AdEPT

AdEPT Acceptable Usage Policy For Broadband Users

Contents

1. Introduction
2. Internet Access – Acceptable Use Policy
3. Email – Acceptable Use Policy
4. Newsgroups – Acceptable Use Policy
5. Webspace – Acceptable Use Policy
6. Chat, Instant Messaging and Video Messaging Services – Acceptable Usage Policy
7. Glossary

1. Introduction

For the Internet to operate in a manner that satisfies the majority of its users, all users need to observe some rules and behaviours governing their use of it. These requirements are usually contained or referred to in the relevant terms and conditions governing the particular Internet service as well as the law.

To enable its customers to have a better understanding of what is and is not acceptable when using the Internet, and to help you get the best out of the Internet, AdEPT has developed a number of Acceptable Usage Policies. These policies should help you benefit from safer surfing and minimise the risk of suffering "online abuse".

We have also included some general advice on how to protect you and your computer to each of these policies which we encourage you to follow.

Illegal and inappropriate activities

As an Internet user, whilst connected to the Internet via AdEPT you must comply with the relevant laws that apply in the UK. You should also be mindful of the fact that the Internet is a global medium and is regulated by the laws of many different countries. Material which is legal in this country may be illegal in another and vice versa.

These are some of the things that you must not do whilst connected to the Internet:

You must not, by using the service, download, possess or transmit in any way, illegal material (for example indecent images of children).

You must not send, publish, distribute, circulate or otherwise propagate any material that may be deemed to be grossly offensive or of an indecent, obscene nature or menacing in character.

You must not send, with the intention of causing annoyance, inconvenience or needless anxiety a message that you know to be false, or to cause such a message to be sent or to persistently make use of our service for that purpose.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the Internet.

You must not, without authorisation intentionally impair or attempt to impair the operation of any computer, prevent or hinder access to any program or data held in any computer or to impair the operation of any such program or the reliability of any such data (this could include deleting files, changing the desktop settings introducing viruses etc.).

You must not infringe the rights of others, including the right of privacy and copyright (an example would be sharing without permission of the copyright owner protected material such as a music or video file).

Many of these activities could result in legal action, a fine or a term of imprisonment or both.

If you are in any doubt as to the legality of anything, take independent legal advice before proceeding.

AdEPT's obligations

AdEPT is obliged under the Regulation of Investigatory Powers Act to disclose information to Law Enforcement Agencies and Public Authorities that are legally entitled to obtain such information. Similarly AdEPT must comply with court orders to disclose information. In serious instances of abuse we may also notify the police or relevant law enforcement agency.

AdEPT cannot and does not monitor content of its' customers webspace or content of chat rooms, instant messaging, email, newsgroup or indeed of any communications and therefore AdEPT cannot and does not guarantee that all of these are free of illegal material or other content considered unacceptable by others including the Internet community.

Changes to the Acceptable Use Policies

We may change the Acceptable Usage Policies' from time to time and will inform you on this website when we do so. To make the most of the guidance contained in the AUPs, please keep up to date with changes and look at them on a regular basis. We hope you will find them useful and informative.

Breaches of Acceptable Use Policies

Reports of breaches of these acceptable use policies by AdEPT customers can be sent to customerservice@adept.co.uk

AdEPT may operate systems to ensure compliance with these acceptable use policies, including without limitation network scanning and testing of open servers and mail relays.

2. Internet Access – Acceptable Use Policy (AUP)

While connected to the Internet via AdEPT you must comply with the law.

You must not send email which has forged header information, nor should you attempt to impersonate any other individual or organisation.

You must not run "**port scanning**" software which accesses remote machines or networks, except with the explicit prior permission of the administrator or owner of such remote machines or networks. This includes using applications capable of scanning the ports of other Internet users.

If you intend to run a port scanning application, you must provide AdEPT with a copy of the written consent received from the target of the scan authorising the activity. This must be supplied to AdEPT prior to the application being run.

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.

You must not participate in the sending of unsolicited email, bulk or otherwise or in any form of email or newsgroups "abuse". This applies to material which originates on your system as well as third party material which passes through your system with or without your knowledge.

Your account should only be used for one direct connection to the Internet at a time. You are responsible for the security of your username or password and you should not disclose these to anyone.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

The majority of AdEPT's online customers will be using commercial software to connect to and navigate the Internet. This software implements the technical aspects of the connection but there are also some simple common sense measures that customers can implement.

You should keep your operating system (for example Windows XP) up to date with the latest updates. Ideally you should enable the automatic tool for this purpose (for example Windows automatic updates) provided by your operating system’s manufacturer.

Install and keep up to date anti-virus, firewall and anti-spyware software:

Viruses often rely on being introduced to a computer through opportunism and simple user mistakes. They can also be introduced if you visit a corrupted or malicious website, via Internet attacks, where they are known as "worms" and even via the macros in some documents.

Once it infects a computer the damage a virus can do ranges from simply changing your Internet home page to deleting entire file systems on your computer or making it slow, perhaps even unusable and can even lead to the compromise of your identity details which can in turn lead to fraudulent use of your personal information.

Installing anti virus software on your computer will help by scanning your incoming emails for attachments infected with known viruses and scanning attachments for infection when you open them; it also makes checks of your computer for infected files.

With anti-virus software as with any other security software for your computer you should ensure that you purchase from a reputable vendor and that having made a purchase that you keep it up to date.

A firewall protects your computer from being accessed without your permission. When you are connected to the Internet you are on a vast public network, because of this hackers can try and gain access to your computer for such purposes as stealing your personal files and information or even to use your computer as a hidden means of attacking other computers on the Internet. A firewall monitors all incoming and outgoing data traffic to and from your computer and can block unauthorised attempts to access your computer, safeguarding your computer and its data.

Spyware programs can monitor your Web browsing habits and also make changes to your computer settings that you do not want, allowing strangers to see what you're doing on the Internet, pop up unwanted advertisements on your computer and even block access to certain websites. At the extreme end of the scale there are spywares like viruses that can capture personal information.

Increasingly the distinctions between what viruses, worms, spy ware and firewall breaches can do to your computer are blurred and it is important that you are aware of and protect your computer against all of these threats.

Only download files from sources that you trust. This applies equally to files such as music and movies as it does to software downloads. You should always ask yourself whether you trust the writer and or the source of the file. Many computer viruses and **Trojans** are installed unknowingly while installing shareware or freeware applications that are supposedly designed to make your life easier. We recommend that when you download new files you scan them with your anti virus software before opening or installing them. If in doubt, don't do it.

The Internet is often used for the sharing and downloading of files, typically images, software, videos and documents via peer-to-peer networks. A consequence of the installation of the software necessary to join these networks is that each computer on a peer to peer network acts as a server for others and you usually have access to files on other peoples' computers as they have access to yours. Peer to peer applications allow users to connect to each other directly, without the need for a central management point, you search for your favourite music, films, games etc. and if other users have what you want on their computer it can be sent to you. As a result these files can often be downloaded at reasonable costs or even for free. However, it is important that you are aware that peer to peer networks have been used for the unauthorised copying of files. Various bodies representing copyright owners, for example music and film companies, now actively target those persons sharing unauthorised copies of files. They use a variety of Internet tracking tools. AdEPT like any service provider is obliged to disclose information in relation to customers connecting to the Internet when a lawful instruction, such as a court orders is served upon us.

If you keep sensitive information on your computer, it is worth using encryption software to protect it.

If you have a dial up Internet connection make sure that the computer is dialling the whole and correct number for your ISP, including the area code. This will reduce the possibility of other people receiving unwanted calls or you connecting to a service to which you had not intended.

3. Email – Acceptable Use Policy (AUP)

While connected to the Internet via AdEPT you must comply with the law.

You must not intentionally or unwittingly participate in the sending of unsolicited email, bulk or otherwise. This applies to material which originates on your computer system as well as third party material which passes through your system, with or without your knowledge

You must not send email which has forged header information, nor should you attempt to impersonate any other individual or organisation.

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.

If you are a business user and use a mailing list to send marketing or similar correspondence it is your responsibility to keep it up to date and to ensure that all un-subscribe requests are dealt with promptly; failure to so may result in any subsequent complaints being dealt with in the same manner as complaints of unsolicited mail, bulk or otherwise.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

Exchanging emails with others generally involves using common sense regarding the content material and being polite and courteous. The vast majority of AdEPT's customers understand what is appropriate when sending or receiving emails. Regrettably, there are occasions when individuals or groups of people exchange emails or involve in online activities, which are considered to be unacceptable by the Internet community. This is described by the generic term of "abuse".

It is not always obvious whether an activity is innocent, inadvertent, or intentional but as a general rule, 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 or cause to be sent any emails which cause annoyance, inconvenience or needless anxiety (e.g. subscribing someone to a mailing list without their authorisation). You should not send false messages likely to cause distress (e.g. advising the recipient that a relative has been in an accident when they have not), 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 to people on grounds of gender, race, colour, religion or other similar categorisation.

Although much unsolicited bulk email (**SPAM**) may just be a harmless but annoying way of advertising of products or services, some can be as distressing as receiving malicious telephone calls.

Email is sometimes used as a vehicle to attempt to lure Internet users into divulging personal information via bogus emails and or websites in what are known as “phishing” attacks. Increasingly, criminals are becoming very adept at creating accurate facsimiles of official communications and websites of financial and other institutions and you should satisfy yourself that you are in receipt of genuine email from them. If you are not, you should contact the organisation by another means to validate the communication.

There are some simple steps you can take to minimise the likelihood of receiving nuisance emails:

Don't give out your email address unless you are absolutely sure you can trust the recipient; you should treat your email address as you would treat your telephone number.

Be careful when sending details such as your credit card number by email. Unless you are completely sure you can trust the recipient and the details of the recipient's email address don't do it.

Consider that if you post your email address publicly on the Internet (for example on a personal website) it may be harvested by others for the purpose of adding to **spam** lists.

Be wary of so-called spam email cancellation services. They might be bogus services that collect rather than block email addresses for spam lists.

When filling in on-line forms always look for and complete any “opt in” or "opt out" boxes to reflect your wishes about being contacted regarding advertisement and promotion of any products and services.

If you become a victim of abusive emails, there may be little that your Internet Service Provider (ISP) can do to stop the abuse. However, the ISP of your abuser may be able to take action under its own terms and conditions as AdEPT would try to do on receipt of such a complaint. Accordingly, we recommend that you send an email to the "abuse department" of the email sender’s ISP (i.e. abuse@ the ISP) attaching the abusive email and all of it’s header (the full addressing) information.

It is unlikely that any ISP will provide you with the name and details of an alleged offender. However, an ISP may be obliged to divulge such information to appropriate authorities, such as the police or the courts, if formally requested to do so.

In cases of extreme abuse, you may need to contact the police if you think further action should be taken. If you decide to do so, you must be prepared to provide the police with any evidence you have. The police will then consider whether a criminal offence may have been committed and whether further action can or should be taken.

4. Newsgroups – Acceptable Use Policy (AUP)

While connected to the Internet via AdEPT you must comply with the law.

You must not post material that you did not create, unless you have the permission of the owner of the relevant rights to that material.

You must not make statements that are defamatory to or misrepresent others. Defamatory postings may include but are not limited to postings which harm the personal or business reputation of another or exposes him to hatred, contempt or ridicule, or lowers him in the estimation of his community, or deters other people from associating or dealing with him.

You must not post the same message repeatedly in one or more newsgroups.

You must not post chain letters or pyramid schemes messages or any other similar messages.

You must not blatantly disregard the intended subject matter in a newsgroup by making off topic postings with apparent malicious intent or in large volumes.

You must not maliciously try to incite other newsgroup users to deviate from the stated topic of the group. Attempts to anger others and to draw them into off topic debates are known as “trolling”.

You must not send data via the Internet which has forged addresses nor should you attempt to
impersonate any other individual or organisation.

You must not breach the charter of the newsgroup that you are in.

You should not post binary attachments such as images or files into newsgroup not designed for that purpose.

You should not post commercial advertisements to newsgroups. Most groups do not welcome contributions from business or commercial websites; even private promotional postings may be frowned upon.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

Newsgroup services are an easy method of communicating with large numbers of individuals. It is also a facility which can offer endless sources of information. Just about every topic one can think of is covered in one newsgroup or other and participating successfully in the various newsgroups is mostly a matter of common sense and extending courtesy to other participants. Unfortunately, it is also a source of abuse over the Internet. Posting into newsgroups may reach your desired audience, but it is not limited to that audience. Although the majority of newsgroup subscribers are helpful and courteous, some hide behind their anonymity and take great pleasure in replying to the often-innocent postings of a "newbie" (someone who is new to the Internet), with abusive or offensive language.

As with the rest of the Internet, newsgroups are subject to netiquette these are the conventions of Internet etiquette particularly associated with the use Newsgroups and their users. There are many resources on the Internet that list these rules, which can be found by searching for the term “netiquette” with a search engine.

Newsgroups are un-moderated and AdEPT provides feeds to a number of them. However many of them are subject to their own charters, and these charters are posted into the Newsgroups on a regular basis. Newsgroups are outside of AdEPT's control and AdEPT has no say in the type of material that can and cannot be posted to them.

AdEPT aims to filter out access via the AdEPT feed to Newsgroups that AdEPT perceives by their titles to have illegal content. However, AdEPT does not monitor the content contained in any of the Newsgroups and is not responsible for the content of any Newsgroup. In the interest of the safety of children, if you identify a Newsgroup with illegal content, you can notify us in order that we can consider adding it to our list of barred groups.

Newsgroups are often used for the sharing of files, typically images, software, videos and documents. It is important that you are aware that Newsgroups can be used to post or download unauthorised or even illegal material. AdEPT, like any service provider is obliged to disclose information in relation to our customers using the service when a lawful instruction, such as a court order is served upon us.

We recommend that you take some simple steps to minimise the likelihood of receiving abuse through participation in a newsgroup:

Do not give out your email address unless you are absolutely sure you can trust the recipient. You should treat your email address as you would treat your telephone number.

When posting into newsgroup configure your newsreader so that it doesn't show your email address or disguises it i.e. joe.bloggs32@nospam.isp.com. In the posting you would say "to reply to Joe, remove the nospam". The respondents would then need to remove the nospam section of the email address. This makes it more difficult for automated newsgroup trawlers to strip email addresses from the postings for the purposes of sending spam.

Avoid posting into Newsgroup if you are not entirely sure about the nature of their subject matter. If you are going to post into these groups, be aware that there is very little AdEPT, as your Internet Service Provider (ISP), can do to protect you if you become a victim of abusive emails resulting from your posting or a "**flame war**". If you do post into a Newsgroup that you are not entirely sure about, it is a sensible precaution to keep your email address private.

Be mindful of what you post. What may seem amusing to you may very well be offensive to another participant in a Newsgroup. Try not to cross-post .i.e. posting the same article to a number of groups.

If you do become a victim of Newsgroup abuse we recommend that you:

1. Block further communications from a particular sender. Within your newsreader software you will have the option to block the receipt of further messages from any particular sender; this is known in newsgroups as a “kill file”.
2. Send an email to the "abuse department" of the sender’s ISP (i.e. abuse@ the ISP) attaching the abusive communication and all of it’s’ header (the full addressing) information.
3. It is unlikely that an ISP will simply give out the name and details of an alleged offender. However, an ISP may need to divulge such information to appropriate authorities, such as the police or the courts, if formally requested to do so. We cannot address incidents of spam or other abuse unless it was posted through a AdEPT Internet connection.

5. Webspace – Acceptable Use Policy

While connected to the Internet via AdEPT you must comply with the law.

You must not have illegal material on your website or host a link to material that is illegal, wherever it is hosted.

Your webspace may not be used to distribute or advertise any of the following material:

1. Software for sending unsolicited bulk emails, excessive news postings etc.
2. Software for port scanning, virus creation, hacking or any other illegal or antisocial activity.
3. Lists of email addresses except where all the addressees have given their explicit permission.
4. Any collection of personal data other than in accordance with all applicable data protection legislation.
5. Links to websites hosting illegal content.
6. Content designed to offend or cause needless anxiety to others.

Your webspace should not be used to incite disorder or publish any material which constitutes instructions to commit illegal activities.

You must not use expressions that are offensive to others on grounds of gender, race colour, religion or other similar categories.

You must not make statements that are defamatory to or misrepresent others. Defamatory postings may include but are not limited to postings which harm the personal or business reputation of another or exposes him to hatred, contempt or ridicule, or lowers him in the estimation of his community, or deters other people from associating or dealing with him.

You must not publish or link to material or content in which you do not own the rights, without the permission of the owner of the relevant rights.

You must not publicise the personal details of others without their consent.

You must ensure that your index.htm or default.htm file (the first page to be viewed on your webspace) does not contain any material liable to offend. A clearly readable warning page must be displayed before any adult material is displayed. Equally, if you have any doubt about the suitability of your content for others, in particular to minors, you must display a warning page before a visitor reaches the content. If in doubt, seek independent legal advice.

You must not share the password for your webspace. Your passwords are your responsibility and must not be disclosed to a third party.

AdEPT cannot and does not 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 by the Internet community.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

As part of certain Internet services, AdEPT offers its customers personal webspace. This is an area on AdEPT's Internet servers that you can personalise and display to the World Wide Web (WWW).

Make sure you do not display too much personal detail on your webspace and remember that you publish any personal information at your own risk.

Be careful with content that may lead to argument; this is especially important if your website is also your primary email address. Not everyone will have the same opinion as you, and what you say could be offensive to others and lead to a situation where you receive abusive e-mails.

6. Chat, Instant Messaging and Video Messaging Services – Acceptable Usage Policy (AUP)

While connected to the Internet via AdEPT you must comply with the **law**.

You must not use the service to cause annoyance, inconvenience or anxiety to others.

You must not use the service to impersonate someone else.

You must not make statements that are defamatory to or misrepresent others. Defamatory postings may include but are not limited to postings which harm the personal or business reputation of another or exposes him to hatred, contempt or ridicule, or lowers him in the estimation of his community, or deters other people from associating or dealing with him.

You must not use the service to distribute illegal material or material that you did not create, unless you have the permission of the owner of the relevant rights to that material.

You must not use the service to transfer files that contain viruses, trojans or other harmful programs.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

Chat and instant messaging services are great fun to use and both are tremendously popular services on the Internet for all age groups. However, where there's fun there's also risk because there is no way of checking that the people with whom you may be communicating are who they say they are. In fact most chat rooms encourage you to adopt an alias.

Using chat and instant messaging services on the Internet generally requires politeness, courtesy and caution in exactly the same way as face-to-face and telephone conversations. This is probably more important when communicating with strangers. Whilst we recognise the right to freedom of expression, that right comes with a responsibility to respect the feelings of others. It is not necessary to use inflammatory language to express strongly held views and it is best to avoid getting into heated arguments in public chat rooms. There are many chat rooms out there and it is often best to leave the chat room rather than become involved in aggressive arguments.

Of concern to all parents will be the fact that chat rooms and messaging services, even those designed for children only can be used by adults who may, for example, pretend to provide a sympathetic ear for a child's problems, potentially coaxing personal information out of them and trying to arrange a 'real life' meeting – this is known as "grooming". AdEPT, the Government and the Police strongly recommend that a responsible adult supervises children using chat and instant messaging services. Parents and children alike should be careful not to give out any personal details or information that could be pieced together so that they could be identified.

If you decide to meet someone that you've been chatting with, arrange to meet in a public place and make sure that you've told a friend, preferably an adult, where you're going and who you're meeting. Better still take a friend, preferably an adult, along with you.

If you do become a victim of abuse in a chat room, there's often very little your ISP can do to stop the abuse. However if you do begin to received unwanted communications the simplest thing to do may be simply to ignore or even to block further communications from a particular sender. Within your instant messaging programme you will have the option to block the receipt of further messages from any particular sender. In addition, your chat or messaging programme may have a "report abuse" function. When using that function you should give the service provider as much information as you can and should include full details of your conversation, enclosing the chat logs or a cut and paste of the abusive message.

In cases of extreme abuse, you should contact the police if you think further action is required. If you decide to do so, you must be prepared to provide the police with any evidence you have including the abusive messages. The police will then consider whether a criminal offence may have been committed and whether further action can or should be taken.

7. Glossary

Applet

A type of computer program that allows animation and other interactive functions on a file or Web page.

ADSL

Asynchronous Digital Subscriber Line - A new technology that allows you to access the **internet** over standard phone lines at very high speeds.

Bit

The smallest piece of digital information understood by computers.

Bandwidth

The rate information travels from one place to another either inside a computer or between computers. Bandwidth is usually measured in **bits** per second, kilobits (thousands of bits) per second, or megabits (millions of bits) per second. A 28.8 modem allows for a connection of 28.8 kilobits per second.

Blocking software

A computer program that allows parents, teachers, or guardians to "block" access to certain Web sites and other information available over the **internet**. All blocking software has filtered the information before blocking access to it. (See also "**filtering software**")

Bookmark

A placeholder for interesting or frequently used Web sites, so that these sites can be revisited easily without having to remember or retype the internet address.

Browser

A **software** product that lets you find, see, and hear material on the World Wide Web, including text, graphics, sound, and video. Popular browsers are Netscape Navigator and Microsoft Internet Explorer.

Byte

Bytes are a basic measurement of computer memory. A byte is made up of eight **bits**.

Cache

A cache is a place on your hard drive where the **Web browse**r stores information (text, graphics, sounds, etc.) from pages or sites that you have visited recently so that returning to those pages or sites is faster and easier.

CD-ROM

A computer disk that can store large amounts of information; generally used on computers with CD-ROM drives. "CD-ROM" stands for "Compact Disk Read Only Memory". That means it can only play back information, not record or save material.

Chat

A feature of online services or Web sites that allows participants to "talk" by typing messages that everyone can read at the same time. Here's how it works: The participant enters the chat room, types a message on his or her computer, and sends it; and it is instantly displayed on the screens of the other users in the chat room. Admission is generally not restricted. You never know who is going to be reading your messages or responding to them, so it's best to be cautious.

Chat room

A "place" or page in a Web site or online service where people can chat, or "talk," with each other by typing messages. It's "real-time" communication like talking on the phone, except the "talkers" are typing text as with **e-mail**. E-mail, on the other hand, is delayed communication.

Client-based filter

A **software** program that you install on your own computer to block access to inappropriate material, prevent kids from accessing the **internet** at certain times, or to prevent kids from revealing personal information. See also "**filtering software**" and "**blocking software**."

Cookie

A piece of information unique to you that your **browser** saves and sends back to a Web server when you revisit a Web site (the Web **server** is the computer that "hosts" a Web site that your browser downloads or "sees"). The server "tells" your browser where to put the cookie on the server. Cookies contain information such as log-in or registration information, online "shopping cart" information (your online buying patterns in a certain retail site), user preferences, what site you came from last, etc.

Commercial service

General term for large online services. These services are like special clubs that require membership dues. Besides providing access to the internet, commercial services have lots of content, games, and **chat rooms** that are available only to members.

Cyberspace

A very general term used in a number of ways. "Cyberspace" can refer to the electronic areas and communities on the **internet** and other computer networks; the culture developing on (or across) the global network of phone wires that make up the internet; a new publishing or communications medium separate from conventional media; and a "place" separate from or in addition to physical space.

Discussion group An area online focused on a specific topic where users can read and add or "post" comments ("post" in the sense of posting something on a bulletin board). You can find discussion groups, also referred to as "discussion boards," for almost any topic. See also "**Newsgroups**".

Directories Similar to **search engines**, directories are indexes of Web pages organised by subject.

Domain name A Web site address, usually followed by .com, .org or.co.uk. See also "**URL**".

Download Copying data from another computer to your computer. "Download" is also used to mean viewing a Web site, or material on a Web server, with a Web **browser**. See also **upload**.

E-mail Electronic Mail. A way of sending messages electronically from one computer to another. Users can send memos, letters, and other word-based messages, as well as **multimedia** documents. E-mailing requires having a **modem**, connecting a telephone line to your computer, and an e-mail address (recognisable because of the "@" symbol, such as joe.bloggs32@yahoo.co.uk).

Ethernet the most common technology for connecting computers together in a network.

FAQ A list of "Frequently Asked Questions" about a specific Web site, mailing list, product, or game. Reading the FAQ first is a great idea when you are new to a site, mailing list, discussion group, or product.

Filtered ISP An Internet Service Provider (ISP) that automatically blocks access to content that is inappropriate for children. Each filtered ISP uses its own company criteria to decide which Web sites are inappropriate. When choosing a filtered ISP, parents and other caretakers should make sure the company's criteria are consistent with their own values and judgments.

Filtering software **Software** that sorts information on the internet and classifies it according to content. Some filtering software allows the user to block certain kinds of information on the internet. See also "**Blocking Software**, "**Client-Based Filtering Software**," and "Server-based Filtering Software."

Firewall A security device that places a protective "wall" around a computer or network of computers, keeping it from being accessible to the public.

FTP File Transfer Protocol - a way to transfer ("**download**" or "**upload**") files from one computer to another, for example from your hard drive to a Web server in order to update a Web site.

Flaming Sending a nasty piece of **e-mail** or posting a nasty comment in a **newsgroup** or **discussion group**, usually in response to a posting that offended someone.

Gateway Generally any device that provides access to another system. For example, an ISP might be called a gateway to the i**nternet**; also a **hardware** device that connects a local network to the internet.

Hardware The nuts, bolts, and wires of a computer and computer-related equipment, also the actual computer and related machines such as scanners and printers.

Hyperlink An image or portion of text on a Web page that is linked to another Web page (either on the same site or in another Web site). If it's a word or phrase, you can tell it's a link because it's another colour, it's underlined, or both. If it's an image, you can tell it's a hyperlink if you see a border around it, or if the cursor changes to a little hand when you drag the cursor over the image with the mouse. You just click on the link to go to another Web page or another place on the same page. See also **links**.

HTML Hypertext Markup Language - The standard language used for creating documents on the **World Wide Web.**

HTTP Hypertext Transfer Protocol - The standard language that computers connected to the **World Wide Web** use to communicate with each other.

Home page The first page or document Web users see when connecting to a Web server or when visiting a Web site.

ICRA Internet Content Rating Alliance rating system - a rating system for Web content (see also **RSACi**).

IMor Instant Message A **chat**-like technology on an online service that notifies a user when a friend is online, allowing for simultaneous communication (like talking on the phone, only with text). See also "**Web-based instant messaging**."

Internet Referred to as "Net" for short, a collection of thousands of connected computers and computer networks.

Intranet A private network that works like the **internet**, except that it can only be seen by a select group of people, such as the employees of a company.

IRC Internet Relay Chat - A part of the **internet** (not on the Web) that allows participants to "**chat**" online in a live forum that usually centers around a common interest. IRC is the earliest form of online chat.

ISDN Integrated Services Digital Network - A technology that allows you to connect to the **internet** over standard phone lines at speeds higher than a 56k modem allows. The technology is older and the connection speed lower than those of **ADSL**.

ISP Internet Service Provider - A company that sells access to the **internet**, most often through a local phone number. ISPs are usually distinguished from **commercial services**, which link to the internet but also offer additional services, such as content and chat, only available to their subscribers.

IP Internet Protocol - The computer language that allows computer programs to communicate over the **internet**.

Java A computer programming language that allows **World Wide Web** pages to have animation, calculators, and other fancy tricks. See also "**applets**".

Keyword On Web **search engines**, these are words that you type into the search form, or search "window," to search the Web for pages or sites that contain your keyword and information related to it.

LAN Local Area Network - A network of connected computers that are generally located near each other, such as in an office or company.

Link
Highlighted text that is designed so that clicking on it will take you to another document, Web page, or Web site. See also **hypertext**.

Modem
A **hardware** device that allows computers to communicate with each other over telephone lines. Modems come in different speeds: The higher the speed, the faster the data are transmitted. A modem enables what is generally referred to as "dial-up access." The fastest widely available modems are "56K" (or 56 kilobits per second).

Monitoring software
A type of **software** product that allows a parent or caretaker to monitor the Web sites or e-mail messages that a child visits or reads, without necessarily blocking access.

Mouse
A small device attached to your computer by a cord, which lets you give commands to the computer by clicking the device. See also **hardware**.

Multimedia
A combination of two or more types of information such as text, audio, video, graphics, and images.

Netiquette
The rules of **cyberspace** civility. Usually applied to the **internet**, where manners are enforced exclusively by fellow users.

Newsgroups
Discussion groups on the **internet** (not on the Web, which is only one area of the internet) that are broken down and categorised by subjects. These discussion groups consist of messages sent by other internet users and displayed publicly for everyone in the group (or under the topic area) to read. The word "news" in "newsgroups" does not mean they are run by news services or journalists.

PICS
Platform for Internet Content Selection - PICS is a technology that allows Web **browsers** to read content ratings of Web sites, but it is not a rating system itself.

Plug-in
A program that works with **browsers** to play audio and video.

Port Scanning
Port Scanning is an activity, which by using a particular type of software gives the user the ability to scan the computer system of another internet user. The purpose of which can be (but is not limited to), obtaining passwords and usernames, remotely controlling that computer or destroying data on that computer.

Posting

Like posting a message on a bulletin board, the sending of a message to a **discussion group** or other public message area on the internet. The message itself is called a "post."

PSTN

Public Switched Telephone Network. A circuit-switched analogue network which makes connections for the duration of telephone call. These connections are usually used for voice but can also carry data between facsimile machines and computers (via a modem).

RSACi

Recreation Software Advisory Council's internet rating system - a rating system for Web content that uses PICS technology. RSACi was recently renamed the Internet Content Rating Alliance (**ICRA**.

Search engine

A tool to help people locate information available on the **World Wide Web**. By typing in **keywords**, users can find numerous Web sites that contain the information sought.

Server

A host computer that stores information and/or **software** programs and makes them available (or "serves" them) to users of other computers. You download the information on a Web server with a Web **browser**.

Server-based filter

Unlike **client-based software**, which is installed on your own computer, server-based filters work on a host **server** (for example, a Web server) generally located at an I**nternet Service Provider** or a **LAN** at a company. Your computer is connected to this server so that you receive only the Web pages that are not filtered on the server.

Software

A computer program. Loosely defined, it's made up of a set of instructions, also called "computer code," to be used on your hardware. There is "system software" that operates the machine itself (such as the Windows and MacOS operating systems), and there is "application software" for specific uses, or applications, such as word processing, playing games, or managing your money.

Spider

A software program that "crawls" the **Web**, searching through Web pages and sites and indexing those pages in a database of Web pages that can then be searched using a **search engine**.

Spam Unsolicited "junk" e-**mail** containing advertising or promotional messages sent to large numbers of people. Sometimes people or companies send sexually explicit unsolicited e-mail, known as "porn spam."

TCP/IP Transmission Control Protocol / Internet Protocol - A computer "language" that allows for transmission, or "publishing," of information across the **internet**.

Time limiting software **Software** that allows time limits to be set for access to the **internet** or software programs such as games.

Trojan (Horse) A Trojan (horse) is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend" Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorised access by other means. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.

Upload Copying or sending data or documents from your computer to another computer, such as the server that hosts your home page. See also **download**.

URL Uniform Resource Locator - The **World Wide Web** address of a site on the internet. For example, the URL for this website is http://www.abuse-guidance.com. See also **Domain Name**.

Web The **World Wide Web** - What most people think of when they think of the **internet**. The Web is actually just one service on the internet. It is a collection of graphical **hyperlinked** documents made publicly available on computers (or Web **servers**) around the world. The information on these servers can be viewed or accessed with a **browser**. Other services on the internet include **Internet Relay Chat** and **Newsgroups**.

Web-based chat As opposed to chat **IRC** found on subscriber-only online services, Web-based chat allows people to chat with each other using a **browser**. Web-based **chat rooms** are found in Web sites.