

VAST Acceptable Use Policy

VAST ACCEPTABLE USE POLICY

1. Introduction

VAST is committed to complying with legislation and ensuring all its Customers have the ability to use its network and the Internet without interference or harassment from other users. VAST's Acceptable Use Policy ("AUP") is designed to help achieve these goals.

By using any of VAST's services, Customers agree to comply with this AUP and to remain responsible for its users, where applicable. VAST reserves the right to change or modify the terms of the AUP at any time, by posting an updated version on its website. Customer's use of VAST's services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

This AUP should be read in line with the VAST terms and conditions.

2. Scope of the AUP

The AUP applies to VAST services that provide (or include) Internet services, including but not limited to, any service providing access to the Internet or any other services provided over the Internet or wireless data networks (collectively "IP Services").

3. Prohibited Activities

You may not use the WiFi Service and/or the WiFi Network to send, receive, store, distribute, transmit, post, upload or download any materials or data which:

- promotes or encourages illegal or socially unacceptable or irresponsible behaviour;
- is in breach of any third party rights (including any third party intellectual property rights);
- has any fraudulent purpose or effect or involves a user impersonating another person or otherwise misrepresenting himself or herself as the source of any communication; or
- damages or may damage our name and/or reputation or the name and/or reputation of our sub-contractors or agents.

3.1. General Prohibitions: VAST prohibits use of the IP Services in any way that is: i) unlawful, incitement to commit criminal acts, harmful to or interferes with use of VAST's network or systems, or the network of any other provider; ii) interferes with the use or enjoyment of services received by others; iii) infringes intellectual property rights; iv) results in the publication of threatening or offensive material which is harmful, obscene, indecent, discriminatory, defamatory, constitutes hate speech; or v) constitutes abuse, harassment, a security risk or a violation of privacy.

Failure 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 that are accessed via a link from a VAST-branded website or from a website that contains VAST-branded content is a violation of this AUP.

3.2. Unlawful Activities: IP Services shall not be used 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.

3.3. Violation of Intellectual Property Rights: IP Service(s) shall not be used 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 VAST 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.

3.4. Threatening Material or Content: IP Services shall not be used 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. In addition, for those IP Services that utilize

VAST provided web or content hosting, VAST reserves the right to decline to provide such services if the content is determined by VAST to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libellous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

3.5. Inappropriate Interaction with Minors: IP Services should not be used for the purpose of commission an offence against a child or in way that would constitute or promote unlawful interaction with children.

3.6. Child Pornography: IP Services shall not be used 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 VAST at the following e-mail address:

abuse@vast.network. VAST 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.

3.7. Messages: You must not send emails or instant messages ("Messages") to anyone who does not wish to receive them. We acknowledge that email and instant messaging are informal methods of communication however you must refrain from sending Messages to another user after receiving a request to stop.

You must not send unsolicited bulk Messages or any other form of abusive electronic communication. In particular, unsolicited advertising mailings (whether commercial or informational) are strictly prohibited.

You must not operate, host, provide hosting facilities to or assist in any way any web site, email address, or any other online service which is advertised or promoted by means of unsolicited bulk Messages (whether commercial or informational), any mass messaging facility or any other form of abusive electronic communication.

You must not send, distribute, or reply to mail-bombs. Mail-bombing is either sending copies of a single message to many you, or sending large or multiple files or messages to a single user with the intention of disrupting their internet experience.

You must not use false Message headers or alter the headers of Messages to conceal their email address or to prevent internet you from responding to messages. You must not use any email address that they are not authorised to use.

You must not suggest or imply that any Message you send is from, authorised or endorsed by, VAST.

3.8. Spam/E-mail Abuse: Spam/E-mail abuse is prohibited using IP Services. Spam/E-mail abuse shall include, but are not limited to, the following activities:

- sending multiple unsolicited electronic mail messages or "mail-bombing" to one or more recipient;
- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the VAST network or of the networks with which VAST interconnects, by virtue of quantity, size or otherwise;
- using another site's mail server to relay mail without the express permission of that site;
- 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;
- using IP addresses that the Customer does not have a right to use;
- collecting the responses from unsolicited electronic messages;

- maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services or the Internet (e.g., through language, frequency, size or otherwise);
- using distribution lists containing addresses that include those who have opted out;
- 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;
- 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;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;
- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- 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.

4. Connectivity Services

- VAST reserves the right to establish policies, rules and limitations, from time to time, concerning the use of the IP Service. You must comply with any bandwidth, data storage and other limitations we may impose, in our reasonable discretion. Failure to comply with these rules will result in your service being restricted, suspended or terminated, in our reasonable discretion.
- We reserve the right to limit the number of emails that you may send in any given period or to limit the total message volume (amount of data) sent per hour.
- You may not restrict, inhibit or interfere with the ability of any person to access, use or enjoy the Internet or the any services, or create an unusually large burden on our network, including, without limitation, continuously uploading or downloading streaming video or audio; continuous FTP uploading or downloading, or otherwise generating levels of traffic sufficient to impede others' ability to send or retrieve information, or to use the services in an abusive manner in connection with any unlimited packages, options or promotions.
- We reserve the right to establish policies, rules and limitations, from time to time, concerning the use of any service. You must comply with any bandwidth, data storage and other limitations we may impose, in our reasonable discretion. Failure to comply with these rules will result in your service being restricted, suspended or terminated, in our reasonable discretion.
- We will manage bandwidth usage to the best of our ability during peak periods, however, it remains a best effort service.
- We reserve the right to manage our network in order to optimize its efficiency for the benefit of all our subscribers, including, without limitation, by way of the following: rate limiting (speed), rejection or removal of spam or otherwise unsolicited bulk e-mail, anti-virus mechanisms, protocol filtering and imposing restrictions on your use. We may take any other action we deem appropriate in order to help ensure the integrity of the network experience for all subscribers, including limiting your data traffic by controlling your network and/or bandwidth usage.

- You may not use service for unattended automated operation, unless otherwise agreed. You may stay connected as long as you are actively using that connection. You further agree not to use Internet applications for the purpose of simulating network activity to avoid session inactivity disconnection.
- We do not make any express or implied representations, warranties or guarantees regarding the availability, accuracy, reliability, timeliness, quality or security of any services.
- We are committed to provide you with uninterrupted services. However, we cannot guarantee that service and the allocated capacity will always be available.
- We can terminate the service at any time if we decide to discontinue the service offering for any reason whatsoever, without any further liability to you.

5. Security Violations

Customers are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates. Any automatic updates that affect the network performance will not be permitted. IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of VAST's (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing. System or network security violations shall include, but are not limited to:

- 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;
- 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;
- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- 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);
- 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;
- engaging in the transmission of pirated software or violating any patents, intellectual property;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to VAST's network or systems, or to the network of any other IP Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

6. Customer Responsibilities

Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. VAST has no responsibility for any material created on the VAST's network or accessible using IP Services, including content provided on third-party websites linked to the VAST network. Such third-party website links are provided as Internet navigation tools for informational purposes only, and do not

constitute in any way an endorsement by VAST of the content(s) of such sites. Customers are responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

7. World Wide Web and surfing the net

You will be solely responsible for your use of the internet and any web pages you own and/or operate that connect to the WiFi Network using the WiFi Service. You must not use World Wide Web pages within or outside the WiFi Network to violate any part of this AUP or to disrupt or attempt to disrupt another internet user's internet experience.

8. AUP Enforcement and Notice

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

If the IP Services are used in a way that we, in our reasonable discretion, believe violates this Acceptable Use Policy or any of our rules or limitations, we may take any responsive actions we deem appropriate. Such actions may include without limitation, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and/or the immediate limitation, restriction, suspension or termination of all or any portion of the services or your account. Should you engage in any one or more of the above activities, which shall be determined in VAST's reasonable discretion and which decision shall be final, then VAST shall be entitled, without prejudice to any other rights it may have, to take any responsive action we deem appropriate, such actions may include, without limitation:

- without notice, temporary or permanent limitation, restriction or suspension of your access to the IP Service concerned;
- terminate all agreements with you with immediate effect;
- bill you for any costs incurred by VAST as a result of the offending activity, including (without being limited to) bandwidth used, administration costs, downtime, usage of VAST's name or registered domain name and CPU cycles; and
- disclose information relating to the offending activity as may be required under the circumstances.

VAST has no obligation to monitor content of any materials distributed or accessed using the IP Services. However, VAST 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 VAST network and its customers.

The actions we can take:

Firstly, you should be aware that we will block any electronic communication that we reasonably consider to have breached this AUP.

Secondly, if a user has breached this AUP, or we or a third party, reasonably suspect that a user may have breached this AUP we will notify you by the contact information you have supplied (provided that this notification does not prejudice any investigation) and we may also:

- immediately suspend access to the WiFi Service until such time as we are satisfied the breach has stopped;
- immediately end this Contract;
- notify and/or pass on the details of the breach of the AUP to any relevant government, statutory, self-regulatory or law enforcement authority;
- investigate the alleged breach of the AUP, which may include gathering information from you and/or the complaining party (if any) and the examination of any other data or material on the WiFi Network or our servers; or

- remove (either temporarily or permanently), copy, store, monitor or otherwise deal with data and/or other material on the WiFi Network and/or our servers.

VAST will use your personal data and other account information in connection with any investigation carried out by VAST in accordance with this AUP, including by disclosing it to any third party authority that VAST considers has a legitimate interest in any such investigation or its outcome.

9. Incident Reporting

Any complaints (other than claims of copyright or trademark infringement) regarding violation of this AUP by a VAST Customer (or its user) should be directed to abuse@vast.network include details that would assist VAST in investigating and resolving such complaint.

You wishing to notify us of a breach of this AUP, or wishing to make a complaint regarding content, data or material that has been stored and/or accessed via the WiFi Network or the WiFi service, can email us at abuse@vast.network.

10. Fair Use Policy

The Fair Use Policy imposes bandwidth restrictions on End- Users who exhibit patterns of internet/Product usage that exceed certain thresholds for a period of time; VAST will be at liberty, at its sole discretion, to implement a cap at which an End User can be disconnected, soft-locked and/or blocked for abusing the Service at VAST's sole discretion. Amendment of the Fair Use Policy, application of same and/or leniency regarding same remains solely within the discretion of VAST. If you exceed this limit then we may immediately suspend your account or we may send you an email telling you to reduce your usage (as the case may be). If you do not act on our notification we may then suspend your account or end your Contract.

To help ensure that all customers have fair and equal use of the service and to protect the integrity of the network, VAST reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof.

VAST may, in future, implement a "heartbeat" service, which will provide a rudimentary service. This service would be implemented outside of any complimentary access that may be offered (i.e. it would apply for the remaining 23 hours and 30 minutes of a 24 hour day). VAST cannot be held responsible for the quality of this rudimentary service during this time.

Services such as peer to peer file sharing or torrent downloads will not be permitted on the VAST Network and could result in a warning, a suspension or termination of Customer's services.

11. Third Party Services

The AUP usage policy as outlined above pertains to the services which VAST offers to its customers. Any service that is offered by a third party provider will be governed by a separate AUP and will be enforced by the third party provider.