# National Capital Authority
# Customer Relationship Agreement

## ACCEPTABLE USE POLICY

**6 November 2018**

---

Rules of interpretation and capitalised terms used in this Acceptable Use Policy are defined in the General Terms of our Customer Relationship Agreement (CRA).

## 1. ABOUT OUR ACCEPTABLE USE POLICY

1.1 To ensure the availability of our Services to eligible customers, we have an Acceptable Use Policy to make sure everyone gets a fair go. We have designed our products to be generous, but we do not want those generous terms abused.

1.2 We may immediately suspend, cancel or restrict the supply of the Service to you under clause 12.3 of the General Terms if you use the Service, or if any person who accesses your Service uses the Service, in any way which breaches this Acceptable Use Policy.

## 2. PROHIBITED USE

2.1 You, and any person who accesses your Service, must not use, or attempt to use, the Service:

(a) for illegal purposes or practices;

(b) for any purpose if we advised you that such purpose was prohibited in your Application or the relevant Service Description;

(c) in any way which damages or interferes (or threatens to damage or interfere) with the operation of a Service or with the efficiency of our Network or a Supplier's Network (including as a result of attempts by you to increase the capacity or performance of your system or Your Equipment);

(d) in any way which makes it unsafe or which may damage any property or injure or kill any person;

(e) to transmit, publish or communicate any material or engage in any conduct which is defamatory, abusive, menacing or harassing;

(f) to engage in abusive behaviour toward our staff;

(g) to make inappropriate contact with children or minors;

(h) to access, store, reproduce, distribute, publish or commercially exploit any information or material of any kind that infringes any copyright, patent, trade mark, design or other intellectual property right;

(i) to send, relay or distribute any electronic data, the contents or properties of which have been manipulated for the purpose of maliciously or illegally impersonating or obscuring the original source of that data. This does not include the use of Virtual Private Networks or similar concepts in circumstances where this is legal and otherwise complies with this Policy;

(j) to access, monitor, use or control any other person's equipment, systems, networks or data (including usernames and passwords) or to otherwise probe, scan or test the vulnerability of any other person's equipment, networks, systems or data, without that person's consent;

(k) to access, or attempt to access, the accounts or private information of others, or to penetrate, or attempt to penetrate, our or a third party's security measures, computer software or hardware, electronic communications system or telecommunications system, whether or not the intrusion results in the corruption or loss of data. This does not include conducting network security testing specifically requested by the owner of the targeted network or system;

(l) to use or distribute software (such as password guessing programs, keyboard loggers, viruses or trojans) with the intent of compromising the security of any network or system;

(m) to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as 'pyramid schemes', 'Ponzi schemes', and 'chain letters';

(n) to engage in any unreasonable activity which impairs the ability of other people or systems to use our Services or the Internet. This includes any malicious activity resulting in an adverse effect such as denial of service attacks against another network host or individual user, flooding of a network, overloading a service, improper seizing or abuse of operator privileges, and attempts to harm a system or network. For the avoidance of doubt, this clause does not capture an activity solely because it unintentionally contributes to network congestion; or

(o) to access, store, reproduce, distribute or publish any content which is prohibited or unlawful under any Commonwealth, State or Territory law or

classification system, or to provide unrestricted access to material that is unsuitable for minors.

2.2 Due to Payment Card Industry (PCI) requirements, You, and any person who accesses your Service, must not use, or attempt to use, our web-hosting Services to store credit card data without our express consent in writing.

## 3. SPAM

3.1 In this clause 3, "Spam" includes one or more unsolicited commercial electronic messages with an "Australian link" as contemplated by the Spam Act 2003.

3.2 You must not use the Service to:

(a) send, allow to be sent, or assist in the sending of Spam;

(b) use or distribute any software designed to harvest email addresses; or

(c) otherwise breach the Spam Act 2003 or any regulations made under the *Spam Act 2003*.

## 4. GENERAL

4.1 You must use reasonable endeavours to secure any device or network within your control against being used in breach of this Acceptable Use Policy by third parties, including where appropriate:

(a) the installation and maintenance of antivirus and firewall software;

(b) the application of operating system and application software patches and updates;

(c) protecting your account information and password and taking all reasonable care to prevent unauthorised access to your service, including taking reasonable steps to secure any Wi-Fi network that your operate;

(d) for residential users, requiring any persons (for example, other members of your household) that you allow to use your Service from time to time to also comply with this Policy; and

(e) for business and government users, maintaining and enforcing appropriate workplace and guest user policies that are consistent with the requirements of this Acceptable Use Policy.

4.2 Unless otherwise stated, our rights to suspend, cancel or restrict the supply of the Service to you applies regardless of whether the breach or suspected breach was committed intentionally, or by means not authorised by you (such as through Trojan horses, viruses or other security breaches).