

ACCEPTABLE USE POLICY

1. OBLIGATIONS

- 1.1. ConnectNet is committed to complying with legislation and ensuring all its Customers have the ability to use its Services without interference or harassment from other users. ConnectNet's Acceptable Use Policy ("AUP") is designed to help achieve these goals. ConnectNet reserves the right to change or modify the terms of this AUP at any time, by posting an updated version on its website at <http://www.connectnet.co.za>. Customer's use of ConnectNet's Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.
- 1.2. The Customer will only use the Services for purposes that are lawful and for which it was designed. The Customer will not use the Services, directly or indirectly, in a way that:
 - 1.2.1. results in the publication of threatening or offensive material which is harmful, obscene, discriminatory, defamatory, constitutes hate speech;
 - 1.2.2. is obscene, discriminatory, defamatory, illegal, indecent, hateful, malicious, racist, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others;
 - 1.2.3. constitutes hate speech, incitement to commit criminal acts, invasion of privacy, abuse, a security risk or a violation of privacy;
 - 1.2.4. interferes with use of ConnectNet's Service or systems, or any 3rd Party Service providers network;
 - 1.2.5. infringes copyright or other intellectual property rights;
 - 1.2.6. spreads viruses or other computer or communications software, code, programs or files that impede or destroy the functionality of any computer or communications software or equipment;
 - 1.2.7. interferes with any third party's use of the Services;
 - 1.2.8. transmits unsolicited bulk messages ("spam");
 - 1.2.9. unlawfully obtain information about or from third parties;
 - 1.2.10. otherwise breaches the Terms or the Agreement; or
 - 1.2.11. in ConnectNet's sole discretion constitutes abuse, a security risk or a violation of privacy.

- 1.3. Customer agrees to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas, bulletin boards, Web pages, applications, or other services.
- 1.4. The Services shall not be used:
 - 1.4.1. in connection with any criminal, civil or administrative violation of any applicable local, provincial, national or international law, treaty, court orders, ordinance, regulation or administrative rules;
 - 1.4.2. to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of ConnectNet or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation;
 - 1.4.3. to host, post, transmit, or re- transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others;
 - 1.4.4. to restrict, inhibit or interfere with the ability of any person to access, use or enjoy the Services, or create an unusually large burden on ConnectNet's or any 3rd Party Service provider's network or otherwise generating levels of traffic sufficient to impede others' ability to send or retrieve information, or use the Services in an abusive manner;
 - 1.4.5. for the purpose of commission an offence against a child or in way that would constitute or promote unlawful interaction with children;
 - 1.4.6. to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to ConnectNet at the following e-mail address: abuse@ConnectNet.co.za. ConnectNet will report any discovered violation of this prohibition to the South African Police services and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers;
 - 1.4.7. for anything other than the Customer's own personal use. Customer may not resell any Services, receive any charge or benefit for the use of any Services or provide any other feature of the Services to any third party or in any other way exploit the Service for any commercial purposes unless agreed in writing by

ConnectNet.

- 1.4.8. to interfere with, gain unauthorized access to, or otherwise violate the security of ConnectNet's Service or any 3rd Party's service or to attempt to do any of the foregoing. Such security violations shall include, but not be limited to:
 - 1.4.8.1. unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses or contact details;
 - 1.4.8.2. hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
 - 1.4.8.3. impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
 - 1.4.8.4. using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with the Services;
 - 1.4.8.5. distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
 - 1.4.8.6. knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
 - 1.4.8.7. engaging in the transmission of pirated software;
 - 1.4.8.8. using manual or automated means to avoid any use limitations placed on the Services;
 - 1.4.8.9. providing guidance, information or assistance with respect to causing damage or security breach to ConnectNet's Services;
 - 1.4.8.10. failure to take reasonable security precautions to help prevent violation(s) of this AUP.
- 1.4.9. for purposes of Spam or E-mail abuse which shall include, but are not limited to, the following activities:

- 1.4.9.1. sending multiple unsolicited electronic messages or "bombing" to one or more recipient;
- 1.4.9.2. sending unsolicited commercial electronic messages directed primarily at the advertising or promotion of products or services;
- 1.4.9.3. sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- 1.4.9.4. sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- 1.4.9.5. using distribution lists containing addresses that include those who have opted out;
- 1.4.9.6. sending electronic messages, files or other transmissions that create the potential for disruption of the Service or any of ConnectNet's 3rd Party Service Providers networks, by virtue of quantity, size or otherwise;
- 1.4.9.7. using another site's mail server to relay mail without the express permission of that site;
- 1.4.9.8. using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- 1.4.9.9. using IP addresses that the Customer does not have a right to use;
- 1.4.9.10. maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- 1.4.9.11. sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the Services or the Internet (e.g., through language, frequency, size or otherwise);
- 1.4.9.12. sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- 1.4.9.13. falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- 1.4.9.14. using redirect links in unsolicited commercial e-mail to

advertise a website or service;

1.4.9.15. intercepting, redirecting or otherwise interfering or attempting to interfere with electronic messages intended for third parties;

1.4.9.16. knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;

1.4.9.17. using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

1.5. ConnectNet reserves the right to establish policies, rules and limitations, from time to time, concerning the use of the Services. Customer must comply with any bandwidth, data storage and other limitations ConnectNet may impose, in its sole discretion. Failure to comply with these rules will result in Customer's Service being restricted, suspended or terminated, in ConnectNet's sole discretion.

1.6. Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the Services. ConnectNet has no responsibility for any material created using the Services.

1.7. Customer is responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

1.8. Customer's failure to observe the guidelines set forth in this AUP will be regarded as a material breach of the Agreement and may result in ConnectNet taking actions, which may either be a warning, a suspension or termination of Customer's Services. When reasonably possible, ConnectNet may provide Customer with a notice of an AUP violation allowing the Customer to promptly correct such violation.

1.9. Should the Customer engage in any one or more activity, which ConnectNet believes, in its reasonable discretion, violates this AUP or any of our rules or limitations, then ConnectNet shall be entitled, without prejudice to any other rights it may have, to take any responsive action ConnectNet deem appropriate, such actions may include, without limitation:

1.9.1. without notice, temporary or permanent limitation, restriction or suspension of the Customer's access to the Services concerned;

1.9.2. terminate all agreements with the Customer with immediate effect;

1.9.3. bill the Customer for any costs incurred by ConnectNet as a result of the offending activity, including (without being limited to)

bandwidth used, administration costs, downtime, usage of ConnectNet's name or registered domain names; and

- 1.9.4. disclose information relating to the offending activity as may be required under the circumstances.
- 1.10. ConnectNet has no obligation to monitor content of any materials distributed or accessed using the Services. However, ConnectNet may monitor content of any such materials as necessary to comply with applicable laws, regulations or other governmental or judicial requests; or to protect the Service and its customers.