APC Acceptable Usage Policy

1. Introduction

1.1. This acceptable use policy (“AUP”) outlines the principles that govern use of the systems, services and equipment provided by APC Solutions UK Limited (“APC” or “we”) in connection with your APC services.

1.2. You must read this AUP very carefully. It forms part of your contractual services agreement with us.

1.3. “User(s)” or “you” means customers or anyone else who uses or accesses APC’s services.

1.4. We may amend, modify or substitute this AUP at any time. Your continued use of any APC services after any such amendment, modification or substitution constitutes your acceptance of any new AUP. We recommend that you visit our website regularly to check for any updates or amendments to this AUP.

2. APC’s enforcement actions – our rights to investigate, suspend, restrict or terminate your services

2.1. We reserve the right to investigate any suspected violation(s) of this AUP. When we become aware of possible violations, we may initiate an investigation, which may include gathering information from the User involved and the complaining party, if any, and examination of material on our servers, networks or any other equipment associated with the services.

2.2. We will take action if you abuse our services. The actions we may take, in our sole discretion, at any time include but are not restricted to:

(a) a quick chat on the phone or an informal email asking for your cooperation;

(b) a formal warning to you

(c) suspension of your account (with or without notice);

(d) restriction of your access to all or any part of our services (with or without notice); or

(e) termination of your account (with or without notice).

2.3. Notwithstanding our right to restrict, suspend or terminate your services, if you breach this AUP and/or our terms and conditions we may issue a formal warning to you specifying

the unacceptable conduct and notifying you that repeated breaches may result in all or part of our services being temporarily or permanently withdrawn from you.

2.4. If, after we have issued a formal warning in accordance with paragraph 2.3 above, your conduct continues to breach this AUP, then we will withdraw all or any part of the services from you until such time as we are satisfied that you have implemented appropriate steps to ensure that your use of our systems, services or equipment will comply with this AUP.

2.5. If such a suspension is imposed, then this may be lifted at our discretion upon receipt of a formal written undertaking from you not to commit any future relevant abuse. Until the formal written undertaking is received by us using the contact details we specify to you your account will remain suspended. APC is in no way responsible for any loss during transmission (post, email, fax).

2.6. Prior to terminating services as a general rule, we will attempt to work with Users (but are not obliged to do so) to avoid future violations of the AUP and to ensure that there is no reoccurrence of the incident(s) in question.

3. Use of the services

3.1. You must not use our services in any way that is unlawful or illegal or in any way to the detriment of other Internet users. You also must not allow anybody using your connection to use our services in any way that is unlawful or illegal or in any way to the detriment of other Internet users.

3.2. In addition to and without prejudice to your obligations pursuant to our terms and conditions, you agree to comply with (and ensure that others using the services comply with) all applicable laws, statutes and regulations in connection with the services. As the User of record, you are liable for all use of all accounts in your name, irrespective of use

without your knowledge and/or consent.

3.3. You are required to keep your contact details provided to APC up to date. Keeping such records up to date is important as we may need to send notices or other information to you using the contact information you gave us.

3.4. We normally notify customers of AUP-related issues by email prior to suspension/disconnection of services and it is important that you read these emails.

3.5. In the event that your use of our services is under investigation by relevant authorities, we reserve the right to suspend the services for the duration of the investigation.

4. Your responsibilities – security

4.1. The security of the services used by you from your business is your responsibility. We are not responsible for the consequences of your failure to employ adequate security measures (e.g. lost or corrupted files, identity theft, fraud).

Device security

4.2. Users are responsible for the security of their own devices that are directly or indirectly connected to our systems. This includes, but is not limited to: PCs, iPods/iPads (or equivalent), laptops, smart-phones, wired and wireless networking devices.

4.3. If we identify that devices on the end of your connection are causing significant impact to our service or are part of a “botnet” (machines hijacked by others to distribute malicious software or other forms of abuse), we reserve the right to suspend or disconnect your services without notice.

4.4. Users must ensure that their devices are protected with up-to-date anti-virus software and a properly configured firewall as a minimum where applicable.

Account security

4.5. You must keep your password(s) confidential and secure. If you think that your password(s) has become known to any unauthorised person or may be used in an unauthorised way you should take steps to change your password immediately. If you

believe that any of your devices have been used to breach the terms of this Acceptable Use Policy you must inform us immediately.

5. Your responsibilities – APC's systems, services and equipment

5.1. Users must not take any action that may restrict or inhibit any person, partnership, company, firm or organisation (whether a customer of APC or otherwise) in his/her/its lawful use or enjoyment of any of our systems, services or products.

5.2. Specific prohibited acts in relation to APC's systems, services and equipment are:

5.2.1. the sale or resale of our services and products;

5.2.2. any form of advertising or marketing practices - deceptive, misleading or otherwise;

5.2.3. furnishing false data on our sign-up forms, contracts or online applications, including fraudulent use of credit card numbers (and such conduct is grounds for immediate termination and may subject the offender to civil or criminal liability);

5.2.4. attempting to circumvent user authentication or security of any host, network, or account (also known as "cracking" or "hacking"). This includes, but is not limited to, accessing data not intended for the User, logging into a server or account the User is not

expressly authorised to access, or probing the security of other networks without the express authorisation of the owner of such third party network(s);

5.2.5. effecting security breaches or disruptions of communications. Security breaches include, but are not limited to, accessing data of which the customer is not an intended recipient or logging onto a server or account that the customer is not expressly authorised to access. For the purposes of this section "disruption" includes, but is not limited to, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, any otherwise unspecified form of Denial of Service (DoS) attack, or attempts to "crash" a host;

5.2.6. using any program/script/command, or sending messages of any kind, designed to interfere with or adversely affect a User's enjoyment of our network by any means, locally

or by the Internet, including violating the privacy of other Users; and

5.2.7. conducting, for malicious purposes, any form of network monitoring or interception of any data that does not belong to you.

6. Your responsibilities - content/material

General

6.1. You are prohibited from storing, distributing, transmitting or causing to be published any “prohibited material” through your use of the services, including for example your use of the services to send emails, post on online forums and use social media. What constitutes “prohibited material” shall be determined by us (acting in our sole discretion). Prohibited material includes (without limitation):

6.1.1. material that is threatening, harassing, invasive of privacy, discriminatory, defamatory, racist, obscene, indecent, offensive, abusive, harmful or malicious;

6.1.2. material that is in violation of any law or regulation that is enforceable in the United Kingdom;

6.1.3. unsolicited promotional or marketing material;

6.1.4. chain letters or pyramid selling schemes; and

6.1.5. programmes containing viruses, Trojans, malware (malicious software), hoaxes or any tools designed to compromise the security of Internet users, websites and/or systems. However, you may pass samples of malware in a safe manner to appropriate agencies for the purpose of combating its spread.

6.1.6. phishing - material that is designed to acquire information such as usernames, passwords, credit card details or other personal information through masquerading as a trusted source.

6.2. For the avoidance of doubt, the storage upon and/or distribution via our systems and/or services by any User of “pirated” software, or any other materials that are not expressly licensed to the User, will constitute a violation of this AUP.

6.3. At our sole discretion (and without prejudice to any of our other rights pursuant to this AUP and our terms and conditions), we reserve the right to remove any material from any server under our control. In addition to any other action we may take, we reserve the right to notify relevant authorities, regulators and/or other third parties of the use, storage, distribution, transmission, retransmission or publication of prohibited material (and/or any other materials the dealing with or use of which may constitute unlawful conduct by Users).

Email use

6.4. It is your responsibility to back up the contents of your email account. Upon suspension or termination of services the content may be removed and permanently deleted without notice.

6.5. For the purposes of clarity the term ‘unsolicited’ can be defined as ‘not asked for’ or ‘unwanted’.

6.6. Violations of this AUP may result in a large amount of email traffic. If our customers send and/or receive so much email that our resources are affected, we reserve the right to take such action(s) as may be necessary (to be determined at our sole discretion) to protect both the services and our Users, including, but not limited to, deployment of appropriate network security software.

7. Servers

7.1. Users may only run servers to provide Internet Protocol Services (“IPS”) within the limits set out in Sections 4, 5 and 7. Users are deemed wholly responsible for any and all network traffic emanating from relevant servers and are required to ensure that such IPS are secured against abuse by third parties. This includes (but is not limited to) ensuring that servers are running up-to-date security patches and are configured so as to not act as relay servers at any time. “Relay servers” mean servers that can be utilised by another Internet user to relay spam, or any other type of abusive network traffic.

7.2. Failure by Users to secure servers against such abuse may result in immediate suspension or termination of service by us (acting at our sole discretion), with no prior

notice, in order to protect the overall network and the services we provide to other customers.

7.3. In addition to the above, Users' provision of IPS must not adversely affect any other users of our network (including telephony and internet services). Further, Users may not include within and/or distribute via an IPS any content without the express consent of the owner of all relevant rights in such content (including but not limited to intellectual property

rights). We reserve the right to monitor network traffic and to take appropriate action as required, including the right to restrict any IPS. We will not offer any technical support for the provision of IPS.

7.4. We may contact Users at any time to instruct them to stop making server(s) available via their APC services. Upon being notified Users must cease to operate the relevant server(s) with immediate effect.

8. Excessive use

You must use your Service in accordance with any download or capacity limits stated in the specific plan that you subscribe to for the use of that Service. We may limit, suspend or terminate your Internet Service if you unreasonably exceed such limits or 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 of our Network or systems. If APC determines that excessive bandwidth, disk space utilisation or high CPU loads are adversely affecting APC's ability to provide service to other users, APC may take immediate action. APC will attempt to notify the account owner as soon as possible.

9. Reasonable Use

Where a data service is specified as Un-metered or Un-limited use reasonable usage is considered to be within 250 GB per month where this usage is exceeded APC reserves the right

to apply policies in traffic management to limit or restrict the usage above this level or to terminate the Users access to the Services if the limits continue to be exceeded after notification to the User.