

## Supanet Acceptable Use Policy Introduction

This Acceptable Use Policy (or "AUP") applies to all users of services provided by Supanet Limited t/a Supanet Limited ("Supanet"), whether or not they are Supanet customers. BY USING ANY SUPANET SERVICE YOU ACCEPT AND AGREE TO COMPLY WITH THIS AUP. IF YOU DO NOT ACCEPT AND AGREE TO BE BOUND BY THIS AUP YOU SHOULD NOT USE ANY OF SUPANET'S SERVICES.

Supanet may change this AUP from time to time and will inform you when it does so via the Postboard at <http://www.supanet.com/postboard>. You must keep up to date with changes and check the Postboard on a regular basis. Supanet reserves the right to suspend and/or terminate all or any part of any services that it provides to you with immediate effect and to delete any files held on its servers without refunding any fees or paying you compensation if you breach this AUP.

### (A) GENERAL PROVISIONS

#### Responsibility

It is your responsibility to make sure that you comply with all laws applicable to your use of Supanet's services and that you obtain all necessary consents and permissions required for your use of any Supanet service. SUPANET SERVICES ARE PROVIDED FOR USERS IN THE UNITED KINGDOM. THE FACT THAT IT MAY BE POSSIBLE TO ACCESS SUPANET SERVICES FROM OUTSIDE THE UNITED KINGDOM DOES NOT RENDER SUPANET LIABLE FOR OR IN ANY WAY IMPLY THAT SUPANET TAKES RESPONSIBILITY FOR THE COMPLIANCE OF THE SERVICE WITH THE LAWS OF ANY COUNTRY OTHER THAN THOSE IN THE UNITED KINGDOM.

#### Prohibitions

You may not use or permit any other person to use any Supanet service for any of the following: Impersonation/Forgery

For example:

- adding, removing or modifying identifying network header information in an effort to deceive or mislead; and
- attempting to impersonate any person by using forged headers or other identifying information.

#### Hacking/Degradation of Service

For example:

- attempting to gain access to any electronic systems, networks or data without proper consent
- activities which adversely affect the ability of other people or systems to use any Supanet service or the Internet in general (including, but not limited to "denial of service" attacks against other network hosts or individual users); and
- interference with, or overloading, or disruption of use of the Supanet network, network services or network equipment.
- use of port scanning software

#### Harassment and Obscenity

For example:

- threatening, harassing and menacing activity or activity that could be interpreted as such
- activity that is intended to or does cause inconvenience, annoyance or worry;
- use of the services in such a way as to cause irritation, inconvenience or needless anxiety;
- use of the services to transmit expressions of hatred towards racial, ethnic, national, religious or other groups including those pertaining to sexual orientation; and
- obscene, offensive or abusive activity or activity that could be interpreted as such.

#### Illegal/Criminal Use

For example:

- the use of the services for the incitement of any illegal purpose including, without limitation, criminal, fraudulent or defamatory activities; and
- the carrying out of activities that are contrary to UK race, disability or sex discrimination legislation

#### Reselling

For example:

- the provision of bureau services;
- the resale of any Supanet service; and
- the use of any Supanet service to run

server software for use by third parties (Bureau and resale services may only be provided by authorised Supanet resellers. Persons wishing to act as resellers may review details of the Supanet Reseller Programme, available at <http://www.supareseller.com>. Certain Supanet business service packages may permit the running of server software for use by third parties. Please check the relevant terms and conditions or contact Supanet for further details.)

#### Spam

For example:

The sending of unsolicited messages, chain letters and mail bombs, system flooding, bulk mailing and similar activities either directly or by relaying via Supanet's services.

#### Viruses

For example:

The known or reckless transmission of any virus, bug, worm, time bomb or other code intended to damage, destroy, interrupt or limit the functionality of any software, equipment network or data.

#### Facilitating a Violation of this or any other AUP

For example:

Advertising, transmitting, or otherwise making available any software, program, knowledge, product, or service that is designed to violate this AUP or the acceptable use policy of any other Internet service provider (which includes, but is not limited to, the facilitation of the means to spam).

#### Material

You are responsible for all material that you send, transact or publish via a Supanet service. You must make sure that all such material complies with this AUP and that you have all consents and licences necessary for your sending, transmission or publication of such material. You must not use the service to access illegal material. You must use information obtained via any Supanet service for your own personal use and, must not permit any third party, to commercially exploit, copy, distribute or store it without first obtaining the appropriate permissions from the owners of such information. You are also responsible for the selection of material that you access via each Supanet service. Whilst Supanet does not check and will not be responsible for the material that you send, access, transact or publish, if it does become aware of any material in breach of this AUP it reserves the right to remove or block access to such material without penalty or compensation and/or to suspend your access to the whole or any part of the Supanet services. Supanet will cooperate with the police and other law enforcement bodies in relation to the misuse of any Supanet service.

#### Security

It is your responsibility to ensure that your network/computer is configured in a secure manner. You may not, through action or inaction, allow others to use your network/computer for illegal or inappropriate actions or permit your network/computer to be configured to give a third party the capability to use your network/computer in an illegal or inappropriate manner. Supanet does

not guarantee the security or confidentiality of any data transmitted over its network or onward to the Internet. Where security or confidentiality is required, the customer must provide their own end-to-end security mechanism.

#### **Links and Third Party Content**

Supanet does not have control over or accept responsibility or liability for any third party site or any third party content accessible via its services. It is your responsibility to satisfy yourself as to the security, legality and suitability of any third party site and to comply with any terms and conditions applicable to your use of third party sites, content and/or services.

#### **Internet access (dial-up/ADSL)**

Standard dialup accounts are for a single user only although concurrent use of ADSL connections is permitted. Supanet only provides Technical Support for the single user PC USB modem provided as part of the supanet broadband kit. If you chose to provide your own ADSL modem, or set-up your own network via an ADSL router (wireless or otherwise), this will be entirely at your own risk. If you do, Supanet cannot assume responsibility for any hardware or software associated with your network or its compatibility with the Service and will not provide Technical Support or advice for such devices or Configuration. You may not transfer or give out your account details for others to use. You are responsible for all traffic that is sent from your connection. It is therefore your responsibility to ensure that all software on your side of the connection is virus-free and up-to-date with all relevant security patches. In particular, server software running on public-facing ports, such as mail servers and proxy servers, must not be remotely exploitable – the use such software is only permitted with designated supanet business services. If Supanet finds malicious traffic or traffic that breaches the terms of this AUP emanating from your connection, we have an obligation to our other customers and peering networks to take urgent measures to block that traffic. In many cases, this can be achieved by selective port blocking, but in other cases, this will involve connecting and suspending the account until the issue has been resolved. We understand that in many cases, you may not be responsible for or aware of the problem, we will work with you to resolve the issue as efficiently as possible to restore normal service.

#### **Sharing Internet Access on a Private Network and Running Personal SMTP Mail Servers**

You must use the provided smart hosts to send email and not operate your own SMTP mail servers for the purposes of sending e-mail. The only permitted exclusions are customers who subscribe to the designated Supanet business services. Business customers operating mail servers must ensure that they are not open relays – the use of such servers is only permitted on designated Supanet business services. Some methods of sharing Internet access or applications expose our external Internet connection to other Internet users, and enable them to send unsolicited bulk e-mails via your computer (known as SPAM). In order to try and protect your computer from possible intrusion, Supanet has put a block on inbound port 25 communications on all of its narrowband services and broadband services (except designated Supanet business broadband services), and outbound traffic destined for port 25 (with the exception of the provided smart hosts). This will prevent the use of Internet connection sharing software that exposes your Internet session to the rest of the Internet from being used by other Internet users for sending unsolicited e-mails. This also means that if you run your own e-mail server, it will not be able to send or relay e-mails on behalf of other Internet users. This implementation will not affect your own ability to send and receive e-mail through the appropriate mail server for your service product. It will also prevent open relays and proxies from being exploited.

#### **e-mail**

Customers may not forge the sender address of any messages to appear to be from someone they are not. Customers may not use our services to send unsolicited bulk e-mail ("UBE", also known as "Spam"). Supanet will block the

mail services of any customer found to be sending such mail. Sending large volumes of unsolicited e-mail of whatever nature is prohibited. Using a supanet email or Web site address to collect responses from unsolicited commercial e-mail is prohibited. Activities that have the effect of facilitating unsolicited e-mail, or large volumes of unsolicited e-mail, are prohibited. Anonymous bulk e-mailings are not permitted and we will terminate the accounts of any customers who attempt to do this. This may happen without notice. If we receive any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, we may take further action to stop this happening again. This may involve the termination of any accounts the sender has and may occur without notice. In the event that we are alerted to anyone sending bulk e-mails, we will generally prevent further e-mails being sent and attempt to make contact with the sender to discuss appropriate actions.

#### **Customer Web Space**

You are responsible for the content of your Customer Web Space, including obtaining the legal permission for any works they include and ensuring that the contents of these pages do not violate UK law. Supanet reserves the right, without notice or explanation, to remove material, which does not comply with company policy, such as material of an adult nature or pirated software. Supanet reserve the right to suspend any or all of the Customer Web Space service at any time, without prior notice, explanation, or recompense. Customers will be held solely responsible for any defamatory, confidential, secret or other proprietary material made available via your Customer Web Space site. Supanet reserve the right to suspend any sites containing such material. If the account is suspended for any reason, such as non-payment, access to the Customer Web Space, both for viewing and uploading, may also be suspended. Upon closure of an account, the relevant Customer Web Space will be deleted. P2P (Peerto- Peer Software) Whilst Supanet does not prevent the legitimate use of P2P software, you may not use Supanet's services to transfer material of an illegal or immoral nature. You must own any material that you make publicly available or appropriate permissions obtained from the owner(s). Likewise, any material obtained by you must only be obtained with the consent of the original publisher. Supanet will cooperate with any agency wishing to assert their rights in these matters and reserves the right to withdraw the whole or any part of its service under such circumstances.

#### **Usenet (News)**

When using newsgroups, customers must comply with the globally accepted Usenet acceptable use policy. A good place to refer to the policy is <http://www.usenet.org>. Messaging services Messaging services covers any transaction involving software that transmits messages from one user to another, such as e-mail, IRC, instant messaging (IM) or Usenet. Customers may not abuse, racially harass or make physical threats against, another person via any type of messaging service, or any other electronic media/service we provide. Customers must abide by the policies of any messaging or IRC networks they use. We will co-operate with the administrators of such networks to identify abusive users and restrict their access. Customers are reminded that harassment, threatening or slanderous behavior is prosecutable under UK law. Users may not forge the sender address of any messages to appear to be from someone they are not.

#### **Children's Chatroom**

Supanet offers a monitored chatroom for children. The hours of use are detailed on the Supanet portal and may change from time to time. A Supanet staff member is present during the time the children's chatroom is open and has the right to suspend users of the chatroom for breaking the AUP or for making, in Supanet's discretion, improper use of the children's chatroom. Continual or more serious violations could lead to a more lengthy suspension, up to and including suspension or cancellation of the relevant Supanet account. Other than for the children's chatroom, Supanet does not have full-time monitors for its message boards, chat rooms or other elements of its

Services. Staff members may monitor and view these services on an irregular basis and, where users are deemed to be in breach of the AUP take whatever action necessary either with or without warning to stop such breach and/or prevent further breaches.

**Excessive use of flat rate narrowband dial-up services**

Flat rate dial-up services (supahighway and supahighway platinum) are not designed to be always-on services. The access we give you is shared with other customers. This means customers with excessive usage patterns degrade the service to other bona-fide customers. If we believe you to be using the service excessively we may suspend your service without notice, or in extreme cases, terminate your account. As a guide, for supahighway customers daily average usage in excess of 3 hours per day would be considered excessive and 6 hours per day for supahighway platinum customers.

**Technical Support**

Technical Support exists for the benefit of Supanet customers, providing support for questions relating directly to our services. When contacting technical support, please ensure that you have all relevant details to hand, including details of any specific error messages encountered. Please help us to help you.

**Reporting**

Users of Supanet services may report suspected breaches of this AUP by sending an email to Supanet's Network Abuse Team via the link at [abuse@supanet.com](mailto:abuse@supanet.com).