# Acceptable Usage Policy (AUP)

This Acceptable Use Policy ("AUP") specifies the actions prohibited to OnAir Fibre users of the network and systems ("infrastructure") of the Internet Service provider ("ISP") Vox Telecommunications (Pty) Ltd (from here on referred to as "the ISP") and its subsidiaries.

OnAir Fibre users are required to adhere to this policy without exception. The terms "User", "Subscriber" and "Customer" are used interchangeably.

1. **LAWS AND REGULATIONS**

1.1. The ISP's infrastructure may be used only for lawful purposes. Users may not violate any applicable laws or regulations of South Africa within the territory of South Africa. Should the user reside outside of South Africa, the laws of the country in which the user resides shall apply.

1.2. Transmission, distribution or storage of any material on or through the infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secrets or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

2. **THE NETWORK**

2.1. The user acknowledges that the ISP is unable to exercise control over the content of the information passing over the infrastructure and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, the ISP is not responsible for the content of any messages or other information transmitted over its infrastructure.

2.2. The ISP's infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.

2.3. The user may obtain and download any materials marked as available for download off the Internet but is not permitted to use its Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials.

2.4. The user is prohibited from obtaining and/or disseminating any unlawful materials, including but not limited to stolen intellectual property, child pornography, and/or any unlawful hate-speech materials.

3. **SYSTEM AND NETWORK SECURITY**

3.1. All references to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through the ISP) and includes but is not limited to the infrastructure of the ISP itself.

3.2. The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").

# Acceptable Usage Policy (AUP)

3.3. Violations of system or network security by the user are prohibited, and may result in civil or criminal liability. The ISP will investigate incidents involving such violations and will involve and will co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

3.3.1. Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of Vox.

3.3.2. Unauthorised monitoring of data or traffic on the network or systems without express authorisation of the ISP

3.3.3. Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.

3.3.4. Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

4. **FAIR ACCESS POLICY**

4.1. To help ensure that all users have fair and equal use of the service and to protect the integrity of the network, the ISP reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof, the action that the ISP may take includes, but is not limited to:

4.1.1. Limiting throughput

4.1.2. Preventing or limiting service through specific ports or communication protocols; and/or

4.1.3. Complete termination of service to users who grossly abuse the network through improper or excessive usage.

4.2. This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

4.3. Online activity will be subject to the available bandwidth, data storage and other limitations of the service provided, which the ISP may, from time to time, revise at its own discretion and without prior notice to the customer.

5. **EMAIL USE**

5.1. It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc.). This is strongly objected to by most Internet users and the repercussions against the offending party and the ISP can often result in disruption of service to other users connected to the ISP; forward or propagate chain letters nor malicious e-mail; send multiple unsolicited electronic mail messages or "mail-bombing" to one or more recipient; sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender; using redirect links in unsolicited commercial e-mail to advertise a website or service;

5.2. Maintaining of mailing lists by users of the ISP is accepted only with the permission and approval of the list members, and at the members' sole discretion. Should mailing lists contain invalid or

undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed.

5.3. Public relay occurs when a mail server is accessed by a third party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mail-server. Users' mail servers must be secure against public relay as a protection to both themselves and the Internet at large. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed. The ISP reserves the right to examine users' mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. The ISP also reserves the right to examine the mail servers of any users using the ISP mail servers for "smarthosting" (when the user relays its mail off the ISP mail server to a mail server of its own) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in strict accordance with the ISP's policy of preserving customer privacy.

6. **COMPLAINTS**

6.1. Upon receipt of a complaint, or having become aware of an incident, the OnAir reserves the right to:

6.1.1. Inform the user's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AUP.

6.1.2. In the case of individual users suspend the user's account and withdraw the user's network access privileges completely.

6.1.3. Charge the offending parties for administrative costs as well as for machine and human time lost due to the incident.

6.1.4. In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means.

6.1.5. Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies. Any one or more of the steps listed above, insofar as they are deemed necessary by the ISP in its absolute and sole discretion, may be taken by OnAir against the offending party. All cases of violation of the above Acceptable Use Policy should be reported to abuse@bestinternet.co.za