



Acceptable Use Policy

This Acceptable Use Policy (AUP) specifies the actions prohibited by Stelle Telephone Company (STC) by customers and users of internet services provided by STC.

Customer agrees to not use, nor shall it permit others to use, the Services:

- 1) for any unlawful, invasive, infringing, defamatory, fraudulent, or obscene purpose, in accordance with state and federal laws.
- 2) to send unsolicited email of any kind, regardless of the content or nature of such messages or post the same or similar message to one or more newsgroups.
- 3) to send any virus, worm, Trojan horse, or harmful code or attachment.
- 4) to alter, steal, corrupt, disable, destroy, trespass or violate any security or encryption of any computer file, database or network so as to interfere with the use of the STC network by other customers or authorized users.
- 5) in a manner which is inconsistent with the generally accepted rules of Internet etiquette and conduct.
- 6) to resell or distribute the services to third parties without Stelle Telephone Company's written consent. Use of any transmitter, router or wide area network that enables person or entities outside your service address to use the services, whether or not a fee is sought, is prohibited. If the customer, or a third party through customer, violates any of the foregoing prohibitions, STC may immediately suspend the Services and/or terminate this Agreement without further liability or obligation to the customer.
- 7) to impersonate any person on the STC services or communicate under a false name, including forging of any TCP/IP packet header or any part of the header information in an email or newsgroup posting.
- 8) to export software or technical information in violation of United States export control laws.
- 9) to use the STC network in a manner that disrupts the STC network or services for other STC customers, or which threatens to or actually does damage to STC network, services or equipment.
- 10) to perform unauthorized monitoring of data or network traffic, including packet sniffing, or any attempt to probe, scan or test the vulnerability of the system or network.

Indirect or attempted violations of this AUP, and actual or attempted violations by a third party on behalf of customer or a customer's end user, shall be considered violations of the AUP. Stelle Telephone Company will investigate incidents involving such violations and may involve and cooperate with law enforcement if a criminal violation is suspected. Stelle Telephone Company will suspend or cancel your account if you fail to follow the AUP.