EBBE ONE

Acceptable use and Fair use policy for Broadband

Contents

Why do we need a Fair Usage Policy? 3
How will this Fair Use policy affect you? 3
What are our charging models? 3
What can you do with 10 Gigabytes of data transfer? 4
Fair Use Policy for our Fair Usage and Capped Products 4
Fair Use Policy for our Unlimited Products 4
Usage for our Unmetered Products 4
Excessive Usage of Bandwidth 4
Why do we need an Acceptable Usage Policy? 5
Customer Responsibilities when using our Broadband products 5
Use of Email with particular regards to SPAM 6
Bulk Email 7
Traffic Priority Policy 8
Administration of Traffic Priority Policy 9

Why do we need a Fair Usage Policy?

EBBE is committed to providing our customers with a very high quality and low contention service at a price that reflects true value for money.

- We do not add any additional contention to the service over that experienced on the access network
- We do operate a traffic prioritisation policy which safeguards the performance of business-critical applications 24/7
- We carefully manage our capacity and will ensure that, in line with the number of customers on the network and a usage profile that fits business customers, enough capacity is provided.

However, as with all broadband offerings our network is shared and if a group of users use a disproportionately large amount of bandwidth (i.e. transfer a large amount of data) then this will drive up the cost of supplying the service to all users. Therefore, to ensure we can provide a high quality and low contention service at a competitive price, a Fair Usage Policy applies to the use of the service.

How will this Fair Use policy affect you?

The majority of customers that will be affected by this policy are those using file sharing software such as peer-to- peer, who regularly stream media (music, TV or videos) or those who regularly download very large media files e.g. movies. Peer-to-Peer software can be left running throughout the day and can consume very large amounts of bandwidth – this is unreasonable use of the internet and is, in many cases, illegal. Customers using their broadband service for sending e-mails, browsing web-pages and other typical business applications will not be affected.

What are our charging models?

We offer a selection of usage charging models detailed below:

Product Name (WBC)	Downstream	Upstream	Usage
Business Broadband	8 Mbps	1.3 Mbps	10GB, 100GB, 150GB
Business Broadband 2+	24 Mbps	1.3 Mbps	10GB, 100GB, 150GB, unlimited
Business Broadband 2+ Premium	24 Mbps	1.3 Mbps	100GB, 150GB, Unlimited
Business M	24 Mbps	2.5 Mbps	100GB, 150GB, unlimited
Fibre 40/10	40 Mbps	10 Mbps	50GB
Fibre Broadband Business	80 Mbps	20 Mbps	200GB
Fibre Broadband Premium	80 Mbps	20 Mbps	Unlimited
Home Worker IPSC	8 Mbps	448 Kbps	10GB, 100GB
Business Broadband IPSC	8 Mbps	832 Kbps	10GB, 100GB, 150GB, unlimited
FTTC 80:20	20 Mbps	80 Mbps	Unmetered
FTTC 40:10	10 Mbps	40 Mbps	Unmetered
ADSL 2+	1.3 Mbps	24 Mbps	Unmetered
Annex M	2.5 Mbps	24 Mbps	Unmetered
IP Stream	832 Kbps	8 Mbps	Unmetered

What can you do with 10 Gigabytes of data transfer?

- Send and receive a total of 100,000 emails (without attachment)
- View over 100,000 standard web pages
- Transfer over 10,000 1MB files
- Make 80,000 minutes' worth of VOIP calls (@ G729)

Fair Use Policy for our Fair Usage and Capped Products

Each of our broadband products has a monthly bandwidth allowance which is a certain number of GB of data transfer per month within their standard monthly rental. If the allowance is exceeded, then we will automatically charge £2.50 per GB for the excess usage seen on the service.

Please note that

- The usage measurement period in this case is defined as a calendar month
- Usage is rounded up to the nearest GB

Fair Use Policy for our Unlimited Products

For these services, there is no fair use policy. Users can transfer as much data as they wish, but usage must be in accordance with this Acceptable Usage Policy (see below section).

Usage for our Unmetered Products

Our unmetered broadband policy has no usage caps or excess usage charges and is simply subject to our Acceptable Usage Policy (see below section).

Excessive Usage of Bandwidth

The use of bandwidth which is inappropriate for a particular service is to be avoided. In the event that excessive usage of bandwidth on a consistent basis is detected, we will contact you to propose a more suitable service as a replacement. If you decline to accept the suggested replacement service and the excessive usage continues, we reserve the right to restrict, suspend or terminate your access, at our discretion.

Examples of excessive bandwidth usage are:

- A circuit that sends and receives in excess of 100GB of data in any given 24 hour period
- A group of circuits (as part of the same company or end user group) that sends and receives in excess of 100GB of data at each site in any given 24 hour period.

The measures which we may take to restrict the usage of a service are detailed below in the 'Traffic Priority Policy' section.

Large bandwidth requirements across numerous sites would be better suited by a solution that does not have the potential to impact other users, such as EBBE Ethernet.

Why do we need an Acceptable Usage Policy?

This Acceptable Use Policy (AUP) is intended to help protect our customers, and the Internet community, from the inappropriate use of the Internet. This AUP sets out the rules which apply to the use of our internet connection services including your responsibilities, and permitted and prohibited uses of those services.

We remind customers that when they are connected to the internet via our service they must comply with the law. Customers must not use our service:

1. In a manner constituting improper use of a public electronic communications network which is or would be an offence under Section 127 of the Communications Act 2003; or
2. For any unauthorised access or denial of service attack which is or would be an offence under Sections 1, 2 or 3 of the Computer Misuse Act 1990; or
3. to commit an offence under the Regulation of Investigatory Powers Act 2000; or
4. to commit an offence under any other relevant UK legislation;

A customer's use of our service constitutes acceptance of this AUP.

We reserve the right to revise and update this AUP from time to time at our discretion.

Customer Responsibilities when using our Broadband products

You are responsible for your actions when connected to our network and the systems you access through your internet connection. If you act without care or irresponsibly in using your internet connection or your actions put at risk the integrity or security of our network, systems or equipment, your access may be restricted, suspended or terminated, without prior notice.

In particular, but not by way of limitation, you agree that you will not use, attempt to use or allow your internet connection to:

- store, send or distribute any content or material which is restricted, prohibited or otherwise unlawful under any applicable law or which is offensive or obscene;
- store, send or distribute confidential information, copyright material or other content which is subject to third party intellectual property rights, unless you have a lawful right to do so;
- do anything which defames, harasses, threatens, abuses, menaces, offends, violates the privacy of, or incites violence or hatred against, any person or class of persons, or which could give rise to civil or criminal proceedings;
- do any other act or thing which is illegal, fraudulent or otherwise prohibited under any applicable law or which is in breach of any code, standard or content requirement of any other competent authority;
- do anything which interferes with other users or restricts or hinders any person from accessing or using our internet connection service or systems including the excessive usage of bandwidth under the ‘Excessive Usage of Bandwidth’ section below;
- forge header information, email source address or other user information;
- access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network;
- deliberately compromise the security or integrity of any network or system including our network;
- knowingly access, download, store, send or distribute any viruses or other harmful programs or material;

- send or distribute unsolicited advertising, bulk electronic messages or otherwise breach your spam obligations set out below, or overload any network or system including our network and systems;
- invade anyone's privacy by attempting to harvest, collect, store, or publish private or personally identifiable information, such as passwords, account information, credit card numbers, addresses, or other contact information without their knowledge and consent;
- tamper with, hinder the operation of or make unauthorised modifications to any network or system; or
- authorise, aid, abet, encourage, conspire with or incite any other person to do or attempt to do any of the above acts.

In addition you may not use our network to create, transmit, distribute, or store content that:

- violates export control laws or regulations,
- impairs the privacy of communications,
- constitutes deceptive online marketing, causes technical disturbances to our network (including excessive usage of bandwidth under the 'Excessive Usage of Bandwidth' section below), its affiliated networks, or the network used by customers to access the Email services, or
- violates the policies of such networks by, including, but not limited to, the intentional introduction of any viruses, Trojan horses, worms, time bombs, cancel bots or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system or data, or
- assists, encourages or permits any persons in engaging in any of the activities described in this section.

If you become aware of any such activities, you are obligated to immediately notify us and take all other appropriate actions to cause such activities to cease.

Use of Email with particular regards to SPAM

Also known as junk mail or unsolicited commercial email, the term "spam" refers to submitting a commercial email to a large number of recipients who have not requested or opted to receive it and have no reasonable expectation of receiving email from the sender.

Email sent by a company or an organisation with whom the recipient has established a relationship or which was requested or accepted (by way of an opt-in requirement) by the recipient is not considered spam.

Spamming is not only harmful because of its negative impact on consumer attitudes toward businesses that supply Email and interconnection services, but also because it can overload our network and disrupt service to other customers.

As a user of our email service platforms sending direct marketing emails:

You must:

- include a conspicuous notice identifying the message as an advertisement or a commercial solicitation;
- provide a valid physical postal address in each email you send;
- include a valid email address or an unsubscribe link allowing the recipient to opt-out, either by replying to a valid return address, or by using an Internet-based unsubscribe mechanism
- process opt-out requests for at least 30 days after the sending of the commercial email and stop sending email to the requestor within 10 business days upon request;

- comply with any regulations in force that apply to direct marketing regulations.

You may not (in addition to the aforementioned conditions):

- send emails with a false, deceptive or misleading subject line;
- include sexually explicit content in your email;
- add an address into your list without the subscriber's permission;
- maintain an email address in your list for which an opt-out request has been received;
- use lists older than 6 months without obtaining a confirmation of the subscriber's permission;
- harvest email addresses from websites or web services;
- generate an email address by using a dictionary attack combining letters and numbers into multiple permutations;
- use scripts or automated ways to register for multiple email or user accounts to send commercial emails;
- relay emails through a computer or network without permission;
- use your subscription form to subscribe users for an unrelated list or to send content differing from the one agreed to;
- send emails with added words/characters in an attempt to bypass Bayesian filters;
- send, or attempt to send, Spam of any kind from third-party networks using a return email address that is hosted on our network, or referencing an email address hosted on our network;
- send email messages which result in complaints from the recipient or from the recipient's email provider, or which result in blacklisting of the sender's email address or mail server;
- send email messages which are excessive and/or intended to harass or annoy others;
- continue to send email to a recipient who has indicated that he/she does not wish to receive it;
- take any other actions intended to cloak your identity or contact information, including but not limited to intentionally omitting, deleting return addresses; or
- take any other action that results in the blacklisting of the sender's email address or mail server, or negatively impacts other customers who use the Email service.

In the absence of positive, verifiable proof to the contrary from you we will consider complaints by recipients of emails to be conclusive that the recipient did not subscribe or otherwise request the email(s) about which a complaint was generated.

Bulk Email

The use of our network to send bulk email whether opt-in or otherwise, and the use of bulk email to promote a site on our network is strictly forbidden. Bulk mailing is defined as:

- E-mails with more than 50 recipients per email
- Sending E-mails at a rate of over 5 emails per minute

If bulk mailing attempts are detected the relevant ports may be blocked with immediate effect.

Traffic Priority Policy

EBBE provides a high quality broadband product for the business market. We aim to secure the highest quality of service for business critical applications during core business hours. Our network identifies and will offer a priority service for business critical traffic:

Activity/Application	Peak Priority Status: Mon-Fri 08:00-18:00	Off-Peak Priority Status
Assured Services	Level 3	Level 3
Business Services: VPN Email Off-site Backup Database Surveillance Software Markets Presentation Trading Remote Access (inc. Terminal Services, SSH etc.)	Level 3	Level 3
Internet Browsing	Level 2	Level 3
Software updates	Level 2	Level 3
Audio Streaming (Excludes VoIP)	Level 1	Level 3
Video Streaming	Level 1	Level 3
Music & Video downloads, P2P etc.	Level 1	Level 3

- Level 3: Business Critical Products and Services. These services are essential for business operations and continuity and as such are time sensitive, therefore will always take preference over non time-sensitive or non-business critical services.
- Level 2: Managed Products and Services. These are services which are not as time sensitive as those in level 3 but will take priority over services which are not critical for the operation or continuity of core business.
- Level 1: Non-business critical traffic. These services are not classed as business critical or time sensitive.

By identifying the different types of traffic in our network, we can ensure that both business critical and time sensitive products and services take priority over other traffic. This is done so that we can provide our customers with a premium class of business connectivity during core business hours.

Our traffic priority service will be in use during core business hours – Monday to Friday 08:00 to 18:00. Outside of these times there will be no restrictions.

Administration of Traffic Priority Policy

You understand that the administration of this policy requires the exercise of discretion and judgment. We agree to exercise good faith in the administration of this policy and in making determinations under the policy.