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 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.