

ACCEPTABLE AND FAIR USE POLICY

Borderlink Acceptable Use Policy

Introduction

This policy applies to how you use the Services provided by us, Borderlink Broadband Limited (a company incorporated and registered in Scotland (SC582522) and whose registered office is Blackadder West Farm, Blackadder, Duns, Scotland, TD11 3LX) ("we", "our" "us").

It is designed to make sure that all of our customers enjoy great service and that access is fair for everyone. The other important purpose of this policy is to ensure that our customers use our broadband and telephone services (and / or any other services you have purchased from us) (together the "**Services**") in a way that complies with the law and does not harm others or the rights of others. The defined terms in the General Terms and Conditions [[available here](#)] also apply in this policy unless we expressly state otherwise.

If you are the account holder you are responsible for the use our Services by you and any other person using your account to access our Services or network.

BY USING OUR SERVICES YOU ACCEPT THESE TERMS

1 Broadband Fair Use

- 1.1 We do not actively filter or restrict the volume of data or adjust the connection speeds that our customers receive. However, if our network monitoring systems identify an unusual or excessive use of our broadband Services, our technicians will investigate and they may take action.
- 1.2 **Unless expressly stated in any Service Level Agreement for a particular Service, we regard excessive data consumption as being more than three times the average for similar connections in that area.**
- 1.3 We look for activity that can cause problems for other customers. Some examples include:
 - 1.3.1 if a customer is continually sending and receiving large amounts of data, this could be at the expense of good service to other customers in that area. It could also indicate some kind of malicious activity, such as a customer with malware or a customer who is suffering a denial of service attack;
 - 1.3.2 if a customer is "peer-to-peer file-sharing" or undertaking similar excessive bandwidth consuming activities; or

- 1.3.3 if a residential customer is using the Services for commercial use (not including 'working from home').
- 1.4 In the event we identify any excessive activities or unacceptable use of our Services, our technicians may apply temporary restrictions to your Services whilst investigating the cause and they may contact you if it appears that you are consuming excessive data or may have infected equipment in your property. These restrictions may include:
- 1.4.1 applying restrictions to the bandwidth that can be consumed by you;
 - 1.4.2 capping your bandwidth (Mb/s) or applying a total volume per month cap;
 - 1.4.3 a de-prioritisation of internet traffic; or
 - 1.4.4 such other restrictions we consider appropriate in the circumstances.
- 1.5 We may contact you if we suspect there may be a problem with equipment at your property, or your usage appears to be substantially higher than similar connections in the area:

Equipment

- 1.5.1 We will help you to check the equipment and provide advice about security. We have seen examples where customers have installed harmful software on one or more device in their home without realising, or even online gamers who have annoyed other players online and then been targeted by other players with denial of service attacks. Such situations can be disruptive to the customer and can be a security threat, so we give the best advice we can to help and will sometimes limit internet access whilst this can be resolved.

Excessive Data Consumption

- 1.5.2 In the case where data consumption is excessive, we will contact the customer to discuss the nature of this and to ensure that the services they are using are set up correctly and they are on the right type of subscription. For example, a customer may have a family member who is actively file sharing using peer to peer technology, which could be distributing copyright materials. Such activity could attract the attention of the copyright owner and we will advise the customer accordingly. Another example may be where a customer has a camera security system at their property and is streaming HD camera feeds to the web. In some cases, the consumption of traffic can be significantly reduced by altering some basic settings and we will offer advice in this area. In any case, we work to help make your connection work better for you and our other customers and we will work with you to resolve any issues. **However, as a very last resort, we reserve the right to suspend or disconnect your access to our Services if it appears that it may be causing harm to you, nearby customers or our Services or network.**

2 Telephone Fair Use

We operate a fair use policy for certain bundled call packages. If you have a bundled call package, this will be clearly stated on your order and all invoices. The telephone fair use policy means that you can receive as many calls as you wish. However, it caps the total number of free outbound calls allowed within any one billing month. **The total number of free outbound calling minutes to UK fixed line numbers beginning with 01, 02, 03 and standard UK mobile numbers is 3,000. Any outbound calls in excess of this will be charged in accordance with our regular calling tariff.**

Further Information If you would like more information, please contact us via our website.

3 Use of the Services

3.1 You may not use our Services:

- 3.1.1 in any way that breaches any applicable local, national or international law or regulation;
- 3.1.2 in any way that we reasonably consider negatively affects our network or the Services or our ability to provide the Services to other customers;
- 3.1.3 in any way that we reasonably consider damages or could damage our reputation;
- 3.1.4 in any way that we reasonably consider to be fraudulent;
- 3.1.5 to infringe the rights of others; or
- 3.1.6 to knowingly transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

4 Communications

4.1 You may not use our Services:

- 4.1.1 to transmit, or procure the sending of, any unsolicited or unauthorised advertising or promotional material or any other form of similar solicitation (spam);
- 4.1.2 to impersonate or otherwise misrepresent another person, or assist others to do the same;
- 4.1.3 to communicate in a way that gives the impression that your communication originates from us; or
- 4.1.4 to send, knowingly receive, upload, download, use or re-use any material which:
 - 4.1.4.1 breaches any applicable local, national or international law or regulation;

- 4.1.4.2 is defamatory;
- 4.1.4.3 is obscene, immoral, offensive, indecent, abusive, menacing, harassing, threatening, hateful or inflammatory;
- 4.1.4.4 is discriminatory based on race, sex, religion, nationality, disability, sexual orientation or age or promotes any such discrimination;
- 4.1.4.5 infringes the intellectual property rights of any person;
- 4.1.4.6 invades another's privacy;
- 4.1.4.7 impersonates any person or misrepresents your identity or affiliation with any person; or
- 4.1.4.8 advocates, promotes, incites any party to commit, or assists any unlawful or criminal activity or act. .

5 Security

- 5.1 You may not use our Services to access or attempt to access any network or computer system you do not have authority to access.
- 5.2 You must not do anything that adversely affects our network or systems or use our Services to do anything that adversely affects the network or computer system of any third party.

6 Your Obligations

- 6.1 You use our Services at your own risk.
- 6.2 You are responsible for the information, materials, content you access and transmit online. You must take appropriate steps to ensure that your computer system, network and equipment are secure.

Business Customer

- 6.3 If you are a business customer, you must implement appropriate technical and security measures to protect and secure your computer system, network and equipment are secure. If you fail to do this, we will not be responsible if your computer system, network and equipment are subject to unauthorised access or are attacked by viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

Consumer Customer

- 6.4 If you are a residential consumer customer, you must take any security measures to protect your computer system, network and equipment that a reasonable and diligent person using the Services would take.

7 Failure to comply with this policy

- 7.1 If we know you have or reasonably suspect that you have failed to comply with this policy, we reserve the right to take any action that we consider appropriate. This may include:

- 7.1.1 undertaking an investigation into the breach or suspected breach;
- 7.1.2 issuing you with a formal warning;
- 7.1.3 restricting your access to our Services;
- 7.1.4 **exercising our right to suspend and / or terminate our contract with you, which we can do under the General Terms and Conditions; and/or**
- 7.1.5 reporting matters to the police and otherwise providing information to law enforcement.

8 Contact us

If you have any questions concerning this policy, please email help@gofibre.co.uk or call us on 08000 590 980

9 Changes to this policy

We may amend this policy from time to time. You should regularly check these terms to ensure you understand the terms that apply. These terms were most recently updated on 29 July 2022.