Vodafone Business Broadband and Phone Acceptable Use Policy ("AUP")

1. Introduction

1.1. This AUP applies to your use of the Equipment and Services which are provided by Vodafone to you under our Agreement with you.

1.2. Any reference to "we" in this AUP shall be a reference to Vodafone Limited or any other member of the Vodafone Group. Any reference to "you" shall mean you as the Customer and anyone else that you allow to use the Services including all employees or anyone who accesses the Services due to your removal of, or failure to maintain, wireless encryption security on your wireless router.

1.3. All capitalised words which are used in this AUP but are not defined shall have the meaning given to them in the Glossary which is set out in the Service Guide.

1.4 We may update or amend this AUP at any time, so please check our Website regularly at www.vodafone.co.uk/businessbroadband for any updates to this AUP or our Vodafone Business Broadband and Phone Agreement. Your continued use of the Services after any change to the AUP constitutes acceptance of the updated AUP.

1.5 This AUP was last updated January 2018.

2. Your use of the Services

2.1. You must not: (a) use any Equipment or Services in any way that is unlawful or illegal; (b) do anything that causes the Network to be impaired; (c) use automated means to make calls, texts or send data (including via a GSM Gateway); or (d) use the Services to artificially generate revenue or traffic.

2.2. You understand that unauthorised access to computer systems may constitute a criminal offence.

2.3. As the account holder, you shall at all times remain fully responsible for any use of the Services and Equipment by you, any employees or anyone else at your Premises.

2.4. You must refrain from any use of the Services and Equipment that could be to the detriment of any other End Users.

2.5. You are solely responsible for your use of the internet and any web space that you own or control.

2.6. You must not use the Equipment or Services to access, download, send, receive, store, distribute, transmit, upload or in any way deal with material or data that we deem:

i. to be offensive, threatening, defamatory, racist, abusive, harassing, nuisance, invasive of privacy, obscene, harmful, indecent or menacing;

ii. breaches any third party's rights (for example, using or copying another's material without their consent); or

iii. to be for fraudulent, unlawful or illegal purposes or effect.

2.7. You must not use the internet to send information that has forged addresses or are deliberately constructed to adversely affect remote machines or other computer systems.

2.8. You must not forge or alter headers, addresses or other information in emails or other messages in order to make them appear to be coming from or sent by another person or entity.

2.9. You must not alter message headers to prevent visibility of the email address or to prevent the recipient from responding to the message.

2.10. Without the explicit permission of the relevant operators you may not run "scanning" software which accesses remote machines, networks or other computer systems.

2.11. You must ensure that you do not further or allow the sending of unsolicited bulk emails, spam emails, "mailbombs", messages, or any other form of email or Usenet "abuse". This applies to both material that originates on your computer systems and also third party material passing through your computer systems.

2.12. You must ensure that your computer systems and network are not configured in such a way that others are able to exploit them in order to disrupt the internet or any other third party network. This includes but is not limited to ensuring that your network cannot be exploited as an open mail relay, open proxy server, or as a component of a wider network used in denial, or distributed denial of service attacks by third parties.

2.13. We may in certain circumstances be legally obliged to disclose information to relevant authorities, regulators, law enforcement agencies and other third parties. In any event, we reserve the right to notify these entities of any acts that may constitute unlawful conduct.

2.14. We reserve the right to restrict access to any illegal content. However, we do not monitor all content available through the Services and, as such, we cannot guarantee that you will be unable to access illegal or offensive content on the internet. We therefore recommend that you install appropriate security measures on your computer systems, including access controls and up-to-date virus protection and firewalls.

2.15. You must not use Vodafone Business Phone minutes for making or receiving calls for the purpose of financial gain (save for calls made for ordinary business purposes); including but not limited to the generation of any form of credit for use with 3rd party services.

2.16. You are not permitted to spend more than £240 per month and £40 for any single transaction, when using the Services to call numbers beginning with the following prefixes; 118, 0871, 0872, 0873

Third party providers and traffic monitoring

2.16. Please note that the third party service providers which we use to provide the Services may carry out regular traffic monitoring activities across the network. Please be aware that they may reserve the right to throttle or limit your access to the Services in order to ensure that the network and data exchanges are protected.

3. Network security

3.1. You must not take any action that could inhibit or violate the network security of any person or company (including Vodafone) or that could adversely affect their use of the internet.

3.2. You must not adapt, modify, decompile or reverse engineer any part of the Services or Equipment.

4. Actions we may take

4.1. We may, at our sole discretion, run manual or automatic systems and monitoring of your use of the Services in order to ensure that you remain compliant with the terms of this AUP at all times (for example we may scan for open mail relays, or open proxy

servers). By accessing the internet via our Services you are deemed to have granted us permission to access and monitor your computer systems and networks.

4.2. We may block any electronic communication that we reasonably consider to have breached this AUP.

4.3. If we become aware that you may have breached this AUP, we reserve the right to take any action we believe to be appropriate including, but not limited to:

i. investigating the possible breach;
ii. notifying you by email;
iii. contacting you by email or phone to gather further information or to discuss our concerns;
iv. issuing you with a formal warning;
v. restricting your access to the Services;
vi. suspending your access to the Services with immediate effect; and/or
vii. terminating your account with us and disabling your access to the Services (with or without notice).

4.4. We may take any of the above actions that we deem appropriate, but we will always try and work with you before taking any action that will affect your use of the Services.

5. Making a complaint

If you'd like to make a complaint about someone's use of the Services or in relation to any content accessible through the Services, please contact us free on 08080 034 515 from any landline or mobile or 191 from a Vodafone mobile.