

Acceptable Use Policy

Mojo Broadband is committed to providing a Service that supports the open use of the Internet for any lawful purpose without interference, harassment, or threat. The purpose of the AUP is to set forth guidelines and enforcement for appropriate use.

1.0 Prohibited Activities

1.1 Unlawful Activities. The Service shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national, or international law, treaty, court order, ordinance, regulation, or administrative rule.

1.2 Copyright Infringement. Pursuant to the Digital Millennium Copyright Act (the "DMCA") the Customer is prohibited from infringing on any content that is protected by intellectual property rights, trademark laws, or other proprietary rights.

1.3 Threatening Material or Content. The Service shall not be used to host, post, transmit, or re-transmit any content or material that harasses, or threatens the health or safety of others.

1.4 Inappropriate Interaction with Minors. Company complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the National Center for Missing and Exploited Children.

1.5 Child Pornography. The Service shall not be used to publish, upload, download, post, use, copy, or otherwise produce, transmit, distribute, or store child pornography. Company will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children.

1.6 Spam and Email Abuse. The Service shall not be used in violation of the CAN-SPAM Act of 2003, or any other applicable law regulating email services.

1.7 Usenet Abuse. The Service shall not be used to violate any published charters, guidelines, or community standards when posting to newsgroups.

1.8 Network Abuse. The Service shall not be used for any activity that makes or attempts to make computing or network resources unavailable by means of Denial-of-Service (DoS) attacks or Distributed Denial-of-Service (DDoS) attacks.

1.9 Security Violations. The Service may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of any device, server, network, software, data, or other system, or to attempt to do any of the foregoing.

2.0 Enforcement Action; Content Monitoring

2.1 Action with Notice. Customer's failure to observe the guidelines set forth in this AUP may result in Company taking actions anywhere from a warning to a suspension or termination of Customer's Service. When feasible, Company may provide Customer with a notice of an AUP violation via e-mail allowing the Customer to correct such violation. Customer is responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

2.2 Action without Notice. Company reserves the right to act immediately and without notice to suspend or terminate the Service in response to a court order or government notice that certain conduct must be stopped, or when Company reasonably determines that the conduct may: (1) expose Company to sanctions, prosecution, civil action, or any other liability; (2) cause harm to or interfere with the integrity or normal operations of Company's network or networks with which Company is interconnected; (3) interfere with another Customer's use of the Service; (4) violate any applicable law, rule, or regulation; or (5) otherwise present an imminent risk of harm to Company or its Customers.

2.3 Content Monitoring. Company has no obligation to monitor content of any materials distributed or accessed using the Service. However, Company may monitor content of any such materials as necessary to comply with laws, regulations, or other governmental or judicial requests, or to protect Company's network and its customers.

3.0 Incident Reporting

Any complaints regarding violation of this AUP by a Customer of Company should be directed to netabuse@mojobroadband.co. Where possible, include details that would assist Company in investigating and resolving such complaint (e.g. expanded headers, IP address(s), a copy of the offending transmission, and any log files).