

Supanet Acceptable Use Policy for Business Customers

Introduction

This Acceptable Use Policy (or "AUP") applies to all business users of services provided by 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 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.

The Customer shall be responsible for ensuring that all users of the service shall be aware of this Policy. The Customer shall further be responsible for ensuring that this Policy is complied with at all times by any user allowed to access Supanet services through the Customer's account.

All Supanet Customers are required to accept and read e-mail addressed to `postmaster@<yourdomainname>` and `abuse@<yourdomainname>`. Mail addressed to `postmaster` and `abuse` must not be "bounced" or ignored.

You must accept, read and act upon all mail received from postmaster@supanet.net.uk, and abuse@supanet.net.uk, in a timely fashion. Ignoring or bouncing of said email will be considered a breach of this Policy.

The Client acknowledges that Supanet has a responsibility to and may be required by current or future law or regulation, including but not limited to the Regulatory of Investigatory Powers Act 2000, to access, monitor, store, take copies of, or otherwise deal with the Customer's data stored on or transmitted by the Service. Without limitation, the Customer expressly authorises Supanet to use personal data and other account information in connection with any such investigation, including disclosure to any third

party authority that is considered to possess a legitimate interest in any such investigation or its outcome.

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

The integrity and security of the Supanet network is necessarily of prime importance and any action that adversely effects, or threatens to adversely effect, the operation of the network is strictly prohibited under this Policy. Insofar as the Supanet network is linked with any other Network that forms the Internet as a whole, this shall include any such action against any other network.

While Supanet places no obligation upon itself to monitor any traffic, website, customer servers or information transmitted or stored by customer-owned equipment, Supanet will investigate any complaints received concerning use of the network in contravention of this Policy.

This Policy prohibits the customer and by 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.
- attempting to breach any security, host, network, user authentication, account or limits Supanet have put in place.
- execute any form of network monitoring, which will intercept data not intended for the client.
- running of any electronic system known to be insecure that connects directly or in-directly to the Supanet network.
- 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.
- use of any applications that may disrupt the stable operation of the Supanet network.
- Introduction of any malicious programs into the Supanet network or Supanet servers (e.g. viruses, worms, Trojan horses, etc.).

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

Spam

Any mail content considered SPAM, sent directly or indirectly by relaying via Supanet's services.

This includes but is not limited to:

- Sending of, or collecting responses from, bulk email
- Indirect or direct mails with the purpose of, collecting mail address
- Chain Letters and pyramid-selling schemes
- Unsolicited Commercial E-mail (UCE)
- Unsolicited Bulk Mail

- Forged headers and or / Address
- E-mail Bombing

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.

While Supanet does not check and will not be responsible for the material that you send, access, transact or publish, if it does become aware that any of the material may be 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 service. Supanet will co-operate 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)

Supanet only provides Technical Support for the single user PC USB modem or wireless router provided as part of the Supanet broadband kit. If you chose to provide your own ADSL modem or router, 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 beaches the terms of this AUP originating 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 disconnecting 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 e-mail 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 mail servers is only permitted on designated Supanet business services.

Such Business customers must agree to the following:

- Any mail service set up by Customers must be to RFC standards and all network facing mail servers must have both forward and reverse DNS lookups set.
- Network-facing open-relay mail servers are strictly prohibited.

- Disclosure to Supanet of all mail servers IP's which may send mail across the Supanet Network or refer in mails back to a Supanet provisioned IP.
- Mail to Supanet from Customer email services controlled by the said Customer is not guaranteed.
- Supanet holds the right to block at any time any email service from the Customer to any other Supanet Customer.

Some methods of sharing Internet access or applications expose your 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 systems 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 email server, it will not be able to send or relay emails 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 or product. It will also prevent open relays and proxies from being exploited.

Email

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 Email (“UBE”, also known as 'Spam'). Supanet will block the email services of any customer found to be sending such email.

Sending large volumes of unsolicited email of whatever nature is prohibited.

Using a Supanet email or website address to collect responses from unsolicited commercial email is prohibited.

Activities that have the effect of facilitating unsolicited e-mail, or large volumes of unsolicited email, are prohibited.

Anonymous bulk emailings are not permitted and we will terminate the accounts of any Customers who attempt to do this. This may happen without notice.

You must not send via email any item which is illegal to send or possess. This includes material which is prohibited under various Acts of Parliament dealing with material over a public telecommunications network, notably the telephone system. This includes but is not limited to:

- Content that contains or contains links to nudity, pornography, adult content, sex, extreme violence, or foul language

- Content that condones, promotes, contains, or links to warez, cracks, hacks, their associated utilities, or other piracy-related information, whether for educational purposes or not.
- Content that is racist, or otherwise extremely offensive to others, including content which aggravates, harasses, threatens, defames, or abuses others.
- Sites that exploit images of children under 18 year of age, links to said sites or information in regards to access or identification for use of said sites.
- Content that posts or discloses personnel identification, information or private information of individuals under the age of 13 or in connection with materials directed toward individuals under the age of 13 without verifiable parental consent.
- Content that provides, sells, or offers to sell the following: controlled substances: illegal drugs and drug contraband; alcohol; weapons; information used to break copyright or trademark violations; to destroy others property or harm any people or animals.

If we receive any complaints from recipients or other third parties, or if 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 emails, we will generally prevent further emails 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 reserves 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 their Customer webspace. Supanet reserves 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 (Peer-to-Peer Software)

While 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 obtain appropriate permissions 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 email, IRC, instant messaging (IM), SMS 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 cooperate with the administrators of such networks to identify abusive users and restrict their access. Customers are reminded that harassment, threatening or slanderous behaviour is prosecutable under UK law.

Users may not forge the sender address of any messages to appear to be from someone they are not.

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.

Supanet has in place a procedure for handling your complaints about material stored and/or accessed via our services. If you wish to make such complaint, please ensure that you make your complaint via email to abuse@supanet.net.uk or by fore agreed channels.

If you do not use the agreed facility, Supanet cannot guarantee that your complaint will be dealt with promptly.

Copyright © Supanet Ltd 2005. All rights reserved.