

1. Introduction

- 1.1 This is the ACN Pacific Pty Ltd ("ACN", 'we', 'us' 'our') Acceptable Use Policy ("Acceptable Use Policy") applicable to all users of ACN Services (in which case it forms part of ACN's Standard Terms) and to all ACN Independent Business Owners (in which case it forms part of ACN's Independent Business Owner Agreement). ACN may modify this Acceptable Use Policy at any time in its sole and absolute discretion.
- 1.2 This Acceptable Use Policy applies to all ACN products, equipment and services ("Services").
- 1.3 The provisions of this Acceptable Use Policy are designed to protect the quality of our Services and the operation of our networks, the networks of our Network Providers and the internet, and to prevent or reduce uses of such networks that are illegal or otherwise harmful to other people. They are also designed to protect us against liability from the activities of third parties including users of our Services. You are responsible for ensuring that use of the Services complies with this Acceptable Use Policy. You are responsible for any use of the Services even if, for example, it was used without your consent by a friend, family member, guest, employee or other person who gains access to the Services.

2. Excessive or unreasonable use

- 2.1 We will consider your use of our Services to be excessive or unreasonable if you:
 - a. use the Services other than for your personal (including small business) use;
 - b. share your Services with the occupants of other dwellings or premises, or connect your Services to networking equipment located in other dwellings or premises;
 - c. use the Services for commercial or wholesale purposes (including for the purpose of resale, refile, transit or aggregation);
 - d. use the Services for SIM-boxing or in connection with a device that switches or re-routes calls to and from our network or the network of any Supplier;
 - e. use the Services in a manner which causes significant congestion to, or disrupts or otherwise unreasonably and adversely affects, our networks or the networks of our Network Providers;
 - f. set up devices which may potentially allow a line or call to be kept open, limiting the ability of other customers to access our network or the network of any Supplier; or
 - g. engage in other similar or comparable activities.
- 2.2 If we identify that your use is excessive or unreasonable or identify usage of your Services that reasonably indicates excessive or unreasonable use, we may, at our discretion, choose to apply standard call rates to excess calls or minutes of use (as applicable) or refuse you further access to the Services and/or the relevant Plan or suspend or restrict your use of the Services. If we refuse you access to the relevant Plan we will then charge you our standard rates for all calls or minutes of calling which otherwise would have been eligible for the Plan.

3. Unlawful or prohibited use

- 3.1 ACN Services may be used only for lawful purposes. You may not use our Services in order to transmit, distribute or store material:
 - a. in violation of any applicable local, state or international law, order, regulation or industry code of practice;
 - b. for any fraudulent activities including impersonating any person or entity or forging anyone else's digital or manual signature;

- c. 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. You assume all risks regarding the determination of whether material is in the public domain; or
- d. that is obscene, threatening, abusive or hateful; or
- e. that contains a virus, worm, Trojan horse, or other harmful component ("Malicious Program"); or
- f. that promote pyramid or other illegal soliciting schemes.

4. No Spam

4.1 It is a prohibited use of our Services to transmit or distribute unsolicited and/or bulk data (which includes, without limitation, e-mail, bulletin boards, newsgroups, software, files in bulk). The only circumstances in which our Services may be used to send unsolicited and/or bulk data of an advertising or promotional nature is where the unsolicited 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 data from the sender from time to time, for example by ticking a box to that effect on the sender's web site. Unless these requirements are met, you must not send unsolicited bulk data on our Services. If these requirements are met, you must also provide an unsubscribe function on their web site (and make this function known to recipients in the relevant data) which allows those recipients to elect to be removed from that mailing list.

5. Other Prohibited Uses

5.1 The following activities are also prohibited uses of our Services:

- a. sending data, or causing data to be sent, to or through our Services 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 bulk unsolicited data whether the original was sent via our Services or not or hosting a web site to which recipients of bulk unsolicited 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 e-mail addresses of others for the purpose of sending unsolicited e-mails 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 computer;
- g. persistently sending data without reasonable cause or for the purpose of causing annoyance, inconvenience or needless anxiety to any persons;
- h. sending mass postings of messages to post advertisements other than in newsgroups that specifically encourage or permit advertising;
- i. sending post binary files other than in newsgroups that specifically encourage or permit such postings;
- j. distributing or making available indecent, obscene, offensive, pornographic, illegal or confidential information.

6. System and preventing unauthorised access

6.1 You must take reasonable steps to ensure that others do not gain unauthorised access to the Services. You must notify us immediately of any unauthorised or attempted unauthorised use of your Service and any other breach or attempted breach of security. It is your responsibility to ensure that you have in place appropriate protection for your systems and to prevent circulation of Malicious Programs from your computer or networks through our Services.

6.2 You are prohibited from violating or attempting to violate the security of our Services including without limitation by:

- a. accessing material not intended for you or logging into a server or account which you are 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 service to any user, host or network, including, without limitation, via means of overloading, "flooding", "mail bombing", "crashing" or a denial of service attack;
- d. forging any TCP/IP packet header or any part of the header information in any e-mail or newsgroup posting; or
- e. taking any action in order to obtain services to which you are not entitled.

7. Viruses, Worms, Trojan and Denial of Service Attacks

7.1 As you should be aware, it is important to protect your computer or other Internet access device and any connected networks against higher level computer programs (such as viruses, worms, Trojans and other malicious programs) and lower level Denial of Service (DoS) attacks that can be distributed or propagated via the Internet, including electronic mail. It is your responsibility to ensure that you have in place appropriate protection for your systems and to prevent circulation of such computer programs and attacks from your computer or networks through our Services. Such protection methods may include firewalls, an appropriate policy regarding email attachments and the most up-to-date virus scanning software.

8. Suspension or Termination of Service

8.1 If we determine, in our sole discretion, that you have violated any element of this Acceptable Use Policy you will receive a written warning, and may be subject, at our discretion, to a temporary suspension of service pending such your agreement in writing to refrain from any further violations; provided, however, that if we deem it necessary, and in our sole discretion, we may immediately suspend or terminate your Service(s) without issuing such a warning. If we determine that you have committed a second violation of any element of this Acceptable Use Policy, you will be subject to immediate suspension or termination of service without further notice and we may take such further action as we solely determine to be appropriate under the circumstances to eliminate or preclude such violation. We will not be liable for any damages of any nature suffered by you, another user, or any third party resulting in whole or in part from our exercise of our rights under these policies. If required by applicable law we may suspend or terminate a service immediately and without notice.

9. Monitoring

- 9.1 We have no obligation to monitor your usage of the Service(s), but reserve the right to do so,
- a. to identify violations of this Acceptable Use Policy; and
 - b. to protect our network, the other users of the Service(s) and the rights of other Internet users, including as required by applicable law, and remove any material at our sole discretion. We take no responsibility for any material input by others and not posted to our Services by us. We are not responsible for the content of any other web sites linked to ACN websites; links are provided as Internet navigation tools only.
- 9.2 We may intercept communications for the purposes of the Department of Internal Affairs' Digital Child Exploitation Filtering system.

10. Incident Reporting

10.1 Any complaints regarding the violation of this Acceptable Use Policy by an ACN customer or user should be directed to the contact numbers listed below. Where possible, include details that would assist us in investigating and resolving the complaint (e.g. expanded headers and a copy of the offending transmission).

Contact us:

By email: abuse@acnpacific.com.au

By phone: 0508 226 000

Post: ACN Pacific Pty Ltd, PO Box 90694, Victoria Street West, Auckland 1142