NGV Fair & Acceptable Use Policy

It is important to us that our customers can access our services. Because of this, you must follow our Fair & Acceptable Use Policy when you use any of our services giving you calls or data with no limit.

This Policy is intended to ensure that our customers do not use our services in an excessive, unacceptable, unreasonable or fraudulent manner, or in connection with equipment that has not been approved by us. Such usage may impact the reliable operation of our network and/or the quality or reliability of our services. Generally, legitimate use of our services for their intended purposes for which they are supplied to you will not breach this Policy.

We can rely on this Policy where we reasonably consider that you have used our services in a way that is excessive or unreasonable or in the situations set out below under "Prohibited Use" and "Commercial use".

Prohibited Use
You, and any person who accesses our service, must not use, or attempt to use, the service:

a. For illegal purposes or practices;
b. For any purpose if we advised you that such purpose was prohibited in your application or the relevant service description;
c. In any way which damages or interferes (or threatens to damage or interfere) with the operation of a service or with the efficiency of our network or a supplier's network (including as a result of attempts by you to increase the capacity of performance of your system or your equipment);
d. In any way which makes it unsafe or which may damage any property or injure or kill any person;
e. To transmit, publish or communicate any material or engage in any conduct which is defamatory, abusive, menacing or harassing;
f. To engage in abusive behaviour toward our staff;
g. To make inappropriate contact with children or minors;
h. To access, store, reproduce, distribute, publish or commercially exploit any information or material of any kind that infringes any copyright, patent, trade mark, design or other intellectual property right;
i. To send, relay or distribute any electronic data, the contents or properties of which have been manipulated for the purpose of maliciously or illegally impersonating or obscuring the original source of that data. This does not include the use of Virtual Private Networks or similar concepts in circumstances where this is legal and otherwise complies with this Policy;
j. To access, monitor, use or control any other person's equipment, systems, networks or data (including usernames and passwords) or to otherwise probe, scan or test the vulnerability of any other person's equipment, networks, systems or data, without that person's consent;
k. To access, or attempt to access, the accounts or private information of others, or to penetrate, or attempt to penetrate, our or a third party's security measures, computer software or hardware, electronic communications system or telecommunications system, whether or not the intrusion results in corruption or loss of data. This does not include conducting network security testing specifically requested by the owner of the targeted network or system;

l. To use or distribute software (such as password guessing programs, keyboard loggers, viruses or trojans) with the intent of compromising the security of the network or system;
m. To make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as 'pyramid schemes', 'Ponzi schemes', and 'chain letters';
n. To engage in any unreasonable activity which impairs the ability of other people or systems to use our services. This includes any malicious activity resulting in an adverse effect such as denial of service, attacks against another network host or individual user, flooding of a network, overloading a service, improper seizing or abuse of operator privileges, and attempts to harm a system or network. For the avoidance of doubt, this clause does not capture an activity solely because it unintentionally contributes to network congestion;
o. To access, store, reproduce, distribute or publish any content which is prohibited or unlawful under any Commonwealth, State or Territory law or classification system, or to provide unrestricted access to material that is unsuitable for minors;
p. To send, allow to be sent, or assist in the sending of spam;
q. To use or distribute any software designed to harvest email addresses; or
r. To otherwise breach the Spam Act 2003 or any regulations made under the Spam Act 2003.

Due to Payment Card Industry (PCI) requirements, you, and any person who accesses your services, must not use, or attempt to use, our web hosting services to store credit card data without our express consent in writing.

Commercial use
The services we make available are intended for residential and retail customers to use for their own personal and business usage. Customers who use our services in their capacity as carriers or carriage service providers (or as suppliers of carriers or carriage service providers) must acquire services for such purposes under wholesale terms and conditions. The following clauses are intended to ensure that this occurs.

1. You must not resell or commercially exploit any of our services. You must not re-route call traffic in order to disguise the originating party or for the purposes of resale.
2. You may not use our services in your capacity as a carrier or carriage service provider or as a party supplying services to a carrier or carriage service provider.
3. We can rely on this Policy if we reasonably think that you have breached any of the two abovementioned clauses.

Excessive use
You must not use any of our services in a way that is abnormal or excessive. For avoidance of doubt, your ordinary domestic use of a home broadband service will not breach this Policy; example, a high level of ordinary domestic use of a broadband service with no data limit will not be a breach of this Policy.

General
You must use reasonable endeavours to secure any device or network within your control against being used in breach of this Policy by third parties, including where appropriate:

a. The installation and maintenance of antivirus and firewall software;
b. The application of operating system and application software patches and updates;

c. Protecting your account information and password and taking all reasonable care to prevent unauthorised access to your service, including taking reasonable steps to secure any Wi-Fi network that you operate;
d. For residential users, requiring any persons (for example, other members of your household) that you allow to use your service from time to time to also comply with this Policy; and
e. For business and government users, maintaining and enforcing appropriate workplace and guest user policies that are consistent with the requirements of this Policy.

What we can do

If we reasonably believe that you are in breach of this Policy, we can:

a) restrict your right to use a service without telling you before we do so; and
b) suspend or cancel your services by telling you in writing 7 days before we do so.

Unless otherwise stated, our rights to restrict, suspend or cancel the supply of the service to you applies regardless of whether the breach or suspected breach was committed intentionally, or by means not authorised by you (such as through Trojan horses, viruses or other security breaches).