any Person protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.
4. Actions that restrict or inhibit any Person, whether Customer of the Company or otherwise, in its use or enjoyment of any of the Company's systems, services or products.
5. Resale of Company's services and products, without the prior written consent of Company.
6. Deceptive on-line marketing practices.
7. Furnishing false data on the signup form, contract, or on-line application, including fraudulent use of credit card numbers (such conduct is ground for immediate termination and may subject the offender to civil or criminal liability).

B. Prohibited Actions: System and Network Security

1. Attempting to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for Customer, logging

into a server or account Customer is not expressly authorized to access, or probing the security of other networks (such as running a SATAN scan or similar tool).

2. Effecting security breaches or disruptions of Internet communications. Security breaches include, but are not limited to, accessing data of which Customer is not an intended recipient or logging onto a server or account that Customer is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, and attempts to "crash" a host.
3. Using any program/script/command, or sending messages of any kind, designed to interfere with a user's terminal session, by any means, locally or by the Internet.
4. Executing any form of network monitoring which will intercept data not intended for Customer.
5. Sharing of passwords or accounts with others who are not authorized access.

C. Prohibited Actions: E-Mail

1. Harassment, whether through language, frequency, or size of messages, is prohibited.
2. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material ("e-mail spam"). Customers are explicitly prohibited from sending unsolicited bulk mail messages. This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, and political tracts. Such material may only be sent to those who have explicitly requested it. If a recipient asks to stop receiving e-mail, Customer must not send that person any further e-mail.
3. Creating or forwarding "chain letters" or other "pyramid schemes" of any type, whether or not the recipient wishes to receive such mailings.
4. Malicious e-mail, including, but not limited to, "mail bombing" (flooding a user or site with very large or numerous pieces of e-mail).
5. Unauthorized use, or forging, or mail header information.
6. Using a Company or Customer account to collect replies to messages sent from another provider.
7. Use of unsolicited e-mail originating from Company network or networks of other Internet Service Providers on behalf of, or to advertise any service hosted by Company, or connected via Company network or networks.
8. Willful failure to secure open SMTP ports so as to prevent the unauthorized use of Customer resources for the purposes of sending unsolicited e-mail by a third party.

D. Prohibited Actions: Usenet Newsgroups

1. Posting the same or similar messages to large numbers of Usenet newsgroup ("Newsgroup spams or USENET spam").
2. Posting chain letters of any type.
3. Posting encoded binary files to newsgroups not specifically named for that purpose.
4. Cancellation or superseding of posts other than your own, with the exception of official newsgroup moderators performing their duties.
5. Forging of header information. This includes attempting to circumvent the approval process for posting to a moderated newsgroup.
6. Solicitations of mail for any other e-mail address other than that of the poster's account or service, with intent to harass or to collect replies.
7. Postings that are in violation of the written charters or FAQ's for those newsgroups.
8. Posting of Usenet articles from Company network or networks of other Internet Service Providers on behalf of, or to advertise any service hosted by Company, or connected via Company network or networks.
9. Failure to secure a news server so as to prevent the unauthorized use of Customer resources by a third party which may result in Usenet posts that violate this policy.
10. Advertisements posted in newsgroups whose charters/FAQ's explicitly prohibit them. The poster of an advertisement or other information is responsible for determining the etiquette of a given newsgroup, prior to posting to it.

Complaint and Enforcement

A. Complaint

Complaints regarding abusive conduct may be reported by email to info@castwebdesign.com or by mail to:

Cast Web Design
3184 S. Chestatee St.
Dahlonega, GA 30533

Complaints will also be accepted via e-mail, so long as a valid return address is included. Company must be able to independently verify each instance of abuse, and so each complaint must include the COMPLETE TEXT OF THE OBJECTIONABLE MESSAGE, INCLUDING ALL HEADERS. Please do NOT send excerpted parts of a message; sending a copy of the entire message, including headers, helps to prevent misunderstandings based on incomplete information, or information used out of context. Full headers demonstrate which path the message has taken, and enable us to determine whether any part of the message has been forged. This information is vital to our investigation.

B. Enforcement

Company may, in its sole discretion, suspend or terminate Customer's service for violation of any of AUP at any time and without warning. AS a general matter, Company attempts to work with customers to cure violations and to ensure that there is no re-occurrence of the violation prior to terminating service.

Liability

In no event will Company be liable to any customer or third party for any direct, indirect, special or other consequential damages for actions taken pursuant to this AUP, including, but not limited to, any lost profits, business interruption, loss of programs or other data, or otherwise, even if Company was advised of the possibility of such damages.

Miscellaneous

A. Modification of AUP

Company retains the right to modify the AUP at any time and any such modification shall be automatically effective as to all Customers when adopted by Company.

B. Applicability of AUP

The actions listed herein are also not permitted from other Internet Service Providers. Deceptive marketing, as defined by the Federal Trade Commission Deception Policy Statement, is not permitted through the Company services, network or networks. These rules apply to other types of Internet-based distribution mediums as well, such as RLG's Ariel system (a system for sending FAX-like documents over the Internet).

C. Company Is Not Responsible For Content

Company is not responsible for the content of any USENET posting, whether or not the posting was made by a Customer of Company.

D. Removal of Materials

At its sole discretion, Company reserves the right to remove materials from its servers and to terminate internet access to customers that Company determines have violated this AUP