

Acceptable Use Policy

This Acceptable Use Policy has been formulated with the following goals in mind:

- Ensure the security, reliability and privacy of Complex Drive's network and systems, and the networks and systems of others.
- Preserve the value of the Internet as a resource for information and free expression.
- Preserve the privacy and security of Internet users.
- Discourage irresponsible practices which degrade the usability of network resources and thus the value of Internet services.
- Avoid situations that may cause Complex Drive to incur legal liability.
- Maintain the image and reputation of Complex Drive as a responsible provider.

This Acceptable Use Policy in no way supercedes or overrides Complex Drive's Terms of Service.

A. Complex Drive operates under a strict "No Spam" policy. The sending of any unsolicited e-mail advertising messages from, to, or through Complex Drive's services may result in the imposition of civil liability against the sender, in accordance with California Business & Professions Code Section 17538.45. A copy of the California Business & Professions Code may be obtained on-line from <http://www.leginfo.ca.gov>. "Unsolicited bulk" messages include, but are not limited to, commercial advertising, informational announcements, and political or religious tracts.

B. The following activities are expressly prohibited, and may result in account suspension or termination:

1. Sending unsolicited bulk e-mail (UBE) which advertises a Web site, e-mail account, or other service provided by or through Complex Drive.
2. Making Usenet postings which advertise a Web site, e-mail account, or other service provided by or through Complex Drive, to any newsgroup whose charter does not specifically allow such advertisements.
3. Sending UBE or posting advertisements to Usenet (except where specifically allowed by newsgroup charters) from a service provided by or through Complex Drive.
4. Hosting "spam-friendly" Web sites, including spam software sites.
5. Harrassment, whether through content, frequency, or size of e-mail or Usenet messages.
6. Sending e-mail to any person who does not wish to receive it. If a recipient asks to stop receiving email, the Customer must immediately and permanently cease to send that individual any further e-mail.
7. Forwarding or otherwise propagating chain letters or "e-mail hoaxes," whether or not the recipient wishes to receive them, unless such propagation is both solicited and in the clear context of debunking or discrediting chain letters/hoaxes.
8. Transmitting any electronic communication, including e-mail, using the name or address of another person or organization, for purposes of deception.

9. Impersonating another individual by altering source IP address information, or forging e-mail/Usenet headers or other identifying information.
10. Any attempt to fraudulently conceal, forge, or otherwise falsify one's identity in connection with use of the service.
11. Any use of another party's electronic mail server to relay e-mail without express permission.
12. Collecting replies to messages sent from another Internet service provider, where those messages violate this Acceptable Use Policy or any applicable policies of the other provider.
13. Denial of Service, including, but not limited to, any form of Internet packet flooding, packet corruption, or abusive attack intended to impact the proper functioning of any party's Internet servers or services.
14. Using Complex Drive's network, services, or systems to store or send content which is illegal according to the laws of United States of America, the state of California, the city of San Diego, or any International treaties respected by the United States of America, is not permitted for any reason.
Storing or sending any material deemed either illegal or inappropriate for our networks, including but not limited to child pornography, copyrighted images, software, or music, and spam-related materials including mass e-mail lists, is grounds for immediate termination of services. Note also that child pornography includes related material, such as simulated child pornography, non-nude child pornography, or sites linking to such material, whether it is determined to be legal or not. Offenses of this nature will be reported to the federal authorities and prosecuted to the fullest extent of the law.
15. Using or storing any type of software which is designed to or is likely to abuse or negatively impact Internet service, including, but not limited to, portscanners, hacking tools, ping flooding programs, security/root exploits, packet sniffers, and spam software.
16. Modifying, changing, or obscuring the MAC (Media Access Control) or IP (Internet Protocol) address(es) of servers or services. Doing so may be considered cause for service suspension or termination.
17. Intercepting or attempting to intercept, through any method, network traffic intended for other customers.
18. Running proxy servers, such as squid or BNC, unless they are available only to users whose verified contact information is known by the proxy operator and can be disclosed to Complex Drive or law enforcement authorities upon request. All usage of such services must be brought to the attention of the Complex Drive security team and cleared by the Security Manager before you begin running such services.
19. Any previous or current behavior, such as the sending of unsolicited e-mail, that results in the addition of Complex Drive to any e-mail blackhole lists, or otherwise negatively impacts the overall services of Complex Drive, is grounds for termination.
20. All e-mail lists operated by our customers, either advertising resources on our networks or being sent through our networks, must conform to the double opt-in standards. For more information regarding double opt-in lists and standards, please visit www.complexdrive.com.