Fair Go Policy

This Fair Go Policy ("Policy") applies to all services provided by Australian Postal Corporation trading as Australia Post Mobile and Australia Post Broadband ("Us").

It is important to us that all eligible customers are able to access our services. Accordingly, we have devised this Policy which applies to:

- using our services and plans; and
- any promotions or services which are advertised by us as subject to this Policy ("Fair Go Promotions").

We reserve the right to vary the terms of this Policy from time to time.

We may rely on this Policy where:

- your usage of our services is unreasonable; or
- your participation in a Fair Go Promotion is excessive or unreasonable, as defined below.

1. Unreasonable Use

Unreasonable use of our services is usage that's reasonably considered by us to be excessive or fraudulent or could adversely affect our network or other customers' use of or access to any of those services or network.

Among other things, "fraudulent use" includes resupplying one of our services without our consent so that someone else may access, or use, our data services or take advantage of a Fair Go Promotion.

Example of uses which we consider 'unreasonable' include but are not limited to:

- using the service for fraudulent purposes;
- abnormal or excessive use of back to base services;
- SIM boxing or using the service in connection with a device that switches or re-routes calls to or from our network to another carrier's network;
- wholesaling any service or using the service in connection with any device that switches or reroutes calls potentially keeping a line open for hours;
- using the service to wholesale supply of any service (including transit, refile or aggregate domestic or international traffic) on our network.
- calling 13xx or 18xx numbers to make indirect calls through other providers (eg. through a calling card);
- using the service for the purposes of arbitrage;
- using the service in connection with a device that automatically dials numbers either from a list or are generated randomly;
- using the service to make or receive calls on our network for the purposes of resale, resupply or commercial exploitation;
- using the service for continuously call forwarding or multiple simultaneous calling;
- using the service for bulk messaging;
- using a 'mobile voice' SIM card in a non 'mobile voice' device;
- using the service for anything which isn't standard person to person communication.

2. Unacceptable Use

You may not use the services in any manner which improperly interferes with another person's use of the services or for illegal or unlawful purposes. You may not use any equipment or devices on the network (including SIM cards) which have not been provided by us.

Examples of uses which we consider 'unacceptable' include but are not limited to:

- providing us with any type of false information to use the service;
- using the service to send unsolicited or unwanted commercial electronic messages;
- using the service to gain improper access to another person's private or personal information;
- using the service to distribute or make available indecent, obscene, offensive, pornographic, illegal or confidential material;
- using the service to defame, harass or abuse anyone or violate their privacy;
- contravening any applicable laws when you use the service;
- using the service to communicate with emergency service organisations where an emergency situation does not exist;
- using the service to distribute or make available material that is misleading or deceptive as to your identity;
- infringing any person's intellectual property rights, including copyright, when you use the service;
- using the service to monitor data or traffic on any network or system if you do not have the authorisation of the owner of the network or system to do so;
- using the service in a way which interferes or disrupts the service, any computer system access through it or any other person's use of it;
- using the service to obtain or attempt to obtain unauthorised access to any computer, system or network;
- using the service in a manner designed to compromise the security or interfere with the operation of the service or any other computer, system or network.

3. Use of the Internet

You are responsible for all risks associated with use of the service. We, nor the network supplier (being Optus) bear any responsibility or liability relating to your use of the internet.

Customers accessing Australia Post Broadband must also comply with any fair use policy published by NBN Co from time to time.

3.1 Responsible Usage

You are responsible for your actions on our telecommunications network ("Network") and any systems you access through your Service. If you use your Service recklessly or irresponsibly or your actions endanger any person or the integrity or security of our Network, systems or equipment, your access may be restricted, suspended or terminated, without prior notice.

In particular, you agree that you will not use, attempt to use or allow your Service to be used to:

- store, send 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;
- store, send or distribute 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;
- do anything, including do anything, including store, send or distribute material which defames, harasses, threatens, abuses, menaces, offends, violates the privacy of, or incites violence or hatred against, any person or class of persons, or which could give rise to civil or criminal proceedings;
- do anything else that 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;
- 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;
- forge header information, email source address or other user information;
- access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network;

- compromise the security or integrity of any network or system (including ours);
- access, download, store, send or distribute any viruses or other harmful programs or material;
- send or distribute unsolicited advertising, bulk electronic messages or overload any network or system (including ours);
- use another person's name, username or password or otherwise attempt to gain access to the account of any other customer;
- tamper with, hinder the operation of or make unauthorised modifications to any network or system;
- host or assist in the hosting of a Tor relay and/or exit node; or
- authorise, aid, abet, encourage or incite any other person to do or attempt to do any of the above acts.

3.2 Spam

In this Policy, "Spam" includes one or more unsolicited commercial electronic messages to which the *Spam Act 2003* (Cth) (“Spam Act”) applies. Any variations of the word "Spam" have corresponding meanings.

3.3 Codes of Practice

The Internet Industry Codes of Practice registered with the Australian Communications and Media Authority ("ACMA") set out how service providers, such as us, and email service providers must address the sources of Spam within their own networks. They also require service providers and email service providers to give end-users information about how to deal with Spam so they can make an informed choice about their filtering options.

3.4 Suspension or Termination

This Policy prohibits you from using your Service to send Spam. If you breach this prohibition, we may suspend or terminate your Service. The circumstances in which we may do so are set out in section 3.14 below.

3.5 Reducing Spam

You can reduce the amount of Spam you receive if you:

- do not open emails from dubious sources;
- do not reply to Spam or click on links, including ‘unsubscribe' facilities, in Spam;
- do not accept Spam-advertised offers;
- block incoming mail from known Spammers;
- do not post your email address on publicly available sites or directories. If you need to do so, look for options, such as tick boxes that allow you to opt out of receiving further offers or information;
- do not disclose your personal information to any online organisation unless they agree (in their terms and conditions or privacy policy) not to pass your information on to other parties;
- use separate email addresses for different purposes, such as a personal email address for friends and family and a business email address for work;
- install a Spam filter on your computer to filter or block Spam. We strongly recommend that you install a Spam filter on your computer, even if you receive a Spam filtering service from us. Information on the availability of anti-Spam software for end-users is available at the Internet Industry Association (“IIA”) website.
- report any Spam you receive to us or to ACMA (see "Complaints" below); and
- visit the ACMA website (http://www.acma.gov.au/Industry/Marketers/Anti-Spam) for more information on ways to reduce the volume of Spam you receive, including how to:
    - reduce Spam if you operate a website; and
    - avoid becoming an accidental Spammer.

3.6 Your Spam Obligations

You agree that you will use your Service in compliance with the Spam Act and will not engage in practices which would result in a breach of the Spam Act. In particular, you agree that you will not use, attempt to use or allow your Service to be used to:

- send, allow to be sent, or assist in the sending of Spam;
- use or distribute any software designed to harvest email addresses;
- host any device or service that allows email to be sent between third parties not under your authority or control; or
- otherwise breach the Spam Act or the *Spam Regulations 2004* (Cth) (your "Spam Obligations").

You agree to do your best secure any device or network within your control from being used in breach of your Spam Obligations by third parties, including where appropriate:

- installation and maintenance of antivirus software;
- installation and maintenance of firewall software; and
- applying of operating system and application software patches and updates.

We may scan any IP address ranges allocated for use with your Service to detect any open or otherwise misconfigured mail and proxy servers. If we detect an open or misconfigured mail or proxy servers, we may suspend or terminate your Service.

3.7 Excessive Use

You must use your Service in accordance with any download or capacity limits stated in the specific plan that you subscribe to. We may limit, suspend or terminate your Service if you unreasonably exceed those limits – or excessively use the capacity or resources of our Network in a way that could hinder or prevent us from providing services to other customers, or may pose a threat to the integrity of our Network or systems.

For customers accessing Australia Post Broadband using the nbn® Fixed Wireless access technology, excessive use is considered:

a) where the average download usage exceeds 200GB of data in a calendar month; or
b) where the average upload usage exceeds 60GB of data in a calendar month.

3.8 Security

You are responsible for maintaining the security of your Service – including protecting your account details and passwords, as well as any unauthorised usage of your Service by a third party. We recommend that you take appropriate security measures, like installing a firewall and using up to date anti-virus software. You are responsible for all charges incurred by other persons who you let use your Service – including anyone you've disclosed your password and account details to.

3.9 Copyright

It is your responsibility to make sure that you do not infringe the intellectual property rights of any person through material that you access or download from the Internet and copy, store, send or distribute using your Service.

You must not use your Service to copy, adapt, reproduce, distribute or otherwise make available to other persons any content or material (including but not limited to music files in any format) which is subject to copyright or do any other acts relating to that copyright material which would infringe the exclusive rights of the copyright owner under the *Copyright Act 1968* (Cth) or any other applicable laws.

You acknowledge and agree that we have the right to immediately cease hosting – and to remove from our Network or systems – any content that we've received a complaint or allegation about for infringing copyright or any other intellectual property rights of any person.

3.10 Content

You are responsible for determining the content and information you choose to access on the internet when using your Service.

It is your responsibility to take all steps you consider necessary (including the use of filtering programs) to prevent access to offensive or obscene content on the Internet by children or minors who you allow to use your Service. You can find out more about content filtering products at the IIA website.

You must not use, or attempt to use, your Service to make inappropriate contact with children or minors.

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, including to send or distribute classes of restricted content to children or minors if that is prohibited or an offence under such laws.

Failing to comply with these requirements may lead to your Service being immediately suspended or terminated without notice. If we have reason to believe you have used your Service to access child pornography or child abuse material, we are required by law to refer the matter to the Australian Federal Police.

3.11 Regulatory Authorities

You must label or clearly identify any content you generally make available using your Service in accordance with the applicable classification guidelines and National Classification Code (issued pursuant to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth)) or any industry code which applies to your use or distribution of that content.

Commonwealth legislation allows ACMA to direct us to remove any content which is classified, or likely to be classified, as 'prohibited', from our Network and servers. We also co-operate fully with law enforcement and security agencies – including any court orders for the interception or 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 all the necessary steps to comply with any direction from ACMA or any other law enforcement or security agency. You acknowledge we reserve the right to limit, suspend or terminate your Service if there are reasonable grounds for suspecting that you are engaging in illegal conduct or where use of your Service is subject to any investigation by law enforcement or regulatory authorities.

3.12 Complaints about content

If you have a complaint about content accessible using your Service you can contact ACMA by filling out an online complaint form at acma.gov.au, emailing online@acma.gov.au or faxing your complaint to the ACMA Content Assessment Hotline Manager on (02) 9334 7799. Please note that all complaints to ACMA must be in writing. You may also report a complaint about content via email.

3.13 Complaints about Spam

All internet and email service providers are required by the Internet Industry Code of Practice to maintain an "abuse@" email address (or other email address as notified by the service provider) so that end users to report Spam. If you think you have been sent Spam by one of our subscribers, please contact us by emailing abuse@australiapostconnect.com.au. If you think you have been sent Spam by a subscriber of another internet or email service provider, you can report it by emailing that service provider at their "abuse@" email address or other email address as notified by the service provider for that purpose.

You can report or make a complaint about Spam you have received by contacting ACMA by filling out an online complaint form at acma.gov.au or via the ACMA Spam Reporting System Spam Matters.
You may also make complaints to other bodies about Spam where the content is in some other way offensive or contrary to law. For example, you may complain to ACMA about Spam that contains content you believe is offensive or relates to online gambling.

You can report a Spam message that contains fraudulent or misleading and deceptive content (for example, email scams) to the Australian Competition and Consumer Commission ("ACCC") via the ACCC website by phoning 1300 302 502 (business hours, Monday to Friday).

The Australian Securities and Investment Commission ("ASIC") also deals with certain complaints about the contents of Spam messages, particularly with regard to fraudulent conduct by Australian businesses. The ASIC website outlines the types of complaints they deal with and has an online complaint form: www.asic.gov.au (click on 'Complaining About Companies or People').

If you are concerned that your personal information has been misused to send you Spam, the Office of the Australian Information Commissioner ("OAIC") recommends that you complain to the organisation first, especially if you know how to contact it and have had dealings with it in the past about other goods or services. If the matter is not resolved adequately, you can visit the OAIC's website for details on how to make a complaint.

3.14 Suspension or Termination

We reserve the right to suspend your Service if you are in breach of this Policy, provided that we will first take reasonable steps to contact you and give you the opportunity to rectify the breach within a reasonable period. What is reasonable in this context will depend on the severity of the problems being caused by the breach (for example, if you commit a serious or continuing breach, it may be reasonable to immediately suspend your Service without notice to you).

If, after we have contacted you, your excessive or unreasonable use continues, we may, without further notice to you:

- Apply a service reduction to your Service;
- Suspend or limit the Service (or any feature of it) for any period we think is reasonably necessary; and/or
- Terminate your Service with us.

If we notify you of a breach of your Spam Obligations, 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 your Spam Obligations.

Our right to suspend your Service applies regardless of whether the breach is committed intentionally, through misconfiguration, or by other means not authorised by you including but not limited to through a Trojan horse or virus.

In the event your Service is terminated, you may apply for a pro rata refund of any pre-paid charges for your Service, but we will have the right to levy a reasonable fee for any costs incurred as a result of the conduct that resulted in the suspension.

3.15 Changes

We may vary this Policy by updating these conditions on our website or elsewhere in accordance with the notice provisions of your service agreement with us. Continuing to use your Service after this notice will constitute your accepting of the changes.