IPComms Fair & Acceptable Use Policy

What is a Fair usage policy?

The following list details all the uses of IPLabs Communications (Pty) Ltd's ("IPComms") Internet services that we consider unacceptable - in other words, unfair usage. IPComms maintains and promotes a policy of fair and acceptable usage at all times, so please ensure that any use of IPComms services, by yourself, your customers (if you are a partner), or anyone in your household or office doesn't in any way contradict the restrictions listed below.

Please ensure that anyone who use your IPComms Internet service agrees with this Policy and is aware of their obligations under it.

What can IPComms' services not be used for?

1. Unlawful, fraudulent, criminal or otherwise illegal activities
2. Sending, receiving, publishing, posting, distributing, disseminating, encouraging the receipt of, uploading, downloading or using any material which is offensive, abusive, defamatory, indecent, obscene, unlawful, harassing or menacing or a breach of the copyright, trademark, intellectual property, confidence, privacy or any other rights of any person
3. Sending or uploading unsolicited emails, advertising or promotional materials, offering to sell any goods or services, or conducting or forwarding surveys, contests or chain letters except as permitted by Law.
4. Knowingly or negligently transmitting or uploading any electronic material (including, without limit, files that contain viruses, corrupted files, or any other similar software or programmes) which is known or likely to cause, interrupt, damage, destroy or limit the functionality of any computer software, hardware or telecommunications equipment owned by IPComms or any other Internet user or person
5. Activities that invade another's privacy, cause annoyance, inconvenience or needless anxiety to any person
6. Activities that are in breach of any other third party's rights, including downloading, installation or distribution of pirated software or other inappropriately licensed software, deletion of any author attributions, legal notices or proprietary designations or labels in any file that is uploaded, falsification of the origin or source of any software or other material
7. Anything that may disrupt or interfere with IPComms' network or services or cause a host or the network to crash
8. Launching "denial of service" attacks; "mailbombing" attacks; or "flooding" attacks against a host or network
9. Granting access to your IPComms services to others not residing at (for Standard or Home) or located at (for Business) the premises at which these Internet services are provided
10. Making excessive use of, or placing unusual burdens on, the network, for example by sending or receiving large volumes of email or excessively large email attachments
11. Circumventing the user authentication or security process of a host or network
12. Creating, transmitting, storing or publishing any virus, Trojan, corrupting programme or corrupted data

What about security?

You are responsible for ensuring that any confidential account information held by you remains confidential so that the network cannot be used by any unauthorised person.
The Account information referred to includes, but is not limited to, those controlling access to (a) any computer hardware systems or networks; (b) any computer software or applications; or (c) any other services accessed by you in the use of either of the above.

You shall not disclose any account information to any third party or use the same for any purpose connected with the improper use of the network including accessing or attempting to access other parts of the services for which you do not have access rights. You are responsible for taking all reasonable steps necessary to prevent a third-party obtaining access to the network. You must immediately advise us if you become aware of any violation or suspected violation of these Security provisions.

What about usage by others without you knowing?

You are responsible for all uses made of IPComms Internet services through your account (whether authorised or unauthorised) and for any breach of this Policy whether an unacceptable use occurs or is attempted, whether you knew or should have known about it, whether or not you carried out or attempted the unacceptable use alone, contributed to or acted with others or allowed any unacceptable use to occur by omission. You agree that IPComms is not responsible for any of your activities in using the network. Although the Internet is designed to appeal to a broad audience, it's your responsibility to determine whether any of the content accessed via IPComms' Internet service is appropriate for children or others in your household or office to view or use.

Anything else you should know?

IPComms does not accept the sending of Spam email through its services and reserves the right to block any emails that have the characteristics of spam. You'll be contacted by IPComms if any emails sent by you are blocked for this reason. Any spamming activity may result in suspension or termination of your service at IPComms' option and sole discretion.

What about excessive network usage?

If it is determined that any customers Internet activities are so excessive that other customers are detrimentally affected, IPComms may give the customer generating the excessive web traffic a written warning (by email or otherwise). In extreme circumstances, should the levels of activity not immediately decrease after the warning, IPComms may terminate that customer's services.

What happens if the Policy is breached?

If any customer's use of these services constitutes a breach of this Policy, IPComms may, at its option and discretion, either give the customer notice to stop the unacceptable use(s) or terminate that customer's services (with or without notice as IPComms considers appropriate).

To report any illegal or unacceptable use of IPComms services, please send an email to support@ipcomms.co.za

Appendix A – Product Specific AUPs

Syndeo, Octotel, Vumatel and Frogfoot Fibre

All of our Fibre products are unshaped, our Contention and FUP are available in the following table:

Package Name	Download	Upload	Profile	Contention	FUP
FTTH Home 4/2	4 Mbps	2 Mbps	Home	20:1	200 GB
FTTH Home 10/5 : 10/2	10 Mbps	5/2 Mbps	Home	20:1	500 GB
FTTH Home 20/5 : 20/2	20 Mbps	5/2 Mbps	Home	20:1	1000 GB
FTTH Home 100/25 : 100/10	100 Mbps	25/10 Mbps	Home	20:1	5000 GB
FTTH Home 200/25	200 Mbps	25 Mbps	Home	20:1	10000 GB
FTTH Home 1000/25	1000 Mbps	25 Mbps	Home	20:1	50000 GB
FTTH Premium 10/10	10 Mbps	10 Mbps	Premium	5:1	1500 GB
FTTH Premium 20/20	20 Mbps	20 Mbps	Premium	5:1	3000 GB
FTTH Premium 100/100	100 Mbps	100 Mbps	Premium	5:1	15000 GB
FTTH Premium 200/200	200 Mbps	200 Mbps	Premium	5:1	30000 GB
FTTH Business 5/5	5 Mbps	5 Mbps	Business	5:1	
FTTH Business 10/10	10 Mbps	10 Mbps	Business	5:1	
FTTH Business 50/50	50 Mbps	50 Mbps	Business	5:1	
FTTH Business 100/100	100 Mbps	100 Mbps	Business	5:1	
FTTH Business 200/200	200 Mbps	200 Mbps	Business	5:1	
FTTH Business 300/300	300 Mbps	300 Mbps	Business	5:1	

Further notes on our products:

Home

Our home package is intended for light home use. FUP limits are calculated on the basis of full line utilisation for an average of 4 hours / day. Speeds may be halved if FUP is exceeded. Not available at business premises.

Premium

The premium home packages is ideal for heavier users doing lots of streaming, downloads and uploads on a regular basis. FUP limits are calculated on the basis of full line utilisation 50% of the time (i.e. average 12 hours / day). Speeds may be halved if FUP is exceeded. Not available at business premises.

Business

Built for business, these packages are built with no shaping or throttling so business can experience fast, uninterrupted fibre services. No FUP limits apply.

DSL and FTTH products

Affected Networks:

- ADSL
- Openserve

Home Uncapped / Premium Uncapped

Home Uncapped services are best suited for average home users who make little to no use of high bandwidth services such as NNTP, Peer-to-Peer and Torrents (and similar but not limited to). Home Uncapped services are proactively managed by the Protocol Manager.

Premium Uncapped services are better suited to more advanced users and are managed proactively by the Protocol Manager.

Premium Uncapped - Protocol Manager

The Protocol Manager is used to provide all uncapped users on our network with the best possible internet experience. During peak network times, we give priority to real time services (such as browsing, email, streaming etc), high bandwidth services such as NNTP, Peer-to-Peer and Torrents (and similar but not limited to) will receive less priority.

Clients deemed to be continuously uploading/downloading or using the service for unattended automated processes will be managed by the Protocol Manager. The Protocol Manager may be used to manage clients by rate limiting (slowing down speed) and limiting or preventing service using specific protocols or ports. We reserve the right to use the Protocol Manager to manage the integrity of our network should network capacity not be available at any time, we assure our clients that we will do this in a responsible manner should the need arise. Any user that is found attempting to bypass or circumvent the Protocol Manager will be suspended and could have their service cancelled.

Home Uncapped – Protocol Manager

Home Uncapped services are managed according to the last 7 days usage projected to 30 days as well as the available capacity on the network at all times.
There are predefined thresholds set and when exceeded the account speed will be managed down to a maximum of 50% of the account speed. Should the demand on the network exceed available capacity these thresholds may be managed more aggressively by the Protocol Manager and differ to the table below.

The thresholds per account speed are:

Speed	Threshold
1Mbps	20GB
2Mbps	40GB
4Mbps	80GB
8Mbps	100GB
10Mbps	120GB
20Mbps	200GB
40Mbps	400GB
100Mbps	800GB

Any user that is found attempting to bypass or circumvent the Protocol Manager will be suspended and could have their service cancelled.

Business Uncapped (DSL and Fibre)

This is an uncapped service that is prioritised for Business Users based on available network capacity where high priority is required for typical business protocols. Business protocols such as VOIP, Terminal Services, Web Browsing and Email are unshaped.

Clients deemed to be continuously uploading/downloading or using the service for unattended automated processes or non-typical business protocols (such as but not limited to NNTP, Peer-to-Peer, Https Downloading and Torrents) will be managed by the Protocol Manager. The Protocol Manager may be used to manage clients by rate limiting (slowing down speed) and limiting or preventing service using specific protocols or ports. reserves the right, to at its discretion manage non typical business protocols such as but not limited to NNTP, Peer-to-Peer, Https Downloading and Torrents and/or rate limit service speed.

We reserve the right to use the Protocol Manager to manage services in order to protect the integrity of our network according to the available network capacity, we assure our clients that we will do this in a responsible manner should the need arise.
Any user that is found attempting to bypass or circumvent the Protocol Manager will be suspended and could have their service cancelled.