Acceptable Use Policy

Updated: 1 February 2018

Pennytel reserves the right to change this Acceptable Use Policy at any time and notify you by posting an updated version of the Policy on our website.

The amended Policy will apply between us whether or not we have given you specific notice of any change. We encourage you to review this Policy periodically because it may change from time to time. This Policy applies to all End Users who use the mobile network supplied by Pennytel.

PENNYTEL AUSTRALIA PTY LTD
4/580 George Street Sydney NSW 2000
ABN: 12 166 566 632

1. Use only for lawful purposes

The network, including the network of any service provider from whom Pennytel acquires a service for the purpose of resale, and including the web sites operated by Pennytel may be used only for lawful purposes.

Users may not use the network in order to transmit, distribute or store material:

a) in violation of any applicable law;
b) in a manner that will infringe the copyright, trade mark, trade secret or other intellectual property rights of others or the privacy, publicity or other personal rights of others;
c) that is obscene, threatening, abusive or hateful; or
d) that contains a virus, worm, Trojan, or other harmful software or component.

2. No spam

Users are prohibited from using the network to accept, transmit or distribute unsolicited bulk data, commonly known as spam (which includes, without limitation, email, SMS messages, MMS messages, bulletin boards, messages to communities or groups or web sites, software and files).

The only circumstances in which the network may be used to send bulk data of an advertising or promotional nature is in accordance with any applicable laws relating to spam and the sending of bulk data and where the bulk data is sent to persons with whom the sender has a pre-existing business, professional or personal relationship or to persons who have previously indicated their consent to receive such data from the sender from time to time (for example by giving their consent by filling in information to that effect on the sender's web site).

The sender must also provide an unsubscribe function on their web site (and make this function known to recipients in the relevant data as sent) which allows those recipients to elect not to receive further bulk data. Unless these requirements are met, Users must not send bulk data on the network.

3. Other prohibited uses

The following activities are also prohibited uses of the network:

a) Sending data, or causing data to be sent, to or through the network that hides or obscures the source of the data, that contains invalid or forged headers or domain names or deceptive addressing;

b) Receiving or collecting responses from unsolicited bulk data (spam), whether the original was sent via the network or not, or hosting a web site to which recipients of unsolicited bulk data are directed;

c) Relaying data from a third party's mail server without permission or which employs similar techniques to hide or obscure the source of the data;

d) Collecting or harvesting screen names or email addresses of others for the purpose of sending unsolicited emails or for exchange;

e) Sending large or numerous amounts of data for the purpose of disrupting another's computer or account;

f) Sending data that may damage or affect the performance of the recipient's equipment;

g) Persistently sending data without reasonable cause or for the purpose of causing annoyance, inconvenience or needless anxiety to any person;

h) Sending mass messages (including for the purpose of advertising), other than within communities, groups or web sites that specifically encourage or permit advertising; and

i) Sending binary files (rather than text files), other than within communities, groups or web sites that specifically encourage or permit this.

j) not promote or market or otherwise encourage the use of the Mobile Services for M2M Use or to facilitate voice calls over the IP protocol (VOIP) or for sending or receiving SMS over an IP network

4. System and network security

Users are prohibited from violating or attempting to violate the security of the network, including, without limitation:

a) accessing material not intended to be accessed by the User or logging into a server or account which the User is not authorised to access;

b) attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorisation;

c) attempting to interfere with, disrupt or disable services to any other User, host or network, including, without limitation, via means of overloading, flooding, mail bombing or crashing;
d) forging any TCP/IP packet header or any part of the header information in any email or any community, group or web site posting; and
e) taking any action in order to obtain services to which such User is not entitled. Violations of system or network security may result in civil or criminal liability for the User. Pennytel and/or our Network Operator will investigate occurrences which may involve such violations and may involve, and cooperate with, law enforcement authorities in prosecuting Users who are involved in such violations.

5. Viruses, worms, trojans and denial of service attacks

It is important to protect networks and devices on them against higher level malicious programs (such as viruses, worms and Trojans) and lower level Denial of Service (DoS) attacks that can be distributed or propagated via the Internet, including email.

All customers must ensure that they have in place appropriate protection for their systems, networks and devices to reduce the risk of transmission of such computer programs, and reduce the likelihood of such attacks originating, from their networks, systems and devices through the network. Such protection methods may include firewalls, an appropriate policy regarding email attachments and the most up to date virus scanning software.

6. Suspension or termination

Pennytel may suspend or terminate any User's service if we determine, that the User has violated any element of this policy.

We may give notice to a User warning that the User's use of a service is in violation of this policy and that their service will be suspended or terminated. If the User does not rectify their use of a service, we will suspend or terminate the User's service.

We may also immediately suspend or terminate a User's service without notice or waring if we determine, at our sole and absolute discretion, that the User has violated any element of this policy. We may also suspend or terminate a service if required by any applicable law.

Pennytel may seek written assurances from Users that they will cease using a service in a way that violates this policy.

Pennytel is not liable for any damages of any nature whatsoever suffered by any end user, or any third person resulting in whole or in part from Pennytel's exercise of its rights under this policy.

If required by applicable law, Pennytel may suspend or terminate a service immediately and without notice.

7. Monitoring

Pennytel has no obligation to monitor the network, but reserves the right to do so, including as required by applicable law, and to remove any material on, or block any data transmitted over, the network in its sole discretion.

Pennytel takes **no responsibility** for any material input by third persons and not hosted on or transmitted over the network by Pennytel itself. Pennytel is not responsible for the content of any web sites hosted on or accessible using the network other than its own web sites.

8. Site blocking

Pennytel may block access to Internet sites or Internet access where required to do so by applicable laws.