



Internet
Association
of Australia

Acceptable Use Policy

December 2016

Category:	I.T.
Status:	Approved
Version:	1.1
Approval Date:	5 December 2016
Prepared by:	K. Ireland



Table of Contents

<i>Acceptable Use Policy</i>	3
<i>Change History</i>	5



Acceptable Use Policy

This policy applies to all Members who obtain Member Services from Us and any person for whom Members are responsible when they use Our Member Services.

Your failure to comply with this Policy (including by any person who you allow to use Member Services that We supply to You) may lead to the suspension or termination of your Member Services.

1.1. You agree that:

- (a) using the Websites, Members Portal and/or Member Services to violate all or any legal rights of any person or company or other entity in any jurisdiction is strictly prohibited;
- (b) using the Websites, Members Portal and Member Services in relation to crimes such as theft and fraud is strictly prohibited;
- (c) using the Websites, Members Portal and/or Member Services in breach of laws relating to the protection of copyright, trade secrets, patents or other intellectual property and laws relating to spam or privacy and whether such violation is by way of the installation or distribution of "pirated" software or otherwise, is strictly prohibited;
- (d) introduction of malicious programs into Our network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs) is strictly prohibited;
- (e) revealing Your account password to others or allowing use of Your account on the Websites and/or Members Portal or to allow use of the Member Services by others is strictly prohibited;
- (f) using another person's name, username or password or otherwise attempting to gain access to the Member Portal or Member Services account of any other person is strictly prohibited;
- (g) using the Websites, Members Portal and/or Member Services to make fraudulent offers of goods or services is strictly prohibited;
- (h) using the Websites, Members Portal and/or Member Services to carry out security breaches or disruptions of network communication is strictly prohibited. Security breaches include, but are not limited to, accessing data of which You are not an intended recipient or logging into a server or account that You are not expressly authorised to access or corrupting any data. For the purposes of this paragraph, "security breaches" includes, but is not limited to, network sniffing, pinged floods, packet spoofing and denial of service;
- (i) compromising the security of Our property, systems, networks, equipment or services, or those of any other Members is strictly prohibited;
- (j) using the Websites, Members Portal and/or Member Services to execute any form of network monitoring which will intercept data not intended for You is strictly prohibited;
- (k) using the Websites, Members Portal and/or Member Services to circumvent user authentication or security of any of Our hosts, networks or accounts or those of Our



-
- customers, Members or suppliers is strictly prohibited;
- (l) using the Websites, Members Portal and/or Member Services to interfere with or deny service to anyone is strictly prohibited;
 - (m) using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, any person's use of the Websites, Members Portal and/or Member Services is strictly prohibited;
 - (n) forging header information, email source addresses or other user information is strictly prohibited;
 - (o) sending unsolicited email messages through or to users of the Websites, Members Portal and/or Member Services in breach of the *Spam Act 2003* is strictly prohibited;
 - (p) using the Websites, Members Portal and/or Member Services to send any form of harassment via email, or any other form of messaging, whether through language, frequency, or size of messages is strictly prohibited; and
 - (q) use of the Websites, Members Portal and/or Member Services in breach of any person's privacy (such as by way of identity theft or "phishing") or in breach of the *Privacy Act 1998 (Cth)* is strictly prohibited.
- 1.2.** You must notify Us if the security of any of Your Equipment is compromised, hacked or used to carry out any network attack, denial of service attack or similar.
- 1.3.** You must not aide, abet, incite or encourage any person to breach this Acceptable Use Policy.



Change History

Version:	Date:	Nature of change
1.0	5 December 2016	Initial document approved
1.1	18 November 2021	Updated template Updated Inc to Ltd