Terms and Conditions of using Pinewoods Wi-Fi

By using our internet service, you hereby expressly acknowledge and agree that there are significant security, privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology. Security issues include, without limitation, interception of transmissions, loss of data, and the introduction of viruses and other programs that can corrupt or damage your computer. Accordingly, you agree that the owner and/or the provider of this network is NOT liable for any interception or transmissions, computer worms or viruses, loss of data, file corruption, hacking or damage to your computer or other devices that result from the transmission or download of information and materials through the internet service provided.

Use of the wireless network is subject to general restrictions outlined below. If abnormal, illegal, or unauthorized behaviour is detected, including heavy consumption of bandwidth, the network provider reserves the right to permanently disconnect the offending device from the wireless network.

Examples of Illegal Uses:

The following are representative examples only and do not comprise a comprehensive list of illegal uses:

1. Spamming and invasion of privacy – sending unsolicited bulk/or commercial messages over the internet using the service or using the service for activities that invade another's privacy.
2. Intellectual property right violations – engaging in any activity that infringes or misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, service marks, trade secrets, or any other proprietary right of any third party.
3. Accessing illegally or without authorization computers, accounts, equipment or networks belonging to another party, or attempting to penetrate/circumvent security measures of another system. This includes any activity that may be used as a precursor to attempted system penetration, including, but not limited to, port scans, or other information gathering activity.
4. The transfer of technology, software, or other materials in violation of applicable export laws and regulations.
5. Export Control Violations
6. Using the service in violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available ponzi schemes, pyramid

schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items or services.

7. Uttering threats;
8. Distribution of pornographic materials to minors;
9. And child pornography.

Examples of Unacceptable Uses:

The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

1. High bandwidth operations, such as large file transfers and media sharing with peer to peer programs (i.e. torrents).
2. Obscene or indecent speech or materials.
3. Defamatory or abusive language.
4. Using the service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.
5. Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.
6. Facilitating a violation of these Terms of Use.
7. Hacking.
8. Distribution of internet viruses, Trojan horses, or other destructive activities.
9. Distributing information regarding the creation of and sending internet viruses, worms, Trojan horses, pinging, flooding, mailbombing, or denial or service attacks. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the node or any connected network, system, service, or equipment.
10. Advertising, transmitting, or otherwise making available any software product, product, or service that is desired to violate these Terms of Use, which include the facilitation of the means to spam, initiation of pinging, flooding, mailbombing, denial of service attacks, and piracy of software.
11. The sale, transfer, or rental of the service to the customers, clients or other third parties, either directly or as part of a service or product created for resale.
12. Seeking information on passwords or data belonging to another user.
13. Making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to other.
14. Intercepting or examining the content of messages, files or communications in transmit on a data network.

Using WiFi boosters:

1. Externally provided WiFi boosters should not be used on Pinewoods, unless permission is granted from Rural Broadband and Pinewoods.
2. Users should not enter the configuration page of the WiFi booster, unless permission is provided, or the user is being instructed to do so by Rural Broadband.
3. WiFi boosters should not be removed from site and used for private use.
4. General WiFi terms of use still apply when using a WiFi booster.

Any questions relating to the above, please contact Rural Broadband – 01485 572253