1. DEFINITIONS

1.1	"**Customer**"	means the person or legal entity entering into an agreement or entering into Terms and Conditions with MetroFibre for the provision of any Services;
1.2	"**MetroFibre**"	means Metro Fibre Networx Proprietary Limited, registration number 2007/024366/07, a company incorporated in terms of the laws of the Republic of South Africa, which is a Network Provider and Internet Services Provider;
1.3	"**MetroFibre Network**"	means the communications network used for the distribution of Services which are provided by MetroFibre as envisaged in the respective agreement entered into between MetroFibre and the Customer;
1.4	"**Service(s)**"	means any services provided by MetroFibre and which are made accessible to the Customer in terms of the respective agreement or Terms and Conditions entered into between MetroFibre and the Customer.

2. PURPOSE

2.1 This Acceptable Fair Use and Access Policy (the "**Policy**") serves to define the accepted behaviour of users on the MetroFibre Network.

2.2 The Policy is intended to allow MetroFibre to:

2.2.1 maintain the integrity and quality of its Service;

2.2.2 protect its Customers and infrastructure from abuse;

2.2.3 adhere to current laws and regulations governing organisations and service providers in the Republic of South Africa; and

2.2.4 co-exist with the global internet community as a responsible service provider.

3. GOVERNING LEGISLATION

3.1 The Customer undertakes to use MetroFibre's Network and Services in accordance with any restrictions imposed under the following legislation:

3.1.1 Electronic Communications and Transactions Act 25 of 2002;

3.1.2 Electronic Communications Act 36 of 2005;

3.1.3 Regulation of Interception and Provision of Communication-Related Information Act 70 of 2003 ("**RICA**")

4. THE NETWORK

4.1 The Customer acknowledges that MetroFibre is unable to exercise control over the data passing over the infrastructure and the Internet including, but not limited to, any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, MetroFibre is not responsible for data transmitted over its infrastructure.

4.2 The MetroFibre infrastructure may be used to link into other networks worldwide and the Customer agrees to abide by the acceptable use policies of these networks.

4.3 The Customer is prohibited from obtaining, disseminating or facilitating any unlawful materials over the MetroFibre Network including, but not limited to:

4.3.1 copying or dealing in intellectual property without authorisation;

4.3.2 child pornography or unlawful interactions with minors;

4.3.3 any threatening or offensive material which is harmful, obscene, discriminatory, defamatory, constitutes hate speech or the unlawful incitement to commit criminal acts; and

4.3.4 promotion, facilitation or funding of terrorist activities.

4.4 The Customer is prohibited from using the MetroFibre Network in any way that:

4.4.1 constitutes criminal activity or the aiding of criminal activity;

4.4.2 constitutes Spam/E-mail abuse, a security risk or a violation of privacy; and

4.4.3 interferes with the use or enjoyment of the MetroFibre Network by others.

4.5 In order to ensure that all Customers have fair and equal use of the Service and to protect the integrity of the MetroFibre Network, MetroFibre reserves the right, and will take whatever steps MetroFibre deems necessary, to prevent improper or excessive usage of the Service. These steps may include but are not limited to:

4.5.1 any action required to prevent prohibited usage (whether intended or unintended) i.e., actions to prevent the spread of viruses, worms, malicious code, etc;

4.5.2 limiting throughput;

4.5.3 preventing or limiting Services through specific network ports or communication protocols;

4.5.4 complete termination of Service to Customers who grossly abuse the MetroFibre Network through improper or excessive usage;

4.5.5 suspending the Customer's account;

4.5.6 charging the offending Customer for administrative costs incurred as well as for machine and human time lost due to the incident;

4.5.7 implementing appropriate mechanisms in order to prevent usage patterns that violate this Policy and/or any applicable laws; and/or

4.5.8 sharing information concerning the incident with other internet access providers or publish the information and/or make available the Customer's details to law enforcement agencies.

5. SYSTEM AND NETWORK SECURITY

5.1 Any reference to systems and networks under this section refer to all systems and networks to which the Customer is granted access through MetroFibre, including, but not limited to, the infrastructure of MetroFibre itself and the Internet.

5.2 The Customer may not circumvent authentication or security of any host, device, network or account (referred to as "hacking" or "cracking"), nor interfere with Service to any user, host, device or network (referred to as "denial of Service attacks"). The host, device, network or account shall also not be used for any illegal purpose, including but not limited to phishing.

5.3 Violations of system or network security by the Customer are prohibited and may result in civil and/or criminal liability. MetroFibre will investigate incidents involving any violation or suspected violation and shall involve and co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

5.3.1 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 any security or authentication measures without the express authorisation of MetroFibre;

5.3.2 unauthorised monitoring of data or traffic on the network or systems without the express authorisation of MetroFibre;

5.3.3 interference with Service to any user, device, host or network including, without limitation, email bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

5.3.4 forging of any TCP-IP packet header (spoofing) or any part of the header information;

5.3.5 knowingly uploading or distributing files that contain malware, including but not limited to 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 session or system hi-jacking;

5.3.6 engaging in the promotion or transmission of pirated software;

5.3.7 using manual or automated means to avoid any use limitations placed on the Services;

5.3.8 providing guidance, information or assistance with respect to causing damage or security breach to MetroFibre's network or systems, or to the network of any other service provider;

5.3.9 impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, social engineering, etc.); and

5.3.10 failure to take reasonable security precautions to help prevent violations of this Policy.

6. INTERCEPTION

The Customer acknowledges that MetroFibre is lawfully required to intercept communications in accordance with the provisions of RICA. Any interception of communications shall be strictly in accordance with the provisions of the said Act.

7. GENERAL

7.1 This Policy forms part of MetroFibre’s standard terms and conditions in respect of any of MetroFibre’s Services and the usage of any MetroFibre Services shall be subject to this Policy.

7.2 Any cases pertaining to violation of this Policy, must be reported to abuse@metrofibre.co.za.