Acceptable usage

1. Introduction

For the Internet to operate in a manner that satisfies the majority of its users, we ask all end-users to observe some rules and etiquette governing their use of it. HighNet's Partners must ensure that they know what these requirements are and how they are affected by them. It is the Partners' responsibility to ensure that this Acceptable Use Policy (AUP) is adhered to by them and their end users. HighNet's 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 the AUP from time to time. To make the most of the guidance contained in the AUP, please keep up to date with changes and look at them on a regular basis. Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your services may be suspended or terminated.

2. A Guide to avoiding abuse while connected to the Internet

Software updates

The majority of HighNet's online customers will be using commercial software to connect to and navigate the Internet. End-users should ensure that the software in use is up to date. We recommend that Microsoft For historic updates across all browsers, please visit the software vendor's website.

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 this country, for example, you should not access sites carrying child pornography, hard-core pornography or incitement to violence. These are just three 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 browser's cache files. Storage of illegal material in this way may well constitute a criminal offence. If you or your end-users are in any doubt, we recommend you take independent legal advice. To connect to any of HighNet's online services, end-users will use any of the access types offered by HighNet as noted within the product literature on the HighNet website. In most cases this will be via DSL or Ethernet. While connected to the Internet, end users must comply with legal requirements concerning telephone network misuse. Set out below is an extract from the Telecommunications Act (2003). Network misuse is a serious criminal offence which can lead to fines and/or imprisonment.

Telecommunications Act (2003)

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; or – 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, or both.

Avoiding abuse while connected to the Internet

Taking the following steps should help users to protect themselves 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 hacker attempts as well as viruses. Hackers are people who try to hack into 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 and any other associated network. If you keep sensitive information on your computer, we recommend using encryption software to protect it. While connected, do not publicise your IP address. This is the unique ID that your ISP allocates to you while you are connected to the Internet. This is especially important if you are using applications such as CHAT, Internet Relay Chat (IRC) or video conferencing using a directory service. The number of untrusted applications will continue to grow exponentially. Be careful what you install on PCs, tablets, laptops and mobile phones. Before installing software of unknown origin, ask yourself whether you trust the writer/source. Most computer viruses and Trojans are installed unknowingly while installing shareware or freeware applications that are supposedly designed to make your life easier. If in doubt, don't do it.

Sharing logon details

HighNet prohibits users from sharing details.

Port scanning

HighNet prohibits the use of port scanning software on any of our services.

Sharing Internet access on a Private Network and personal SMTP mail server 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 HighNet do not block any ports it is vital that end-users configure their networks securely, end-users should be fully responsible for security in their own network and failure to secure it properly will result in a disconnection from HighNet services.

Copyright Infringement

All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing. Downloading of film or other content which does not have appropriate permissions from the copyright owner is illegal. HighNet will co-operate with all agencies attempting to assert their rights in these matters.

3. Internet access – Acceptable Use Policy (AUP)

Introduction

HighNet's relationships with its Partners, other networks, and ultimately its connectivity to the rest of the Internet, require its Partners to behave responsibly. Accordingly, HighNet cannot permit irresponsible behaviour by its Partners and end-users, which could damage these relationships, HighNet's network or the use of the Internet by others. The HighNet network and associated products and services are designed to carry business data, and are designed to give lower priority to non-business traffic. We manage the available bandwidth carefully, and if a group of users use a disproportionately large amount of bandwidth (i.e. transfer a disproportionately large amount of data) then this will:

a. Impact the available bandwidth for the rest of the users.
b. Potentially degrade the service.
c. Drive up the cost of delivering the service to HighNet partners.

The majority of end users that will be affected by this policy are those using file sharing software such as peer-to-peer and binary newsgroups (USENET). Such software (for residential applications) is typically used to send and receive large files (such as music, tv and videos) and can be left running throughout the day – this uses a massive amount of bandwidth and in some cases is illegal. Customers using their broadband service for sending e-mails, browsing web-pages and other typical business applications will not be affected. In order to maintain a business grade service, residential applications such as iPlayer should not be used.

Allowances – 'Absolute' Products (DSL and Ethernet)

HighNet Absolute ADSL Broadband products have a data transfer allowance of 150GB per month. VDSL (Fibre to the Cabinet) products on BT tails have a data transfer allowance of 500GB per month, and on Talk Talk Business tails have unlimited usage. All Absolute Ethernet products provide unlimited usage.

Restrictions and additional charges for overuse

End-users will be warned that they are exceeding their allowance and be given a month to moderate their use before being charged at £1.00 per GB. End-users of Absolute Broadband products who exceed their monthly allowance may be subjected to restrictions to limit their data transfer in peak periods. HighNet will advise the end-user and partner if usage has been exceeded and if the end-user is unable to moderate their use, particularly in peak hours, their data throughput may be limited within the HighNet network.

4. What affect will restricting a customer's service have?

The customer will experience a slowing down of their service. The extent of this degradation will depend on what the customer is doing and how many users are connected to the service. If a small number of users are web-browsing and reading emails, they will notice a slowing of the service. If on the other hand they are using Peer-to-Peer or file sharing software, or they are downloading files from the internet or an external server, they will experience a significantly and possibly slower service.

What can an end-user do with 150 GB of data transfer?
a. Send and receive a total of 1,500,000 emails.
b. View over 1,000,000 standard web pages.
c. Transfer 150,000 1MB files.
d. Make 1,200,000 minutes of IP Voice calls.