ACCEPTABLE USE POLICY

This Acceptable Use Policy sets out the terms between you and us under which you may use our Internet related services ("**the Services**") and/or access our website at www.amatisnetworks.com ("**our site"**). This Acceptable Use Policy applies to all users of our Services and to all users of, and visitors to, our site.

Your use of our Services and/or our site means that you accept, and agree to abide by, all the policies in this Acceptable Use Policy, which supplement our standard Terms and Conditions.

INTRODUCTION

For the Internet to operate in a manner that satisfies the majority of its users, all users need to observe some rules and etiquette governing their use of it. These requirements are contained within this document or the amatis terms and conditions of business. Customers must ensure that they know what these requirements are and how they are affected by them.
To enable customers to have a better understanding of what is and is not acceptable when using the internet Amatis has developed this Acceptable Usage Policy (AUP) relating to internet services. Complying with this AUP, which is a contractual requirement, will help you benefit from safer use of the Internet and minimize the risk of suffering online abuse.
The AUP is based on current best internet industry practice and draws on the collective experience of users and service providers across the internet community. We may change this AUP from time to time.

AVOIDING ABUSE WHILE CONNECTED TO THE INTERNET

Common sense
The majority of customers will be using commercial software to connect to and navigate the Internet. This software controls the technical aspects of the connection but there are also some simple common sense checks, which all customers can implement.

Legal compliance
The Internet is a global medium and is regulated by the laws of many different countries. Material, which is illegal in this country, may be legal in another, and vice versa. As a user in the UK, for example, you should not access sites carrying child pornography or incitement to violence. These are just two examples of unlawful material and there are many others. When you visit a website, a copy of the visited pages is stored on your PC in the web browsers' cache files. Storage of illegal material in this way may well constitute a criminal offence. If you are in any doubt, we recommend you to take independent legal advice.
To connect to many online services, you will use a telephone (PSTN) line, ISDN line or ADSL. While connected to the internet, you must comply with legal requirements concerning telephone network use and misuse. Set out below is an extract from the Telecommunications Act illustrating that network misuse is a serious criminal offence, which can lead to fines and/or imprisonment.
"Improper use of public telecommunication System"
A person who;
• Sends by means of a public communication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
• Sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system, shall be guilty of an offence and liable on summary conviction to imprisonment for a term not exceeding six months or a fine.

Practical steps to take
Taking the following steps should help you to protect yourself from becoming a victim of abuse while connected to the Internet.
Ensure that you are running a good quality virus detection application. The majority of these applications have the ability to detect hackers as well as viruses. Hackers are people who try to access your computer to either cause mischief or find your passwords and usernames. You should be aware that some hackers have the ability to seriously damage your computer system or an entire company network.
If you keep sensitive information on your computer, it is worth using encryption software to protect it. While connected, do not publicise your IP address. This is especially important if you are using applications such as CHAT, IRC (internet relay chat) or video conferencing using a directory service.
Never install software of unknown origin. Most computer viruses and Trojans are installed unknowingly by clicking on links in email or while installing shareware or freeware applications.

Sharing log-on details
Never share log-on details.

Port scanning
Amatis prohibits customer or third party use of port scanning software on its network.

Sharing Internet access on a private network and running personal SMTP mail servers
Some methods of sharing Internet access or applications expose your external Internet connection to other Internet users, and enable them to send unsolicited bulk emails via your computer (known as spam).
As Amatis do not block any ports it is vital that you configure your network securely. You are fully responsible for security in your own network and failure to secure it properly will result in your disconnection from the service.

GENERAL

Prohibited Uses
You may use our Services and/or our site only for lawful purposes. You may not use our Services and/or our site:

- In any way that breaches any applicable local, national or international law or regulation (including the Computer Misuse Act 1990 and Data Protection Act 1998).
- In any way that is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect.
- For the purpose of harming or attempting to harm minors in any way.
- To send, knowingly receive, upload, download, use or re-use any material that does not comply with our content standards.
- To transmit, or procure the sending of, any unsolicited or unauthorised advertising or promotional material or any other form of similar solicitation (spam).
- To forge Internet addresses or other fields in IP packets;
- To knowingly transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.
- In any way that threatens the integrity and/or security of any network or computer system.
- In a way that allows access to our network management equipment or that of third parties.
- In any way that attempts to avoid incurring charges or to otherwise avoid being required to pay for such usage.
- In any way that degrades or interferes with other users' use of any of our services (or may do so).
- In a way that breaches third party rights of any kind (including intellectual property rights such as copyright or trade marks, right to privacy)
- In any way that breaches a third party non-disclosure agreement or obligation.
- To transmit or display any material which affects the national security of any country or for terrorist activities.
- In any way that contravenes generally accepted standards of Internet or other networks conduct and usage, including but not limited to denial of service attacks, web page defacement, port or network scanning and unauthorised access to systems.

You also agree:

- Not to reproduce, duplicate, copy or re-sell any part of site in contravention of the provisions of our terms of website use.
- Not to access without authority, interfere with, damage or disrupt:
    - any part of our site;
    - any equipment or network on which our site is stored;
    - any software used in the provision of our site; or
    - any equipment or network or software owned or used by any third party.
- Not to allow any unauthorised use of your password or to use the Services and/or our site to guess passwords or access to other systems or networks.
- You are responsible for the activities of your end-users and ensuring compliance by them of this policy

- To maintain email addresses (preferably as an email alias) of the forms postmaster@customer.domain and abuse@customer.domain for receiving complaints of network abuse activities, as suggested by Internet Official Protocol Standard RFC 2142. Typically, these email addresses will forward emails to the real user accounts of the responsible persons for treating the network misuse complaints.
- All complaints related to network misuse, including email abuse (SPAM) are to be sent to abuse@amatisnetworks.com.

Illegal material
You should not send email which contains any information which is illegal to send or possess in the United Kingdom such as copyright, trade secrets, or pornography. Additionally you should be aware that the transit of material into, or through, other countries may be required to comply with the law in that country. In some cases this may include the transmission of encrypted messages.

EMAIL SERVICES

Introduction
Exchanging emails with others generally involves using common sense regarding the content material and being polite and courteous. The vast majority of business users understand what is appropriate when sending or receiving emails. Regrettably, there are occasions when individuals or groups of people send emails or perform online activities, which are considered to be unacceptable by the Internet community. This is described by the generic term of 'abuse'. This email AUP is based on current 'best internet industry practice' and draws on the collective experience of email users and service providers across the Internet community.

Abusive emails
It is not always obvious whether an activity is innocent, inadvertent or intentional, but email users should be aware that what is unacceptable (and possibly illegal) offline (oral or written) applies equally online. As with telephone calls, you must not send any emails which cause annoyance, inconvenience or needless anxiety. You should not send false messages likely to cause distress or any other material which is distressing, grossly offensive, indecent, obscene, menacing or in any other way unlawful. Particular care should be taken to avoid any material which is offensive or discriminatory to people on grounds of gender, race, colour, disability, religion or belief, age or other similar category.

Spam (unsolicited bulk emails)
You must not use the Amatis email system to send unsolicited emails, bulk or otherwise. The sending of such emails is an abuse of the service and constitutes a breach of the relevant terms and conditions.

Chain letters, pyramid selling, and multi-level marketing schemes
These are similar to the paper and mail-based letters. Typical abuse of this sort includes the 'Make Money Quick' scams. These not only waste resources, but they are illegal in certain countries and may render the poster liable to prosecution.

Unrequested binary messages
The majority of email users are not able to select messages based on size and therefore such emails result in a significant waste of resources for the users concerned.

Forged headers and/or addresses
If email is sent which implies that the sender can be contacted at an email, postal, or fax address which is not under the direct control of the sender, this is considered to be a grave abuse of the email system.

Mail bombing
Mail bombing is the sending of multiple emails, or one/multiple large email, with the sole intent of annoying and/or seeking revenge on a fellow Internet user. It is waste of shared Internet resources, as well as serving no value to the recipient. Due to the time taken to download it, sending long emails to sites without prior agreement can amount to denial of service, or access to email at the receiving site. Note that if binary attachments are added to mail this may increase the size considerably. If prior arrangement has not been made, the mail will be extremely unwelcome.

Denial of service attacks
Denial of service is any activity which prevents a host on the Internet making full and effective use of their facilities. This includes, but is not limited to:

- Mail bombing an address in such a way to make their Internet access impossible, difficult, or costly.
- Opening an unnecessarily large number of mail connections to the same mail host or making a connection to a SMTP relay (sometimes known as a smarthost) without authorisation or permission.
- Sending email designed to damage the target system when executed or opened; for example, sending malicious programs or viruses attached to an email.
- Sending email which is designed to cause confusion, consternation, fear, uncertainty, or doubt, such as fake virus warnings.

Mailing list subscriptions
You must never subscribe anyone other than yourself to a mailing list. You must be aware of how to correctly remove yourself from a mailing list in the event that you alter your email address or terminate your service with us.

Setting up your mail server (open relay)
If you choose to run an SMTP email server on a private network on your premises you must ensure that it is configured correctly, so as to only accept mail from your private domain.

Internet connection sharing
If you share the resources of your internet connection over a private network on your premises, you must make sure that your network is secure, and that any internet connection sharing software that you are using does not permit access from outside of your network. This is especially important if running an open proxy server. This is because an open proxy server will allow other users of the internet to exploit your internet connection, and use it as if it were their own. For example, an external user could access your local network or send unsolicited emails that would appear to come from you.

HOSTING & CO-LOCATION SERVICES

Introduction
The following AUP contains rules governing the use by customers of all Amatis hosting services. It is based on current 'best internet industry practice' and draws on the collective experience of webspace users, service providers and the owners and administrators of computer networks.
Amatis cannot and does not proactively monitor content on its customers' websites and therefore cannot and does not guarantee that all such websites are free of illegal material or other content considered unacceptable (abusive) by the internet community.

Illegal activities
Customers must not have illegal material on their website or link to content that is illegal. You should be aware that as the Internet is a global network, some activities/material, which may be legal in the UK, may be illegal elsewhere in the world and vice versa, and you could risk being prosecuted in another country. Customers must not incite disorder or publish any material which would amount to instructions concerning illegal activities. Customers must not publish content, or link to content in which you do not own the rights, without the permission of the owner of the relevant rights.

Unacceptable behaviour
It is not always obvious whether an activity is innocent, inadvertent or intentional, but generally webspace users should be aware that what is unacceptable (and possibly illegal) offline (oral or written), applies equally online.
Avoid content that may offend. If you have any doubt about the suitability of your content to others, in particular to children, you must give a warning page before reaching the content. Particular care should be taken to avoid any material which is offensive or discriminatory to people on grounds of gender, race, colour, disability, religion or belief, age or other similar category.
Amatis does not make any logs or details of who visited your site available.
• You must ensure that your index.htm or default.htm file (the first to be viewed on a site) does not contain any material liable to offend. A clearly readable warning page must be displayed before any adult material is displayed.
• You must not use your webspace to cause annoyance, inconvenience, offence or needless anxiety.
• You must not publicise the personal details of others without their consent.
• You must not use your website to advertise, distribute (or link to another webpage containing) virus creation software, email spamming software or port scanning software.
• Your homepage's site may not be used to distribute or advertise any of the following:
• Software for sending spam (excessive news postings, bulk emails etc.).
• Software for port scanning, virus creation, hacking or any other illegal or antisocial activity.
• Lists of email addresses except where all the addressees have given their explicit permission.
• Any collection of personal data other than in accordance with all applicable data protection legislation.
• Links to websites hosting illegal content, including adult material
• Content designed to offend or cause needless anxiety to others.
• You must not advertise your homepages or websites, or cause another person to advertise it, by techniques that would be classified as abuse, e.g. bulk emailing and excessive news posting.

Security
You must not share passwords. Your passwords are your responsibility, and must not be disclosed to any third party. This is also important for your own protection.

USENET SERVICES

Our customers are asked to remain courteous to others when accessing USENET newsgroups and not to abuse the service provided by us.

The following non-exclusive list of conduct would be considered as an abuse of the news service:

Chain letters, pyramid selling, and multi-level marketing schemes
These are similar to the paper and mail based letters. Typical abuse of this sort includes the 'Make Money Quick' scams. These not only waste resources, but they are illegal in certain countries and may render the poster liable to prosecution.

Commercial articles
The majority of newsgroups are areas of interest and are not of a commercial nature. Readers of such newsgroups will object to commercial traffic (such as the advertisement of products and/or services for which payment is required). Please check with the FAQ of the newsgroup concerned before posting articles of a commercial nature.

Binary postings to non-binary groups
Outside of the alt.binaries.*, alt.pictures.*, and comp.binaries.*, newsgroup hierarchies, the posting of encoded binary data is considered inappropriate. The majority of USENET news sites and readers are not able to select articles based on size and therefore such postings result in a significant waste of resources for the users concerned. In some cases, posting of this sort could be considered to be a denial of service attack on multiple recipients.

Excessive multi-posting (SPAM) and excessive cross-posting (velveeta)
This occurs when the same (or similar) article is posted, or cross-posted, to a large number of unrelated newsgroups. A more complete description of these (and other related) terms, can be found in the FAQ regularly posted to news.admin.net-abuse.announce newsgroup.

Forged headers and/or addresses
If a posting is made which implies that the sender can be contacted at an email, postal, or fax address which is not under the direct control of the poster, this is considered to be a grave abuse of the USENET news service.

SUSPENSION AND TERMINATION

We will determine, at our sole discretion, whether there has been a breach of this Acceptable Use Policy through your use of our Services and/or our site. When a breach of this policy has occurred, we may take such action as we deem appropriate.

Failure to comply with this Acceptable Use Policy constitutes a material breach of the General Terms and Conditions and the terms of use upon which you are permitted to use our Services and/or our site, and may result in our taking all or any of the following actions:

- Immediate, temporary or permanent withdrawal of the Services and/or your right to use our site without notice to you.
- Immediate, temporary or permanent removal of any posting or material uploaded by you to our site.
- Issue of a warning to you.
- Legal proceedings against you for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach.
- Further legal action against you.
- Disclosure of such information to law enforcement authorities as we reasonably feel is necessary.
- If we receive a court order requesting us to reveal your identity to someone complaining that you have used our Services abusively, we will do so.

We exclude liability for actions taken in response to breaches of this Acceptable Use Policy. The responses described in this policy are not limited, and we may take any other action we reasonably deem appropriate.

CHANGES TO THE ACCEPTABLE USE POLICY

We may revise this Acceptable Use Policy at any time by amending this policy. You are expected to check this policy from time to time to take notice of any changes we make, as they are legally binding on you. Some of the provisions contained in this Acceptable Use Policy may also be superseded by provisions or notices published elsewhere on our site.