

Acceptable Use Policy

poa! (the "**Service**") is a wireless internet connectivity service provided by Poa Internet Kenya Limited. ("**Poa**") which provides you with Internet connectivity for smartphones, tablets, and laptops and other WiFi enabled devices to the Poa Wi-Fi network ("**Poa Wi-Fi Network**" or "**Network**"). Each user of the Service or Network (each a "**Customer**") is responsible for complying with Poa's acceptable use policy, the ("**Acceptable Use Policy**") when using the Service.

The Acceptable Use Policy may be updated from time to time. Customers are bound to subsequent updates of the Acceptable Use Policy and should periodically familiarise themselves with its contents. The latest version of this Acceptable Use Policy can be found on the Web Site.

CUSTOMER AGREES TO BE BOUND THIS ACCEPTABLE USE POLICY. THIS ACCEPTABLE USE POLICY IS EXPRESSLY INCORPORATED INTO AND MADE A PART OF THE AGREEMENT BETWEEN POA AND CUSTOMER REGARDING USE OF THE SERVICE (THE "**AGREEMENT**").

WITHOUT LIMITING ANY OF ITS RIGHTS OR REMEDIES UNDER THE AGREEMENT OR THIS ACCEPTABLE USE POLICY, POA RESERVES THE RIGHT TO SUSPEND OR TERMINATE CUSTOMER'S USE OF THE SERVICES OR NETWORK IN THE EVENT CUSTOMER DO NOT COMPLY WITH THIS ACCEPTABLE USE POLICY.

Use of the Poa WiFi Network and Service

- i. Customer acknowledges that Poa is unable to exercise control over the data passing over the Network and via the Service and the Internet, including but not limited to any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Poa is not responsible for content transmitted over its infrastructure.
- ii. The Network and associated infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.
- iii. This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.
- iv. The use of the Service and Network will be subject to the available bandwidth, data storage and other limitations of the Service and Network.

Laws and Legislation

- i. Customer may only use the Network and Service for lawful purposes. Customer must not violate any applicable laws or regulations of Kenya.
- ii. Transmission, distribution or storage of any material on or through the Network infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
- iii. Customer will use the Network and Service in accordance with any restrictions imposed under the Kenya Information and Communication Act and any other legislation in Kenya.

- iv. Violations of this Acceptable Use Policy by the Customer are prohibited, and may result in civil or criminal liability. The Poa will investigate incidents involving such violations and will involve and co-operate with law enforcement officials if a criminal violation is suspected.

Managing Abuse & Legal Rights

- i. To help ensure that all of Poa's clients have fair and equal use of the Service and Network and to protect the integrity of the Network, Poa reserves the right to:
 - a. Investigate suspected violations of this Acceptable Use Policy
 - b. Take action to recover costs and expenses incurred in identifying and resolving a breach of this Acceptable Use Policy, including charging Customer for administrative costs as well as for machine and human time lost due investigating and remedying any breach.
 - c. Suspend the Customer's account and withdraw the Customer's use of the Network and Service for any Customer.
 - d. Take such action as may be necessary to protect the integrity of the Service and Network including, but not being limited to, system monitoring, as well as protocol management and shutting down of ports affected by viruses, worms or other malicious code.
 - e. Implement appropriate technical mechanisms in order to prevent usage patterns that violate this Acceptable Use Policy.
 - f. Share information concerning any breach with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies.
- ii. Any one or more of the steps listed above, insofar as they are deemed necessary by Poa in its absolute and sole discretion, may be taken against any Customer or Customers it deems as having breached this Acceptable Use Policy.
- iii. In addition, the Poa reserves all available rights and remedies with respect to such activities at law or in equity.

CUSTOMERS RESPONSIBILITIES

At all times Customer will follow the following rules when using the Service or Network:

- i. Maintain the confidentiality of their passwords and account information.
- ii. Not attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal functioning, operation, or security of any network, system, computing facility, equipment, data, or information compromising all or part of the Service or Network.
- iii. Not distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials.
- iv. Not attempt to gain unauthorized access to, or use, data, systems or networks, including any attempt to probe, scan or test the vulnerability of the Service or Network
- v. Not attempt to gain unauthorized access to, or use, data, systems or networks, including any attempt to probe, scan or test the vulnerability of any third party network or system connected to the Service or Network

- vi. Not breach or attempt to breach the security or authentication measures of the Service or Network. This includes, but is not limited to, accessing data not intended for Customers, logging into or making use of the Service or Network.
- vii. Not engage in any act of a malicious nature which may reasonably result in harm or damage to another Customer's service, equipment, or privacy. This includes Syn-flood attacks, or any attempt to overburden a recipient's computer system by sending a high volume of spurious data with the intent to impede functionality, or totally disable recipient system(s), and any other methods of denial of service. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.
- viii. Not interfere with, the Service or the Network with the intent to render said system dysfunctional including, without limitation, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks. This includes "denial of service" (DOS) attacks against another network host or individual user.
- ix. Not operate Maillist, Listserv, 'auto-responders', 'cancel-bots' or similar automated or manual routines which generate excessive amounts of net traffic, or disrupt net newsgroups or email use by others.
- x. Not attempt to intercept, redirect, or otherwise interfere with communications intended for other Customers.
- xi. Not use the Service or Network to transmit excessive volumes of unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient.
- xii. Not use the Service to send unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e.g., E-mail "Spam"); or distribute, advertise or promote software or services that have the primary purpose of encouraging or facilitating unsolicited commercial E-mail (e.g., email "Spam").
- xiii. Not use the Service for anything other than periodic, active use of email, newsgroups, file transfers, Internet chat, messaging, browsing of the Internet, and other legitimate personal and business use. Customer may stay connected so long as they are actively using their connection for these stated purposes. Further, Customer may not use the Service on a standby or inactive basis in order to maintain a connection including using any mechanism to defeat any idle timer or system tool intended to enforce the part-time and personal nature of User's connection, including the use of pingbots and other methods of avoiding timing disconnection. Poa reserves the right to terminate a Customer's connection following any extended period of inactivity.
- xiv. Not operate bit torrent or other peer to peer content sharing services.
- xv. Install and maintain anti-virus software, anti-malware, anti-trojan software on devices accessing the Network or Service.
- xvi. Not use an email server to relay mail without the express permission the server's owner.
- xvii. Not attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than the Customer for purposes of deception.
- xviii. Will only maintain mailing lists only with the permission and approval of the list members, and at the members' sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed.
- xix. Not forward nor propagate chain letters nor malicious e-mail.
- xx. Not operate a public email relay.

- xxi. Not alter, add, remove or modify a source IP address information or by using forged headers (a.k.a. "spoofing") in an effort to deceive or mislead.
- xxii. Not attempt to fraudulently conceal, forge, or otherwise falsify a Customer's identity in connection with use of the Service.
- xxiii. Comply with the following rules regarding usenet use:
 - a. Before using usenet, familiarise themselves with the contents of the following newsgroups: news users' questions, news announcers, news users' answers.
 - b. Not perform excessive cross-posting (i.e., posting the same article to a large numbers of newsgroups).
 - c. Post irrelevant (off-topic) material to newsgroups (also known as USENET spam).
 - d. Post binaries to a non-binary newsgroup.
 - e. The Poa reserves the right to delete and/or cancel posts which violates the above conditions.
- xxiv. Not use the Service or Network to transmit, distribute, retrieve, or store any information, data, or other material in violation of any applicable law or regulation (including, where applicable any tariff or treaty). This includes, without limitation, the use or transmission of any data or material protected by copyright, trademark, trade secret, patent, or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory, or otherwise unlawful.
- xxv. Not monitor the data or traffic of the Network or Service without express authorisation of the Poa.
- xxvi. Not interference with the provision of the Service or Network to another Customer, device, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- xxvii. Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.
- xxviii. Not use the Service or Network to knowingly commit verbal or written threats towards another person. This may include posting or transmitting a person's real life information (name/address/phone number) in a malicious manner.
- xxix. Not use the Service or Network to send threatening or harassing messages which suggest that the sender is planning to engage in some type of criminal activity including but not limited to threats to public officials, references to bombings, bank heists, and activities that threaten national security.
- xxx. Not use the Service or Network to intentionally transmit files containing a computer virus or corrupted data, or post or transmit any information or software which contains a virus, cancelbot, trojan horse, worm or other harmful component.
- xxxi. Not use any malicious software (virus, spider, trojan horse) that will distort, delete, damage, emulate, or disassemble the Service, Network or any other Poa products or services.
- xxxii. Not use the Service or Network for the purposes of phishing, or impersonating or misrepresenting affiliation with another person or entity, causing or intending to cause embarrassment or distress to, or to threaten to invade the privacy, or collecting or harvesting any personally identifiable information, including account names.
- xxxiii. Not use the Network or Service for

- f. copying or dealing in intellectual property without authorization,
- g. child pornography, and/or
- h. Any unlawful hate-speech materials.

xxxiv. Report any actual suspected or actual breaches of this Acceptable Use Policy to Poa at security@poainternet.net