AAPT [BusinessConnect]

Acceptable Use Policy

This Acceptable Use Policy (**Policy**) applies to all users of the services supplied by any of our corporate group businesses, including Ethan Group Pty Ltd, Connect ANZ Pty Ltd and AAPT Business Connect, including but not limited to individual end users, company or corporate use, or guest use (**Users**).

We may modify this Policy at any time in our sole and absolute and any changes will be reflected on this page. Use of any of our services after the posting of any changes will be considered acceptance of those changes.

1. AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK (ACORN)

Users must not engage in any cybercrime whatsoever, including but not limited to cyber-bulling, email spam and phishing, identity theft, accessing or otherwise dealing with prohibited offensive and illegal content, engaging in online scams or fraud or other online trading issues.

For further information on cybercrime, please visit https://www.acorn.gov.au/learn-about-cybercrime.

2. USE ONLY FOR LAWFUL PURPOSES

Users must only use our services, including any upstream carrier network, or websites operated by us for lawful purposes.

Users may not use our services in order to transmit, distribute or store material:

(a) in violation of any applicable law;

(b) in violation of the Communications Alliance industry code C525:2017 - Handling of Life Threatening and Unwelcome Communications. For more information please visit http://www.commsalliance.com.au/__data/assets/pdf_file/0018/56223/C525_2017.pdf;

(c) in a manner that will infringe the copyright, trade mark, trade secret or other intellectual property rights of others; or

(d) in a manner that will infringe the privacy, publicity or other personal rights of others, as required under any applicable privacy related legislation, including the Privacy Act 1988 (Cth). For further information on the Australian Privacy Principles, please visit https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.

3. SYSTEM AND NETWORK SECURITY

Users are prohibited from violating or attempting to violate the security of our services, 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. Authorisation may be sought via your Service Delivery Manager; or

(c) taking any action in order to obtain services to which such User is not entitled. For example, SIP or VOIP hacking, or allowing contracted services to be used by other unauthorised parties.

Violations of system or network security may result in civil or criminal liability for the User. We will investigate occurrences that may involve such violations and may cooperate with law enforcement authorities in prosecuting Users who are involved in such violations.

4. SUSPENSION OR TERMINATION

We may suspend or terminate any User's service, including without notice, if we determine, in our sole and absolute discretion, that the User has violated any element of this Policy or if required by any applicable law, regulatory authority or law enforcement agency.

We may seek written assurances from Users that they will cease using a service in a way that violates this Policy as a condition of supply.

We are not liable for any loss of any nature whatsoever suffered by any User or third party arising out of or otherwise in connection with the exercise of our rights under this Policy.

5. MONITORING

We have no obligation to actively monitor the use of our services, but reserve the right to do so, including as required by applicable law, and to remove any material on, or block any data transmitted over, our network in our sole discretion.

We take no responsibility for any third party material whatsoever (i.e. any material not developed and hosted on our network by us).

We are not responsible for the content of any websites hosted on or accessible using our services other than content hosted on our own websites.

6. SITE BLOCKING

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