**FAIR USAGE POLICY**

##

**Briskona Fair Usage Policy**

Any terms in capitals not defined in this Fair Usage Policy will have the same meaning as in your Contract. This Fair Usage Policy applies to you and anybody you allow to use Briskona’s Internet Service. Any reference to “you” shall be interpreted to mean you and anybody you allow to use Briskona’s Internet service. You are responsible for the use of Briskona’s Internet services by any person you allow to use it including anyone who accesses Briskona’s Internet service because you have removed the wireless encryption security on your Wireless Router.

**How we update our Usage Policies**

The way our customers use Briskona’s Internet services is changing all the time so we may need to change our Usage Policies to adapt to our customer’s needs. Our latest Usage Policies will always be posted on our website at www.briskona.com so please keep checking for updates.

**Usage**

If you subscribe to a Product that has a cap on the amount of data that you download or upload via your Internet access each month ("Usage Cap"), your usage must not exceed that Usage Cap each month. For the current Usage Caps on each Product, please go to www.briskona.com

If you exceed your Usage Cap, we will contact you to let you know that you have done so.
If, in subsequent months, your usage continues to exceed your Usage Cap, we will continue to contact you to ask you to reduce your usage immediately. If after a reasonable period of time your usage still exceeds your Usage Cap, then we may do one or more of the following things by notice in writing (including by email): (a) charge you fair and reasonable costs for your usage (and any reasonable administration costs) in excess of your Usage Cap; (b) change your subscription to a Product with a higher Usage Cap, in which case we would also notify you of the new price you will be charged; (c) suspend your use of Internet service for the relevant month.

## **Excessive usage on Unlimited Packages during peak times**

We will monitor your Internet usage during peak times from 6pm to 10pm each day. This is when the majority of customers use the network and when speeds could be affected by the excessive usage of a minority. If we consider that your usage is excessive during peak times we may slow down your connection so that it has less effect on others. Only a very small number of customers will be affected by this (less than 2%). If you are affected, you will still be able to use the Internet to do other things normally such as browsing, email, instant messaging.

## **Illegal Activities**

You must not tamper with, reset or attempt to access Briskona network equipment.

You must not, by using the service, possess or transmit illegal material. You should be aware that as the internet is a global network, some activities/material which may be legal in the UK, may be illegal elsewhere in the world and vice versa. When you visit a website, a copy of the visited pages is stored on your pc in the web browsers' cache files. Storage of illegal material in this way may well be a criminal offence, as well as contravening this Acceptable Use Policy.

You must not, by using the service, possess or transmit material in breach of the terms of its copyright. Any of the following activities may be illegal and therefore not permitted on the Briskona’s Network:

* Copying and sharing images, movies, music television shows or other copyrighted material through the use of P2P technology.
* Purchasing copyrighted material and then making copies for others .
* Downloading anything of which you don't legally own a copy of (software, MP3s, movies, television shows, etc.)

If you are in any doubt as to the legality of anything, before proceeding take independent legal advice.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the internet. As well as being in breach of your contract for the particular service, such hacking or attempted hacking is a criminal offence.

## **Forging Addresses and Spoofing**

You must not; add, remove, or modify identifying network header information ("spoofing") or attempt to impersonate any person or piece of equipment by using forged headers or other identifying information.

You must not send data via the internet which has forged addresses or which is deliberately constructed to adversely affect remote machines.

You must not configure your pc as an open relay system.

## **Port Scanning**

You must not run "port scanning" software which accesses remote machines or networks, except with the explicit prior permission of the administrator or owner of such remote machines or networks. This includes using applications capable of scanning the ports of other internet users. If you intend to run a port scanning application, you must provide Briskona Ltd with a copy of either a contract with or the written consent authorising the activity received from the target of the scan. This must be supplied to Briskona Ltd prior to the application being run.

## **Spam or Unsolicited Email**

You must not send or allow a third party to send anonymous bulk e-mailings through either action or inaction.

If we receive any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, we may take further action to stop this happening again. This may involve the termination specific ports that are being used by the sender and may occur without notice.

In the event that we are alerted to anyone sending bulk e-mails, we will generally attempt to make contact with the senders to discuss appropriate actions but we reserve the right to suspend without notice or terminate the accounts of any clients involved in these activities.

We recommend that anybody undertaking any kind of bulk mail has a data protection statement on their Website explaining how the company fulfils their obligations in terms of the Data Protection Act.

## **Due Diligence**

You must not use Open DNS resolvers; these can be used to amplify attacks within Briskona Ltd network.

We strongly recommend against, and additional care must be taken, if running an "Open Proxy Server" as this can allow other users of the internet to exploit your internet connection, and use it as if it were their own. For example, an external user could access your local network and send unsolicited e-mails that would appear to come from you.

In severe cases, including "denial of service" (DoS) attacks originating from your network, against another network host or individual user, your service may be suspended without prior notice and if repetitions occur through actions or inactions may be terminated.

# **What action will we take**

Compliance with this Fair Usage Policy is a contractual requirement. If you fail to do so, your service may be suspended without prior notice or terminated.

# **Account Restoration**

A suspended account may be restored at Briskona’s discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by Briskona on their individual merits.