

Acceptable Use Policy

1. About

1.1. This document is the MedicCom Acceptable Use Policy (Acceptable Use Policy or AUP).

1.2. This policy:

- a) sets out the rules which apply to the use of our Services, including your responsibilities, permitted uses and prohibited uses of those Services; and
- b) seeks to maintain and protect the integrity of the infrastructure, Network and systems used to deliver the Services to ensure that you and all other users can enjoy optimum use of our Services.

1.3. Where capitalised terms are not defined in this policy, they have the meaning given to them in the Standard Form of Agreement.

- a) your Application;
- b) any Service Schedule for your Service;
- c) these General Terms;
- d) Pricing Schedules for your Service;
- e) any Hardware Warranty Information; and
- f) our Acceptable Use Policy.

Where there is any inconsistency between any of the terms of the SFOA, the order of precedence will be as listed above, except that clause 16 takes precedence over all other terms in the SFOA.

2. Application

2.1. This policy applies to all customers who acquire Services from us.

2.2. Your obligation to comply with this policy includes your obligation to ensure any person who you allow to use your Service also complies with this policy.

3. Responsible Use

3.1. You are responsible for your actions on our Network and systems you access through our Services.

3.2. You must not act recklessly or irresponsibly in using our Services or by your actions endanger any person or the integrity or security of our Network, systems or equipment.

3.3. You must not use, attempt to use, or authorise, aid, abet, encourage or incite any other person to use or attempt to use, the Services:

- a) for any illegal conduct or in an illegal manner;
- b) in any manner that may present a threat or risk to the security of our Services or the integrity of our Network;
- c) for any purpose stated to be prohibited in your Application or in your Service Schedule;

- d) in any manner that may cause death, personal injury or damage to property;
- e) to store, send, reproduce, publish, or distribute any confidential information, copyright material or other content which is subject to third party intellectual property rights, unless you have a lawful right to do so;
- f) in any manner which is defamatory, abusive, menacing, threatening, harassing, offensive, violates privacy, or incites violence or hatred towards any person or class of persons, or which could give rise to civil or criminal proceedings;
- g) in any manner which is illegal, fraudulent or otherwise prohibited under any applicable Commonwealth, State or Territory law or which is in breach of any code, standard or content requirement of any other competent authority;
- h) to store, send, reproduce, publish, or distribute any content or material which is restricted, prohibited or otherwise unlawful under any applicable Commonwealth, State or Territory law, or which is likely to be offensive or obscene to a reasonable person;
- i) to make inappropriate contact with children or minors;
- j) to provide unrestricted access to material that is unsuitable for minors;
- k) to do anything (including store, send or distribute material) which interferes with other users or restricts or hinders any person from accessing, using or enjoying the Internet, our Services, Network or systems;
- l) to forge header information, email source address, or other user information, or otherwise maliciously or illegally impersonate or obscure the original source of data;
- m) to access, monitor, use, control, or make modifications to, or otherwise interfere with, any other person's equipment, systems, Networks or data, without that lawful authority;
- n) to attempt to probe, scan or test the vulnerability of any other person's equipment, systems, Networks or data, without lawful authority;
- o) to compromise the security or integrity of any Network or system;
- p) to access, download, store, send or distribute any harmful programs or material with the intent of compromising the security of any Network or system (including viruses, Trojans, or password guessing programs);
- q) to engage in any unreasonable activity which impairs the ability of other people or systems to use our Services or

- r) to tamper with, hinder the operation of or make unauthorised modifications to any Network or system;
- s) to host servers for business or private use, without prior consent.

3.4. You must not use another person's name, username or password or otherwise attempt to gain access to the account of any other user.

3.5. You must not resell our Services or otherwise act as a Carriage Service Provider

3.6. You must not use or attempt to use our Services to store credit card data without our express consent in writing.

4. Spam

4.1. must not use the Service for any purpose contrary to the Spam Act 2003 (Cth) (Spam Act).

4.2. this policy, Spam includes one or more unsolicited commercial electronic messages to which the Spam Act applies.

4.3. You must not use the Service to:

- a) Send, or assist in the sending of Spam;
- b) use or distribute and software designed to harvest email addresses;
- c) host any device or service that allows email to be sent between third parties not under your authority or control;
- d) otherwise breach the Spam Act

4.4. We actively seek to minimise Spam on our Network. We may scan any IP address ranges allocated to you for use with your Services in order to detect the presence of open or otherwise misconfigured mail and proxy servers (although we are not obliged to do so). If we detect open or misconfigured mail or proxy servers we may restrict, suspend or terminate the supply of the Services to you.

5. Excessive, Unusual or Unreasonable Use

5.1. You must use the Services in accordance with any download or capacity limits stated in your specific plan. You must not unreasonably exceed the download or capacity limits stated in your specific plan,

5.2. You must not excessively use the capacity or resources of our Network in a manner which may hinder or prevent us from providing Services to other customers or which may pose a threat to the integrity or security of our Network, systems or equipment.

5.3. You must not use the Service in a manner which could reasonably be regarded as excessive, unreasonable, unusual, or non-ordinary use.

5.4. Without limiting clause 5.3 and by way of example, we consider use of the Service to be unreasonable or unusual where:

- a) a private customer uses the Service in any way which could not reasonably be considered ordinary personal use (for example, using the Service for business or commercial use); or
- b) a business customer uses the Service in any way which could not reasonably be considered as use in the ordinary course of business.

6. Providing the Services and Our Obligations

6.1. You are responsible for maintaining the security of any of your devices or Networks, including protecting your account details and passwords and preventing unauthorised use of devices and Services by third parties.

6.2. We recommend that you take appropriate security measures to prevent unauthorised use of the Services, or use in breach of this policy, by third parties. Such measures may include:

- a) installing and maintaining a firewall and anti-virus software;
- b) regularly updating operating system and application software;
- c) protecting any Wi-Fi Network you operate; and
- d) requiring third parties that you allow to use the Service to abide by this policy.

6.3. You are responsible for all charges incurred by other persons who use your Service, including anyone to whom you have disclosed your password and account details.

6.4. For the avoidance of doubt, our rights to restrict, suspend, or cancel the supply of the Services to you under the Standard Form of Agreement, arise whether or not the breach of this policy was committed by a third party (including by means not authorised by you, such as viruses, Trojans and other security breaches).

7. Copyright

7.1. You are responsible for ensuring that you do not infringe the intellectual property rights of any person in relation to any material that you access or download from the internet and copy, store, send or distribute using the Services.

7.2. You must not use the Services to copy, adapt, reproduce, distribute or otherwise make available to other persons any content or material (including but not limited to music and video files in any format) which is subject to copyright, unless you have a lawful right to do so.

7.3. You must not use the Services to do any other acts in relation to such copyright material which would infringe the exclusive rights of the copyright owner under the Copyright Act 1968 (Cth) or any other applicable laws, unless you have a lawful right to do so.

7.4. We may immediately cease hosting and remove from our Network or systems any content upon receiving a complaint or

allegation that the material infringes copyright or any other intellectual property rights of any person.

8. Content

8.1. You are responsible for determining the content and information you choose to access on the Internet when using the Services.

8.2. You are responsible for taking any steps you consider necessary (for example, installing filtering programs) to prevent access to offensive or obscene content on the Internet by children or minors who you allow to use the Services. Further information on content filtering programs is available on the Communications Alliance website (<http://www.commsalliance.com.au>).

8.3. You are responsible for any content you store, send or distribute on or via our Network and systems including, but not limited to, content you place or post on web pages, email, chat or discussion forums, bulletin boards, instant messaging, SMS and Usenet news. You must not use such services to send or distribute any content which is prohibited, deemed obscene or offensive or otherwise unlawful under any applicable Commonwealth, State or Territory law.

8.4. You must label or clearly identify any content you generally make available using the Services in accordance with the applicable classification guidelines and National Classification Code or any industry code which applies to your use or distribution of that content. We may remove from our Network and servers any content which is classified, or likely to be classified, as 'prohibited' content.

8.5. We cooperate fully with law enforcement and security agencies, including in relation to court orders for the interception and monitoring of our Network and systems. We may take these steps at any time without notice to you. You must not hinder or prevent us from taking any steps necessary to comply with any direction from the Australian Communications and Media Authority (ACMA) or any other Regulatory Authority, law enforcement or security agency.

8.6. We may provide your username, IP address or other identifying material to the Australian Federal Police or other authorities when required to do so.

8.7. If you have a complaint about content accessible on the Internet you may contact the ACMA by lodging an online complaint form at www.acma.gov.au, emailing online@acma.gov.au or faxing your complaint to the ACMA Content Assessment Hotline Manager on (02) 9334 7799. You may also report a complaint about content by emailing us at support@MedicCom.com.au.

9. Breach of the AUP

9.1. We may restrict, suspend or cancel your Service under the Standard Form of Agreement if there are reasonable grounds to suspect that you, or any person who accesses your Services, have failed to comply with this policy.

9.2. If you breach this policy, we will generally contact you and give you the opportunity to rectify the breach. If you do not rectify the breach within a reasonable period, we may suspend or cancel your Service without further notice to you.

9.3. If you commit a serious (such as illegal or non-ordinary use) or continuing breach of this policy, we reserve the right to immediately suspend or cancel your Service without notice to you.

9.4. If we notify you of a breach of your Spam obligations under section 4, we will, at your request and to the extent we are reasonably able, supply you with information as to the nature of open relays and suggested resolutions to assist you to comply with these obligations.

9.5. In the event that the supply of Services to you is cancelled by us, you may apply for a pro-rata refund of any pre-paid charges you have paid for the Services, but we may deduct any reasonable costs incurred as a result of the conduct that resulted in the cancellation.