Contents

List of illustrations

Introduction

As a parent who is an internet enthusiast I want my young son to get the best from this exciting new technology. Yet at the same time, I do not want him to come face to face with anything that could damage him psychologically or even physically. The internet provides children and teenagers with a fantastic resource that us grown-ups can only wish we had to help us with our homework! Yet lurking in the background is a whole host of unsavoury sites that youngsters can access that could harm them. This book will help you

make sure that your children get the best from the internet, without being able to see the worst. You will learn how to set up your own policing system so that you can be sure your children are not exposed to anything dangerous. At the same time, this book will help you ensure your child has the maximum value from the internet. If you are a schoolteacher, this book will also help you establish policies and systems to ensure those in your care are protected.

As always with books about the internet, the material contained in these pages is as up to date as possible at the time of going to print. However, updated information can be found at the following web sites:

- http://www.internet-handbooks.co.uk
- http://www.grahamjones.co.uk

If you have any comments on the material in this book please send you message to:

graham@grahamjones.co.uk

Author's Note

Whilst every care has been taken to ensure the information contained within this book is accurate, no responsibility can be accepted for the consequences of any action taken based on the material contained within these pages. Readers should seek professional advice, which is suited to their own personal circumstances. Readers may also wish to contact computer consultants regarding security issues.

Please also note that comments made about the Web Sites and other Internet pages mentioned in this book are based on how those sites and pages appeared at the time the book was written. Comments should not be taken as a reflection of how a site may appear at the time you access it, unless the site has remained unchanged since this book was written.

Copyright and trademarks

Chapter 1
What you should be worried about

The internet is full of pornography, is run by paedophiles and will have your youngster learning how to make bombs or commit murder – at least that's what you might think if you believed many of the more outrageous newspaper headlines. In fact, the internet is as far removed from this tabloid tittle-tattle as you could possibly be. However, the internet does include a considerable amount of material that your children could be affected or influenced by – and you may wish to protect them from such information. The worrying material falls into some distinct categories:

- Pornography
- Violence
- Racism
- Cults
- Harassment
- Adult centred advertising
- Misinformation
- Child abuse

The truth about online porn

Without pornography, the internet would not be as advanced as it is today. Indeed, much of modern life would not be as we know it. The porn industry was the first to exploit modern photography, videotapes, and now has been pioneering the internet. Indeed, some industry pundits believe that the humble videocassette has only become an everyday item because the porn industry popularised it. There is now considerable evidence that much of the internet technology that e-commerce sites take for granted was only developed because of the demands of the pornographers. For instance internet porn sites first performed online credit card processing and the first banner adverts were sold on sex sites. Added to this, web-based video conferencing was first used on pornographic sites to facilitate 'live sex experiences'. Nowadays, many e-commerce companies privately use the sex pioneers for advice on setting up effective web sites.

The success of internet pornography should not be surprising. To gain such material outside the net, means an individual can be more easily identified. They have to go into a shop, select the magazine or video, then handover money to an assistant who knows what material that particular person has purchased. With the internet it's anonymous – even though it's possible to track you down, it's more difficult and far less obvious. As a result, obtaining internet porn is as least embarrassing as you are likely to get. Small wonder then, that internet pornography is popular. The growing popularity of internet pornography has gone hand in hand with a reduction in the circulation figures of leading 'top shelf' men's magazines. For instance, in just two years from 1995 to 1997, Fiesta Magazine fell by almost a third from 250,000 copies a month to 180,000[i]. Similarly, Penthouse, which sold 400,000 copies a month 20 years ago, now reportedly sells less than 30,000. The internet has provided such established porn with furious competition.

According to a survey of 9,000 anonymous users conducted by the San Jose Marital and Sexuality Center, in the USA, 86% of men who use the internet access sex sites. The vast majority of these men are married or living with a permanent partner and almost none of them has any shame or guilt about their use of internet pornography[ii]. The survey also discovered that one in every 12 men who views internet porn, does so for more than 11 hours each week. Most of the men in the survey admitted to an hour or more viewing every seven days.

Indeed, viewing internet pornography has now become so common that psychologists estimate that there are 200,000 addicts in the USA alone. According to researchers from Stanford University there is a growing problem of 'cybersex compulsion'[iii]. Such addicts are amongst the millions of people spending money online. According to Datamonitor, the business research organisation, adult services on the internet accounted for almost 70% of the $1.4bn spent on the web in 1998/9. Clearly internet porn is big business.

Defining internet pornography

One of the biggest problems for parents in attempting to prevent their children from accessing the vast amount of porn on the net is defining what is pornographic and what is not. For instance, a simple search on AltaVista for the word 'sex' would locate you almost nine million pages as well as 55 discussion groups and more than 3,000 sexual products for sale. However, if you blocked the word 'sex' on your computer you could have problems. For instance, of those nine million pages, there is information on the genetic determination of sex, which would be extremely valuable for GCSE biology students (http://lena.jax.org/pubinfo/media/releases/eicher.html). So defining net porn as anything that has the word 'sex' in it can be highly problematic.

Using a legal definition is just as bad. In fact in the UK, there is no legal definition of pornography. Legislators have been shy of making strict definitions, allowing case law to preside since this reflects the public opinion at the time. For this reason, the Obscene Publications Act (which covers net porn) could allow anything to be online as long as it does not 'deprave or corrupt'. As to what exactly depraves or corrupts is up to a jury and naturally enough, one group of 12 people can have entirely different views to another. This is why some items that are deemed pornographic in one trial, get off Scot free in another. The changing tastes of the public have been seen recently when the British Board of Film Censors was criticised for allowing videos that showed sexual penetration to be given a license for sale in a sex shop. Within a year, similar videos were refused the 'Restricted 18' licence – due to fear that children could view the videos. This refusal arose amid a climate of increased public concern over internet pornography. In other words, the British view of what is pornographic changes over time and hence the legal definition also varies.

This is not the case in other countries. In the USA, for example, the production of almost all kinds of sexual material is completely legal – though some states restrict manufacture and/or sales. Throughout Europe almost all kinds of sexual publication are also legal. Indeed, it is only in Britain and countries where religion is central to the culture, that depiction of sexual acts is illegal. This poses a considerable problem on the internet. What is perfectly legal in France is illegal just 25 miles away at the Kent coast, for example. That means a French internet publisher could legally produce a web site showing explicit sex and make this available for viewing internationally. However, simply looking at these web pages in the UK could be illegal. Yet the statistics show quite clearly that millions of such pages are viewed daily in the UK.

Understanding the British legal position

Internet pornography in Britain is covered by four main laws:

1. The Obscene Publications Act
2. The Telecommunications Act
3. The Criminal Justice Act
4. The Protection of Children Act

Under these Acts the following activities are punishable by fines up to £5,000 or imprisonment up to three years:

- To publish or possess for gainful publication any item that is obscene
- To transmit over a public telecommunication system anything that is grossly offensive, indecent, obscene or menacing
- To possess any indecent photograph or 'pseudo photograph' of a child
- To take, make, distribute or show to others any indecent photograph or 'pseudo photograph' of a child

Some interesting case law has recently been established that impacts on internet pornography. For instance, the courts have decided that making a web page available constitutes publication in the UK, even if that page is hosted on a web server elsewhere in the world. In addition, the courts have now decided that 'making a photograph' includes copying it to a computer hard disk.

More information on these laws can be found at:
http://www.policelaw.co.uk/internet.htm

Catching the pornographers

Under British law, considerable amounts of material that are freely available on the Internet are actually illegal. Simply opening up a particular web page could lead you to commit a serious offence since the images are copied to your hard disk when you view the page. If you are a regular viewer of sex sites, your computer could be full of images that a court might believe you had collected for gainful publication. In essence, therefore, any regular sex site surfer could be caught and punished. However, with almost all internet users looking at sex sites, the courts would be awash with people who had done little more than seek titillation. Hence, the police are only really interested in the serious troublemakers – people who produce, publish or distribute some of the more dubious material such as bestiality or child porn. Indeed, police forces are co-operating like never before in an attempt to curb child pornography in particular. For example, a dawn raid at the end of 1999 involved 20 different police forces at 27 locations throughout the UK. Several arrests were made and a large amount of computer equipment confiscated. Central to such investigations is the Paedophile Intelligence Section of the National Criminal Intelligence Service, based at Scotland Yard (http://www.ncis.co.uk/pa.html). A significant role of this organisation is to monitor internet activities to make sure that child pornography is curtailed. However, in an interview with The Observer, Chief Superintendent Martin Jauch of the Metropolitan Police said: 'Our internet unit is very small. We can't monitor what goes on right across the internet.'[iv]

Indeed, the most famous case of child pornography in the UK involved pop star Gary Glitter (Paul Gadd). He admitted 54 charges of possessing child pornography downloaded from the internet – but the offending pictures were only discovered when the computer was taken to PC World in Bristol for repair. Another pop star, Derek Longmuir, of the Bay City Rollers, was also found in possession of child pornography – but only after a tip-off to local police. What these high profile cases reveal, is that child pornography can circulate easily, since the police resources to attack the problem are considerably limited. Catching the culprits is usually more by chance than the police would like us to believe. With the risk of being caught so slight, is it any wonder that an estimated 20,000 pornographic pictures are added to the internet every day[v].

Identifying the real porn problems

The internet has three main areas where vast numbers of sexual images are posted each day:

1. The World Wide Web
2. Email
3. The Newsgroups

Pornography is littered throughout these, but in varying degrees of danger for children. The least problematic is the web, in spite of it being so easy to find pornography. Enter the innocuous word ‘boob’ into the Yahoo search box and you’ll be able to go straight to ‘The Boob Cruise’ – a web site devoted to a holiday in the company of 24 large breasted topless models. The web site (http://www.boobcruise.com/) does not require any adult verification and within seconds you can see naked women, including many in provocative poses simulating masturbation. Fine, if that’s your kind of thing, but would you want your six year old to see it?

Even so, in spite of such problems (which can be solved – see chapters 3 and 4) the web is the least of your concerns. That’s because the companies who host web sites generally, though not always, police their machines to ensure that illegal material is not made available on them. In the UK, for instance, this is a requirement of membership of the Internet Service Provider Association (http://www.ispa.org.uk). Internet service providers also publish their ‘acceptable use’ policies, to which anyone running a web site is required to adhere. You can see a typical policy at:

http://www.unipalm.pipex.com/customerservices/usepolicy/

However, such policies do allow for the publication on the web of considerable amounts of sexual material. You might not like pictures of women with their clothes off, or men with erections, but they are not illegal and hence can be found easily on the web. Equally it's not illegal to watch other people engaging in sexual acts, or to talk to consenting adults in a suggestive manner – hence you can gain access to all sorts of interactive sexual services via the web.

You can also receive sexual material as an email. This is how some people have lost their jobs – using email systems to distribute pornographic images to work mates. But the widespread use of email and its speed and ease means that your children could be sent messages that you would rather they did not receive. The chances of their email address being 'mistakenly' sent email are slim. More likely is the deliberate sending of pornographic messages. Indeed, one in three email 'spams' is pornographic[vi]. A 'spam' is an unsolicited email sent to a large number of recipients – a sort of mail shot. The people sending porn spams are usually inviting you to look at their web site (from which they then make money). However, because they use bulk email lists they have no idea as to the age of the email recipient, or even if an adult would want to receive these kinds of messages. However, enough people are curious about the emails to try the web site and this is why the promotional technique works. The downside is sending sexual emails to people who have no desire to see them, or allowing them to be viewed by children.

Much worse than this, however, are the newsgroups. These are the non-moderated sections of the internet that are not controlled and can be added to by anyone at anytime from anywhere. Indeed, this instant, international communication is a fantastic boon and is one of the greatest plus points of the internet. However, it is also one of its main downfalls. The lack of control and the non-ownership of newsgroups mean they are open to anything. The worst kinds of sexual imagery and text can be found in newsgroups. Bestiality, child pornography, coprophilia (sexual stimulation as a result of eating human faeces), necrophilia (sexual intercourse with a corpse) and rape can all be found in internet newsgroups. The newsgroups of the internet make the sexual pages of the world wide web look quite tame. Imagine what you might see at the following newsgroups:

alt.binaries.pictures.erotica.bestiality.hamster

alt.binaries.pictures.erotica.hermaphrodites

alt.binaries.pictures.erotica.violence

alt.sex.aluminium.baseball.bat

alt.sex.necrophila.royal-family

These were all widely available newsgroups, for which no adult age verification was required, in the spring of 2000. Little wonder then that the Vice Unit of the Metropolitan Police wanted such newsgroups banned. A letter sent by Chief Inspector Stephen French to internet service providers in August 1996 alerted them to the problem of such newsgroups. Internet service providers now block many of these kinds of newsgroups, but as fast as they curb one, another is published. It is a never-ending battle. Also, no matter that your internet service provider blocks such newsgroups, it's a comparatively straightforward task to access the newsgroups via another server hosted in a country that has few or no restrictions.

The Internet Watch Foundation – a body that represents a host of interested parties, including the police, government and the internet industry - has highlighted the problem of newsgroups. In 1999 the Foundation acted upon 11,487 items of offensive material on the internet. Of these, some 11,412 were child pornography and of these 11,230 were in newsgroups. The clear implication is that the most dangerous part of the internet is 'usenet' where the newsgroups lurk.

Violence on the internet

Newsgroups are also a problem as they can be used to promote violence. For instance the newsgroup 'free.uk.guns' is apparently dedicated for teenagers and there are some pretty nasty messages for anyone who is not in their teens who takes part. However, 'alt.hobbies.serial-murder' is not as damaging as it sounds, since the newsgroup is for people interested in researching serial murders or writing fiction. So you can't simply use the name of a newsgroup to determine whether or not it should be blocked – after all, what provokes serial murder could easily be part of an A Level psychology course. Often messages of a violent nature can lurk anywhere within newsgroups. Some people appear to gain enjoyment from writing offensive messages to just about anyone. So even though there are no newsgroups as explicit as those for sexual imagery, violent material does exist within the usenet area of the interent.

Even though the newsgroups are a breeding ground for violent material, you can much more easily obtain violent material on the web. That's because the legal position is far less clear than exists for pornography. For example, explaining how to make a bomb is not actually illegal. Therefore, internet service providers would not block such material, nor be able to ask their clients to remove it. Equally, in the USA, where over half the world's web sites exist the constitutional commitment to free speech means that violent material is perfectly allowable.

A quick search for 'bomb making' can take you to instructions on how to make a 'grenade' from a tennis ball, razor blades and some matches. That's just

four clicks away from the Yahoo search page. Such instructions are littered throughout the internet, often in web based discussion pages. The 'tennis ball' grenade instructions are contained in a web site devoted to 'trebuchets' – large catapults used for hurling stones in medieval times. However, because the discussion pages of such web sites are not moderated or edited, anyone can post details of anything they like – and they do. This means that web discussions, like the newsgroups can contain a host of violent material, often hidden in unlikely places.

However, it's not just non-moderated discussions that can pose a problem for children. One internet site in Japan, for instance, advertised the sale of cyanide capsule for suicide. The web site was aimed at people who had decided to commit suicide but did not know what drugs to take or in what quantities[vii]. Other dubious web sites exist as well. There is a web site to 'legalise the enslavement of midgets' that advises you to kill the wife of any midget and then lock the individual in a garden shed. Although the site proclaims this is a joke, it's pretty sick. Another 'joke' site even includes a price list for various violent acts, including 'killing a parent Texas cheerleader style - $799.95'.

Yet there are serious sites that are just as worrying. You can, for instance, buy CS Gas over the internet. Whilst possession is illegal in the UK, there are no methods of preventing you from buying this from legitimate web sites. At just $5.95 per canister it's within the range of a child's pocket money. Equally you can buy electric stun guns, knuckle dusters and the like, all supposedly for self defence, from a range of web sites – all quite legitimate. The web is also used as a place for threats or to take out revenge.

At the beginning of 1999, the American Coalition of Life Advocates – an anti-abortion group – was fined $107 million for its web-based campaign that sought the names of doctors who practised abortion. The web site gave rewards of $5,000 for the names. However, the anti-abortionists were caught under an American law that makes it an offence to incite violence against abortion doctors[viii]. Naturally enough, having an anti-abortionist view or even running a web site against abortion is perfectly legal. However, the web site was deemed illegal under a highly specific law that only applies in the USA, and was only brought in during the mid-1990s as a result of violence against doctors. Without this law, the web site may well have been able to continue inciting violence – as many others are able to do because they do not pinpoint the medical profession. Indeed, according to the Simon Wiesenthal Center, a Los Angeles human rights group, there are more than 1,400 web sites devoted to the promotion of hate. These sites promote violence and encourage thoughts about violence against particular groups. For more information go to:

http://www.wiesenthal.com

Racism on the internet
One of the areas that is highlighted by the Simon Wiesenthal Center is online racism. This is found throughout the internet, including the web and usenet. Free speech laws in the USA mean that racist abuse is possible – within some limits. In the UK, there are various laws that govern racial abuse, but one of those that applies to publishing (a web site is a publication) is the Public Order Act 1936. This states that anyone who publishes anything that is likely to incite racial hatred against any group of people in Great Britain can be prosecuted. However, this does not put people off producing racist material for the internet. In fact, they are able to hide behind a degree of anonymity meaning that they can get away with their crime. Equally, they can argue that their incitement to hate is not against a group within British jurisdiction – thus escaping the law altogether.

The internet therefore provides an easy route for people to promote racist views and propaganda that they could not so easily do using traditional publishing. You can find all sorts of racist material on the internet, ranging from 'white supremacy' material, to anti-Semitic information and anti-Moslem pages. You do not need to be of any particular age to enter such sites, so they are accessible to children. Equally, these sites are easy to find. Just three clicks away from the Yahoo search page and you will find an article by David Duke, an American Republican politician whose 'Duke' web site is designed to tell 'the truth' about race in the USA. However, his article that is easy to find for any child, suggests that controlling the birth rate of American blacks is a necessity to avoid increased liberalism. Whilst this is not as extreme as the 'hate' sites around, it reveals the kind of information your children can obtain from 'mainstream' sites devoted to the race issue.

Go on to the murkier sites and you will find material suggesting that all non-whites should be shipped out of the USA, that all Jews should be returned from wherever they live now to Jerusalem or that blacks are intellectually inferior to whites and therefore do not deserve the same rights. Worse, much worse, is not far away as a result of links from the serious-looking sites to sites run by small bands of people who can only be described as evil bigots. Yet, for the most part what they publish on the internet is either legal, or difficult to control. Much is being stamped out, as a result of blocking by internet service providers. Even so, not all service providers can or will do this. The result is racists have the freedom and the anonymity to promulgate their views.

Using the net to gain recruits
The racist groups that exist on the internet love it because it is a fertile source of new recruits. Youngsters in particular can be swayed by the one-sided

information and sign up with the organisations, before they have had a chance to discuss the issues and form a real opinion. This is also why cults have adopted the internet as a way of promoting themselves. Members are attracted to cults via the internet and the 'Heaven's Gate' cult is a prime example. In this cult 39 people committed mass suicide because they believed the arrival of the Hale-Bopp comet signalled the end of the Earth. Friends and relatives of those who had committed suicide believed that the internet played a significant part in the recruitment of the cult's followers. The 'Heaven's Gate' web site was quickly withdrawn by the internet service provder.

Other religious movements also use the internet to attract members, though many of them are 'respectable' and have a huge international following. For example, the Church of Scientology, which follows the teachings of L Ron Hubbard, promises solutions to all of society's ills by encouraging people to live their life to a programme laid down by the religion. Scientology claims it is the world's fastest growing religion and this is reflected in a huge web site that has a vast array of material and a range of interactive activities. These include online church services and a 'personality test'. This consists of 200 questions and you have to give them your name and address and telephone number to take part. Clearly, by providing them with your name and address you open yourself up to being recruited. Whilst Scientology is perfectly legal, some people believe it brainwashes its members (see: http://www.sky.net/~sloth/sci/sci_index.html#HCG). Hence you may not want you children to even view the pages of legitimate religious movements that use the internet to promote their activities. In addition, many religions and cults have more than one web site – scientology, for example, has more than 130 web sites devoted to it.

Being harassed on the internet

Some of the less respectable religions can use internet techniques to harass you or your child, into joining. But it's not just religious groups that can harass you via the internet. The whole area of 'cyberstalking' has become a real issue and a new organisation has been set up to help combat the phenomenon. You can find out more at the following web site:

http://www.haltabuse.org/

Cyberstalking has a number of different ways of being conducted, but essentially via email, newsgroups and pop-up windows on the web, it is possible to target individuals with abuse.

Receiving unwanted advertisements
Another form of abuse for some people is the receipt of unwanted advertisements. These can pop up as a small window when you enter a particular web site. However, web design techniques mean that it is possible to automatically open new windows when you close another. Sometimes, this means that advertisers can be pervasive, causing adverts to repeatedly open, even though you keep closing them. The internet porn industry is most famous for this technique, though other industries are catching on. Although it is annoying for most people, the technique clearly works otherwise it would not be done. For parents, this method of advertising is quite disturbing; not only does it potentially introduce your child to products or services you may not wish them to view, you cannot quickly get rid of the advert as a new one pops up as soon as you close the offending item.

Deciding if something is true
One of the problems with advertising is that it can make exaggerated claims. Whilst there are laws in most countries about the claims allowed in adverts, there are no such laws when it comes to publishing. It is perfectly legal to publish a complete pack of lies. For parents this can be just as worrying. Web sites may actually be telling your children complete nonsense. For instance, the telephone company Ericsson had to produce a special web page to explain that the information circulating on the internet about its 'free telephones' was a myth. Someone purporting to be a member of staff was suggesting that by completing a simple email task, a free internet-enabled WAP phone would be supplied. Teenagers may well have been attracted by such a 'scam'. Many such internet misinformation campaigns are highlighted at Scambusters:

http://www.scambusters.com/index.html

However, it's not just scams that are worrying. Seemingly factual sites can be dispensing falsehoods. That's because it's perfectly possible for anyone to set up, write, edit and publish a web site without their material being checked. In the traditional media all published material goes through several checking procedures to enable the highest possible degree of accuracy. Indeed, five people, apart from the author, will have checked this book before it was printed. A single person can produce web sites with no reference to anyone else, thus allowing myths, lies and factual errors to be made available. With newsgroups it is even worse as people can enter information anonymously and therefore can more easily misinform. The National Council for Reliable Health Information – an American watchdog – has identified, for example, a number of unreliable web sites that provide poor information. One case in point is a web site devoted to the prostate gland, which could provide useful to teenage biology students. However, the information is written by a lawyer and

estate agent, not a doctor. The site tells us that the prostate gland is required for overall health and quality of life. This is plainly not true as many men have their prostate glands removed for a variety of reasons often reporting improved quality of life as a result. Indeed, for some men prostate gland removal can be life saving. Students at GCSE level may not appreciate this, though, and could easily believe such web sites to be statements of fact, rather than opinion.

The most worrying aspect of the internet

Whether your children believe what they read on the internet is of particular concern when it comes to the most troublesome and worrying problem of all – child abuse. The internet has fast become the main way in which paedophiles and other abusers communicate, passing on information and disgusting images. These despicable individuals can also use the internet to target children, often by hanging around in child-related chat rooms pretending to be other children. Children may believe what they are being told in chat rooms and newsgroups may be factually correct. However, such information may be part of the pretence that is necessary for paedophiles to commit their crimes. Indeed, UNESCO, the United Nations Educational Scientific and Cultural Organisation, has identified child abuse on the internet as one of its key programmes and has already held two major conferences on the problem, resulting in a range of projects designed to combat the problem. Governments too are concerned about the problem, as are leading proponents of the benefits of the internet. Microsoft took a leading role in helping to promote the Children's Online Privacy and Protection Act (COPPA), which came into force in April 2000. This requires parental consent to be provided before children under the age of 13 can provide any information to particular web sites. It only applies to American hosted web sites, but that represents more than 50% of the world's internet resources, so should prove helpful in limiting child abuse online. That said, however, much of the child abuse is conducted via newsgroups and chat rooms, which have little if any controls. Even legislation is difficult to produce because of the degree of anonymity that is possible. Even so, the authorities are determined to stamp out child abuse via the internet, because it is the most threatening problem for children using this new technology.

Considering all the problems

A quick trip around the world wide web, newsgroups and email systems can reveal a host of troublesome areas that could affect children detrimentally. By far the most worrying of these is child abuse and paedophilia. However, there are many other areas to worry about, including simply misinformation, through to children being brainwashed by cults or being able to view adult

pornography. For any parent, therefore, the internet is the most dangerous street corner in the world. Your children can hang around there and see all sorts of things you would rather they did not. However, it is also the most exciting street corner anywhere, providing youngsters with the richest, most dynamic and stimulating educational resource ever. That's why you should not allow the darker side of the internet prevent your children from accessing what is so good about it.

Chapter 2

What you don't need to be worried about

The internet gets more press coverage than any other industry. Every newspaper and magazine contains references to the internet and advertisements are full of email addresses or web site names. In one edition of the Times in April 2000, the internet was mentioned 244 times in the editorial alone. Added to that, of 40 display advertisements, 34 were specifically advertising web sites. Clearly, the internet is an important phenomenon and one that is rapidly becoming central to society – judged by the importance newspapers and advertisers give to it. However, some of the editorial coverage could be off-putting. For instance, finding stories about credit card frauds or the prevalence of internet pornography is comparatively easy. These kinds of stories appear in the media almost daily. Word like 'filth', 'scum' and 'porn merchant' are frequently associated with the words 'internet' or 'web' in popular newspapers. The result is a level of concern and fear about the internet that is not really required. One example is a study from Jupiter Communications, which found that 64% of people do not trust internet sites[ix]. Michelle Slak, an analyst with Jupiter commented: 'Web ventures are allowing the media to create an online privacy dialogue with consumers thereby missing out on an opportunity to shape this important dialogue with consumers themselves.' The Jupiter report suggested that the industry has not been very effective in promoting its benefits to consumers, allowing the media to set the agenda.

Even so, the internet has stimulated more business in the last five years than any government-sponsored activity. Equally, internet companies have created more jobs than any other industry. At the same time, people across the world have been able to communicate in ways that they could only have dreamed about in the mid-1990s. Now they are part of everyday life; the internet has already been a significant contribution to society and more benefits are yet to come. However, many of these benefits will not materialise as quickly as predicted if people are put off using the technology by groundless fears.

For parents, the main worry is that the internet could harm their children. The sheer volume of pornography, the potential for racism and other forms of abuse, and the threat of cyberstalking all combine to make many parents very wary about allowing their youngsters to use the internet. Yet the internet can help your children in so many positive ways. These include:

- Learning about the world
- Completing their homework
- Keeping in touch with relatives and friends

- Stimulating their thought processes
- Playing in groups
- Taking part in clubs and societies
- Buying school supplies

Clearly, the internet provides youngsters with more information and resources than any parent could possibly afford – even if they had the time to assemble it all! Yet even these benefits are not enough to convince parents that they should limit their child's use of the internet. There are several reasons for these concerns, though many of them are founded on popular conjecture, rather than hard fact. The list of worries includes:

1. Children will become addicted to the internet
2. Children will choose the internet instead of physical exercise
3. Children will learn about sex too early
4. Children will become violent if they see certain web sites
5. Children will fall prey to abusers who lurk on the internet

These worries are based on no real understanding of what children actually use the internet for. Happily, there is plenty of research to help us.

What do children use the internet for?

According to the online market research firm, NFO Interactive, (http://www.opinionforce.com/about.html) the most popular use of the internet for children is completing homework or school projects[x]. The next most popular use of the internet is for playing games, followed by keeping up to date about sports. The survey also revealed that, on average, children only spend 10% of their time surfing the web – almost the same amount of time they devote to reading books.

Almost half of British children regularly use the internet and most do so from home. Only one in three children gain access to the internet at school[xi]. These findings come from a regular NOP survey of internet usage, which also reveals that less than 20% of children have found something on the internet they believe was 'rude' – meaning of course, that eight out of ten youngsters surfing the web have not found anything so embarrassing. You would be mistaken at thinking this is because a whole raft of internet users are male teenagers, keen to access sites they would not think of as 'rude' but rather stimulating! That's because almost two out of every three internet users under

the age of 18 is female, according to research conducted by the online research specialists, Fletcher Research (http://www.fletch.co.uk/).

There has also been some extensive research of the attitude of children to the internet. Most rate the internet as a better communications tool than the telephone, according to research from Roper Starch (http://www.roper.com). This study also showed that two out of three children prefer the internet to television and that 75% belief the internet has improved their life. The regular NOP survey has found similar views with most British children viewing other internet users as 'clever', 'friendly' and 'cool'. This survey also showed that eight out of ten youngsters believe the internet helps them to learn. This has been backed up by research from the US National School Boards Foundation that showed there was a significant improvement in attitudes towards school attendance in children who used the internet[xii].

From all of this research, it seems that most children use the internet as an educational and communications tool. Few ever see anything 'rude' and most find it stimulating and helpful. Even so, parents worry, largely because of the media hype surrounding the more loathsome aspects of the net. The main parental worries are the same as those that are frequently voiced about television. Parents are worried today, as they were 50 years ago, that TV would lead to lazy children, addicted to watching the screen that filled them with violent or sexual imagery. However, there has been considerable research that shows many of these concerns are quite groundless.

Looking at the psychological research

When Diana Princess of Wales died there was unprecedented media coverage accompanied by an international outpouring of grief. Some observers believe that the media stimulated the grief[xiii]. In other words, the media contributed to the behaviour of many people. The fact that we expect the media to change our behaviour should not be surprising. After all, several billions of pounds are spent each year by advertisers expecting that their media presence will change human behaviour. Their advertising is designed to make people purchase products and services they might not otherwise have done. The advertising world clearly believes that what we see in the media can alter our behaviour.

However, some psychological studies suggest that the media does not influence behaviour[xiv]. Studies suggests that exposure to occasional violence in TV programmes does not make children more violent. This evidence flies in the face of the 'common sense' notion that the media must influence behaviour – as shown by the behaviour of people after the death of Diana, Princess of Wales, or by purchasing items following exposure to advertisements. However, the psychological studies go further than common sense and reveal some interesting facts.

When we alter our behaviour it appears we generally do so if there is some reward for us. We follow the advertiser's encouragement because of the personal benefit buying their product will bring. Many of us may well have been grief stricken by Diana's death out a combination of true sympathy and reward from others for our display of grief. Such conclusions can be drawn from the psychological research on the impact of TV violence, because these have shown that although individual programmes do not make children more violent, there is a group of youngsters who are influenced by them. These children are those who are rewarded for their behavioural change towards a more violent pattern. After watching TV violence, kids who are normally punished by parents for violent acts do not change their behaviour. However, children brought up with few parental controls or who are actively rewarded for violence, become more violent after watching television violence. This is even more likely if the children are repeatedly exposed to TV violence. In a way, the violent children are being conditioned to become violent. Much of the research on the effect of television violence points the same way. It only has an effect on those children who are already violent or brought up within a violent family or where there are no controls over watching TV. In other words, violent TV programmes mostly affect those rewarded for violence. If you think about it, this is the real common sense approach. After all, advertisers have no impact on people who are not rewarded by shopping. So arguing that TV violence must impact on us, because advertising does, misses the subtle point that advertising, or Diana's death, only affects some of us – those ready to be affected. Extending the psychological research on TV violence to the internet implies that children are only going to be affected by the internet if they are already pre-conditioned to be changed by what they see or are rewarded by a behavioural change prompted by the internet. Some interesting facts for parents about violence can be found at:

http://www.cme.org/children/kids_tv/violence.html

You will also find some interesting reading at:

http://www.childpsych.com/sample2.htm

Here you will discover that there is psychological research to show that children who are allowed to play normally are those who develop in a balanced way. Those that are simply slumped in front of the TV or deprived of play in any other way are those most likely to be influenced by negative material on TV or the internet. What all of the psychological research on the impact of the TV on child behaviour shows, is that good parents have nothing to worry about. They will limit and control TV watching so that children can develop normally. Bad parenting, however, allows children to avoid play and be rewarded for behavioural change stimulated by TV programmes.

Let's talk about sex

Although violence, cults and harassment are widespread on the internet, most parents worry about their children viewing pornographic material. This is found throughout the internet and can be easily located. However, as already seen, most children are not browsing 'just to fund anything', where they may be able to view sexual images. Instead, children are using the internet in a structured way to help complete their homework. But what if they see sexual images? Will they become perverted or damaged in any way?

Millions of children have been able to see women in various states of undress in our daily newspapers for almost 30 years. So far, there is no discernable evidence of any damage to society – some people may not like the images appearing in our 'newspapers', but many do. Sexual imagery is also omnipresent in advertising, even though codes of practice in advertising try to limit such material. In fact, children are surrounded by sexual imagery. However, the vast majority of what they are able to see is titillating, rather than explicit. The internet is also stuffed full of such provocative material – topless women, men and women in skimpy clothing or nude pictures. In fact, research by MSNBC has found that most sexual material used on the internet was of the 'Playboy' variety and not, as the media would have us believe 'hard-core porn'. The likelihood is, therefore, that should children 'stumble' across sexual imagery it is more likely to be of the less explicit variety. This does not mean to suggest that there is no hard-core porn – there is a great deal of it on the internet. However, a child is more likely to see soft-core than anything else.

All of the evidence suggests that sexual imagery is not the problem for children that many adults would like to believe. In fact, there are considerable cultural variations in beliefs, with even hard-core pornography being on open sale in supermarkets in much of Europe. It is interesting to note the differences in teenage pregnancies, for instance, throughout Europe. In Britain, where pornography is highly regulated, there is the highest rate of teenage pregnancy[xv]. In France, Germany and Holland, where the laws are more liberal, teenage pregnancy is the lowest. Whilst this does not mean there is a link between the lack of pornography and teenage pregnancy, it does indicate a cultural attitude to sex. In Holland, where sex education happens at an early age and where prostitution and pornography is widely available, youngsters appear to be more at ease with sexuality and therefore in more control. In Britain, where sex education is poor, delivered late and where prostitution and much pornography is illegal, sexual problems are at their greatest. A direct link between these areas probably does not exist, but what the figures reveal is that children are able to take on the world of sex, without damage ensuing. By attempting to protect them too much, we could be doing more harm than good. Indeed, this has been shown in psychological research that has identified the fact that children as young as three years old understand the genitals and what they mean[xvi]. Other research has shown that children brought up in households where they see their parents nude, tend to have fewer sexual hang-ups in later life. In short, children know what sex is all about much younger than we would like to think – they are not as innocent as they seem. Equally, there is little evidence that titillating images

has any impact on them. However, more explicit images could be problematic, especially as much hard-core porn is violent in its approach. A one-off accidental viewing of such images is not likely to be problematic, if parents don't make an issue of it. However, repeated viewing of such material could cause problems; as was shown earlier psychological research shows that regular, unsupervised viewing of violent material can cause behavioural changes in children. The same is likely to be true for hard-core porn as it frequently depicts men as more powerful and often violent towards women. What this all means is that children with good parents will be unlikely to suffer any damage from accidentally seeing sexual images on the internet. As with violence, it is the unsupervised child who could be damaged.

Becoming addicted to the internet

Parents worry that even if their child doesn't see violence or view pornographic pictures, they will become addicted to the internet. Internet addiction is seen as something negative, compared with addiction to a train set or to schoolwork. Yet we can be addicted to anything. Your child could become addicted to the internet, but equally your youngster could become addicted to alcohol, cigarettes or heroin. Children, like adults, can become addicted when the object of their attention provides a degree of gratification that they cannot obtain elsewhere. A child that becomes addicted to the internet is actually telling you they are not getting the best out of their own life and that the addiction is filling a void. Behavioural therapy for addicted individuals replaces the 'bad behaviour' of the addiction, with new behaviours that provide the satisfaction that is sought, but without any problems. In this way, alcoholics, for instance, can replace the high they get from a drink with some other kind of boost. The trick for the therapist is locating the alternative positive behaviour. However, what is clear from these therapists is that the addiction can be controlled, if not cured. So if your child does become addicted to the internet, it is possible to treat the problem – though it's easier to prevent it from getting out of hand in the first place. Parents, who know what their children are doing, are therefore unlikely to allow addictions to be acquired. Once again, you need not worry if you have good parenting skills – the chances of your children becoming addicted to the internet are slim. The worst-case scenario suggested at the American Psychological Association was that six percent of internet users were addicted. However, the research methodology was heavily criticised (http://www.salon.com/tech/log/1999/08/24/addicts/index.html). Other research points to the fact, as is the case for many addictions, that internet addicts display a range of other psychological problems at the same time[xvii]. In other words, internet addiction is a symptom rather than a disorder in its own right. Children who become addicted to the internet are already likely to have a range of other difficulties, already identified by their parents.

Being abused by paedophiles

Whilst the world's police and governments give a high priority to paedophiles that lurk on the internet, the truth is that such people rarely abuse via the internet. Instead, they use the newsgroups to swap pictures and lurid tales. In most cases, the paedophiles are members of the child's family. Although they may use chat rooms to talk to children, they do not usually recruit youngsters for their dreadful practices via the internet. There has been one famous case of a Disney employee who used the internet to meet a 13-year-old girl for sex. However, the girl did not exist – she was the pretence of the FBI, who promptly arrested the man[xviii]. The rare nature of this event made the case an international news item. Yet in reality the chances of young girls agreeing to meet men they have never seen, just for sex, seem remote. Clearly it is possible, but extremely unlikely. Indeed, many of the victims of paedophilia are too young even to use the internet – some sickening pictures of sexual abuse of babies circulate amongst paedophile groups. So, even though paedophiles have taken to the internet – instead of lurking outside school playgrounds with a bag of sweets – the chances of your child being approached or abused by them is extremely slim indeed.

Taking a sensible approach

It is clear that although there is a great deal of potential for damage to children on the internet, the chances of it ever happening are slim. The media hype about some of the dangers has blown out of proportion the true risks. True, there are problems and difficulties, but children only rarely encounter them. Even if they do view unsavoury sites, psychological research would suggest that the potential for damage is negligible of parenting is good. What all of this research tells us, combined with studies of the internet itself, is that if you are aware of the dangers and are a good parent, your children are safe to use the internet and gain the maximum value from it – which for most of them is simply helping them do their homework.

Chapter 3

Making the internet safe and fun

The internet is such a fantastic resource and such an educational storehouse it would be almost criminal to deny children as much access as possible. For this reason it is important that the internet is treated as 'normal' and not some dangerous territory. Psychologists would tell you that a child would associate your emotional reaction to viewing something on the internet with the internet itself. If you display negative, fearful reactions it is possible you will condition your child to dislike, even fear the internet. For an explanation of how this could occur go to:

http://www.as.wvu.edu/~sbb/comm221/chapters/pavlov.htm

However, how can you treat the internet and everything you see on it as 'normal' and 'fun' if your own experience and understanding is limited? For this reason it is essential that parents learn as much as they can about the internet. This will have a dual effect – you will not pass on any negative reaction to your children, plus you will be able to protect them from the nastier aspects, as you will know about them.

Learning more about the internet

The number one rule for parents trying to protect their children online is to learn as much as they can themselves about the internet. In this way you will be able to help your children explore this world in safety. If you don't know much about the internet, the chances are your youngsters will soon learn more than you, and will be able to outwit your feeble attempts at control. Happily there are plenty of resources you can use to learn more.

You could start with a book. Try:

Using the Internet, by Graham Jones, published by How To Books.

This is a slim paperback that provides everything you need to know about the basics of the internet. Alternatively, if you are already a confident internet user, you can find out more using various resources online. Some of the places you might like to visit include:

An Introduction to the Internet for Teachers

http://www.massnetworks.org/~nicoley/tutorial/index.html

Internet 101

http://www2.famvid.com/i101/internet101.html

Learn The Net

http://www.learnthenet.com/english/index.html

The Web Adviser

http://www.the-web-adviser.com

Web Monkey Guides

http://hotwired.lycos.com/webmonkey/guides/

For a list of other useful learning resources go to:

http://www.rgu.ac.uk/schools/sim/research/netlearn/callist.htm

Once you have used these web sites to gain a greater understanding of the internet you'll be in a much better position to help your children. Take a tip from youngsters as well. They have few fears; most are developed as a result of their social environment. This means that they are not afraid of the internet unless someone else makes them believe it should be feared. Equally, they are not afraid of using computers, unless they are told to be careful. Adults, on the other hand, have developed irrational fears about many things. Often we are frightened of using computers, experimenting with software programs, or exploring the internet. Those fears are often developed because we worry about what might happen if things go wrong. Children, however, have grasped that they will only learn if things do go wrong – they see mistakes and errors as an inevitable part of learning. So, don't be afraid of trying everything – few things can go wrong, and even if they do they can always be rectified. So get stuck in and have a go – after all if you don't your children will!

Setting the ground rules
The internet is like a street corner. At your local street corner you can talk to other people, find out about various facts and observe the rest of the local world and so on. You can also buy drugs or create weapons and plot crimes. That's why you have rules about your children and street corners. That's why you have 'curfews' and rules about the kind of people you don't like your children mixing with. Good parents establish a framework for safe and happy development. The internet is no different to your local street corner – sure it's much more exciting and dynamic, but essentially it's much the same. So, make sure you establish the same kind of ground rules that you already have for your children and they way they live their lives in the physical world.

Your internet rules might incorporate the following:

- Times at which internet connections are allowed and not allowed
- Maximum duration of internet usage
- Type of material that is allowed
- Type of material that is off limits
- Whether children should be 'accompanied' by a parent when online

No doubt you may have other rules or not use some of these, depending upon your own youngsters and their age, but you should at least have some rules. Otherwise your children will go roaming anywhere they please as often as they like – something you would doubtless not allow for the local street corner.

Making the internet a family activity
One excellent way of making sure the rules are used is to enjoy using the internet together. This is only really an extension of getting your children to enjoy the physical world – after all, you probably go swimming as a family, go on picnics together, see the local football club in action with your youngsters, take bike rides together and so on. So why not enjoy the internet together? This will help you control internet usage and also monitor what your children are doing online. However, it can be impractical if you have a small computer screen, as you will not be able to see everything clearly. For this reason it's an excellent idea to upgrade your computer for improved access. To do this you'll need the following:

- Large monitor (preferably 19 inches)
- Cordless keyboard
- Cordless mouse

These extras will make it much easier for you all to enjoy one computer together. You can buy such extras online, some good places to check are:

Action

http://www.action.com

Jungle

http://www.jungle.com

PC World

http://www.pcworld.co.uk

You can also buy sophisticated equipment that allows you to monitor what is happening on one computer, from another machine. Such extras can be found at:

http://www.dakota-euro.com/

Check out your service provider

Most internet service providers are just great. Some are not good for children though, since they allow access to every corner of the internet, including some of the murkier newsgroups that the police would like to see banned. You might like to check to find out if your service provider is 'family friendly'. The first step in doing this is to find out if your provider is a member of the Internet Service Provider Association. You can find a list of members at:

http://www.ispa.org.uk/members.htm

If your service provider is a member, it will have to conform to certain rules that require it to make sure that anything it provides is legal. Being a member of the ISPA does not mean your children won't be able to see anything nasty, but it is a good starting point. For instance, if anything horrible is located on one of the web sites provided by an ISPA member, they are required to act – often shutting down the problem site.

Whether or not your service provider is a member of the ISPA, go to the home page of the company you use. This will usually be in one of these forms:

http://www.yourserviceprovider.co.uk

http://www.yourserviceprovider.net

Once you have arrived at the appropriate site, check for the terms and conditions and privacy agreements. You may need to search for these, but usually they should be prominently displayed. Check these items of 'small print' carefully – you want the service provider to offer you the following:

1. A clear statement that your identity will not be revealed to third parties

2. An unambiguous declaration about offending sites

For example, Virgin Net requires anyone publishing a web site on its servers that contains material likely to offend to have a warning page as its first page. If no such warning page exists and the site is likely to offend, Virgin will shut the site down. This is precisely the kind of 'terms and conditions' that you want your 'family friendly' service provider to publish.

Having checked out the terms and conditions, you may want to find out if your service provider has been tested independently. You can do this by going to:

http://www.ispreview.co.uk

This site provides reviews of all the service providers as well as a host of other information that you may find useful. What you learn at this site could help you decide whether it's acceptable to continue using your current service provider, or switch. Two service providers that have in-built parental controls are:

- AOL

- CompuServe

Both of these companies allow you to set up the service so that it allows you to block certain material from being accessed by your computer. These systems are password controlled, so make sure you choose a password you can remember but which will not be obvious to your children. You would be surprised how many people choose their name, or date of birth as passwords – both of which you children would use as 'guesses' within seconds! The best passwords are abstract and include numbers as well as letters.

Setting up a computer password

You can control your child's access to the internet even more rigidly by password protecting your entire computer. In this way you make sure they can only access the internet when you are around, able to supervise. There will be different ways to set up passwords depending upon the type of computer you

use and the operating system. However, most people will be using a version of Windows. Protecting the computer and limiting access is best done with Windows 2000. Although Microsoft has aimed this at the business market, it is not difficult to use and works on most modern computers. You can download a program to check out the compatibility of Windows 2000 with your machine from:

http://www.microsoft.com/windows2000/upgrade/compat/default.asp

If you can use Windows 2000, so much the better, since it will enable you to provide sophisticated controls over who uses your computer and what they can do with it. However, Windows 2000 does not come with a comprehensive manual. You will need a good guide to using the program if you are to control security well. You can obtain such a guide from:

http://www.amazon.co.uk/exec/obidos/ASIN/0764503405/grahamjones

If you have Windows 98 you can set up a password to protect the entire computer by choosing 'Passwords' in the Control Panel. If this does not exist, your computer may not have been set up with password recognition required. If that is the case, you need to re-install Windows 98 again, this time entering a password for the computer when requested. If that seems like too much trouble, download a 'shareware' password program. You can get a variety of suitable programs from:

http://www.softseek.com

However, one of the best, having won several awards, is 'Security Administrator'. You can download this from:

http://www.softheap.com/secagent.html

Monitoring your computer usage

One way of making sure your children stick to the straight and narrow is by letting them know that you are keeping your eye on them! You can do this automatically thanks to the way the internet itself works. Whenever you access a web page the files that are used are downloaded to your machine. In addition, an historical database is stored, showing your movements around the internet. You can check which files have been downloaded and which web sites have been accessed, simply by looking at these index files. How you do this will depend upon which internet 'browser' program you use.

If you have Microsoft Internet Explorer it is straightforward. In the toolbar at the top of the screen you will see the 'history' button. This will show you a list of all the web sites that have been accessed. You can alter the time period the history is kept, up to a maximum of 99 days. To do this, choose 'Internet Options' from the Tools menu and alter the number of days in the 'History'

panel. With Microsoft Internet Explorer you can also check the files that were accessed by looking at the stored materials. To do this, go to the Tools menu and choose 'Internet Options'. Then click on the 'Settings' button. This will pop up a new box, in which you will see a button labelled 'View Files'. Click on this and you will be presented with a list of all the files accessed.

If you have Netscape Communicator, the procedure for checking is slightly different. To check the list of web sites that have been accessed, choose 'History' from the Tools command of the Communicator menu. To view the files that have been accessed you will need to go to the 'Users' folder which should be in the Netscape folder which is inside 'Program Files'. Within the Users folder you should find another folder with the user name you selected when you installed Netscape. Open that folder and then open the 'Cache' folder; this will then show you all the files accessed. You can change the amount of information stored by the Cache and by the History by going to 'Preferences' in the Netscape Edit menu.

If all of this seems complicated, consider using the program 'Cyber Surveillance'. This allows you to keep a complete 'slide show' of everything you children do on the internet. You can then view this to check what they did. The program is password protected and automatic, so provides a complete policing system for your youngsters. You can find out more at:

http://www.intelliquis.com/products/cyber.stm

Ringing the warning bells

It is worthwhile remembering that if you can check the history and look up files that have been accessed by your children, they can do the same to you. It is perfectly possible that you will access sites when you use the internet that you would not like you children to see. For this reason it is important that whenever you use the internet you clear out the stored files and delete the history – otherwise your children could look at those sexy pictures you were admiring last night! Both Microsoft Internet Explorer and Netscape Communicator allow you to clear the histories and empty the stored files directories. However it is quite cumbersome. No parent should therefore be without 'Window Washer'. This is a shareware program that allows you to delete – permanently – files and history logs that you no longer wish anyone to access. You can find out more about Window Washer at:

http://www.webroot.com/washer.htm

You can also download a copy of the program from this site, though registration costs $29.95.

Setting up a privacy system

One of the concerns about children using the internet is the fact that they can be targeted by 'spam' – unsolicited bulk emails. Often these emails contain sexual images and the senders have no idea of the age of the person who will receive their message. However, the lists these companies 'harvest' will not include your child's email address if you have some simple rules about online privacy. These should include:

1. Never give your name and email address to anyone you do not know

2. Never give personal details out over a chat room system

3. Never agree to meet anyone who contacts you via the internet unless a parent is also present at the meeting

You can also use encryption programs to further enhance your email security and that of your children. This will ensure that 'snoopers' online cannot read your details. There is a variety of suitable programs that can be bought from software shops, online and in the High Street. These programs include:

- Norton Internet Security

- Pretty Good Privacy

You should also invest in a digital signature that enables you to pass on emails to trusted individuals in an encrypted form so that other people cannot view them. You can get more details about digital signatures at:

http://www.trustwise.co.uk/welcome.html

Using child friendly sites

Another weapon you can use to ensure that your children enjoy the internet is encouraging the use of child friendly sites and regions of the internet. There are a number of services that now check out the material that is offered and only allow access to material that is of value to youngsters and which has little likelihood of harm. The services you might like to check out include:

http://www.kzuk.net

http://www.yahooligans.com

http://www.freezone.com

A list of child friendly regions of the internet can be found at:

http://www.cyberangels.org

Making sure you all have fun

Using the simple measures outlined in this chapter you can be sure of having a super internet experience that allows you and your children to be safe and avoid any obnoxious material. However, there is even more you can do to make sure that children are kept protected from danger on the internet. You can alter your browser settings to increase the protections available and you can obtain filtering software to block unwanted material. These options are covered in the following chapters.

Chapter 4

Limiting your children with your web browser

Your web browser provides you with a range of measures that you can use to help you ensure your children avoid seeing dubious material on the internet. You can use these measures to:

- Increase privacy and protect your child's identity
- Prevent some web sites from being displayed
- Arrange encryption to provide greater security

The most secure web browsers are usually the most recent versions. That's because any security 'holes' found in previous versions have been plugged. Web browsers undergo constant development and each version is updated on a regular basis. You can expect updates and 'patches' on a monthly basis. If you do not keep your web browser up to date, your risk your child either being able to access dubious material, or have their privacy invaded. Make sure, therefore, your web browser is up to date. To check, go to one of the following web sites, depending upon your chosen browser:

Microsoft Internet Explorer

http://www.microsoft.com/windows/IE

Netscape Communicator

http://www.netscape.com/download/index.html?cp=djudep2

You can also check for periodic updates or patches to each version of the main browsers at the following sites.

Microsoft Internet Explorer

http://windowsupdate.microsoft.com

Netscape Communicator

http://www.netscape.com/smartupdate/index.html?cp=dowdep1

It is a good idea to make updating a regular part of your 'housekeeping' so that you can be sure your computer offers you the best protection. If you need a regular reminder you can download a suitable program from:

http://www.mousehook.com/dforget.htm

Here you can obtain 'Don't Forget', a simple reminder program that pops up a window and plays a sound to remind you of specific events, such as when to update your browser software.

Increasing privacy with web browsers

One of the particular problems facing children on the internet is that their identity can be discovered. Although the risks are small, there are problems associated with the non-privacy of information about children. Cases are rare enough to make headlines and one incident happened at the end of April 2000 when a vigilant mother prevented her 13-year-old daughter from falling into the clutches of a middle aged man, who had pretended he was a teenager[xix]. Even when confronted the 47-year-old 'cyberstalker' suggested he was only 17. Such encounters can occur when criminals realise they are dealing with a child, rather than an adult. Web browsers can give information away that allows such cyberstalkers to know email addresses and so on, providing them with a way of getting in touch. For this reason, you need to ensure your web browser does its utmost to protect you.

You can discover what other people can find out about you at the following web site:

http://www.anonymizer.com

Click on the word 'you' just below the 'Who are you' heading. Within a minute or so you will get a report back, which identifies the following information about your computer:

- Your computer's name
- The size of your screen

- The date and time showing on your computer
- The number of web pages you have visited today
- The exact route of your connection
- Your email address
- The kinds of files your computer is equipped to accept
- The telephone number of the people who own your network

You can also go to

http://privacy.net

to find out similar information and a host of other details. Some of the information that is made available to others is produced via your web browser. In order to make sure that your children are kept free from any possible predators, you need to secure your web browser. To do this you can subscribe to the Anonymizer service to allow anonymous web surfing. However, this does not help protect your children in newsgroups or email systems. Hence you do need to enhance your browser.

Making Microsoft Internet Explorer more private

As with most software programs, Microsoft Internet Explorer has to make compromises. The program is set up automatically with what Microsoft believes will be the 'average' user's requirements. Few of us are 'average' so we need to change the default settings. In Microsoft Internet Explorer the default privacy settings are not that private – that's because Microsoft appears to have assumed that many people want their information broadcast. This may well be the case in the business world, but is not what you want at home when your youngsters are surfing the web.

Changing the settings on Microsoft Internet Explorer is relatively straightforward. Apart from one item, everything you need to change is within the Internet Options command from the Tools menu.

The first thing to do is to set the 'History' levels. Alter this from the default seven days to zero. This will prevent automatic data collection systems from finding out too much about your browsing habits. However, the downside is that you will not be able to use the 'History' feature of the program to go back to pages you viewed recently. For this reason you need to save the details of

any page you might want again as a ‘favourite’. Although you can do this within Microsoft Internet Explorer, it means snoopers could read the data. So, save your favourites and history in another program. One of the best is called the Universal Bookmark Manager and you can download a copy from:

http://www.cdml.com/OurSoft/ubm.htm

Having decreased the amount of information people can obtain from your browser’s history, you now need to limit the material you collect and which could be identifiable. To do this, click on the Settings button in the Temporary Files section of Internet Options. Reduce the amount of disk space you allow to about half of what is set up. This will prevent too much material being stored on your machine.

Now click on the Security tab in Internet Options and select ‘Custom level’. Scroll down until you see the Cookies section. If the computer is only used by your children you can disable all cookies. However, if the computer is used for your work or you shop online, you will need cookies, so change the setting to prompt. You can then teach your children to refuse cookies when they are prompted, though you can choose to accept them. Cookies are small pieces of code that are stored on your computer and can reveal your identity and your browsing habits. If you find you use a number of legitimate sites that require cookies, you can use another piece of software to ensure you only have the cookies you need. This is called ‘Cookie Pal’ and you can download this from

http://www.kburra.com/cpal.html

The program allows you to accept cookies from the sites you want and also block cookies from unacceptable web sites.

Having sorted out cookies and while you are in the Custom Level security settings, scroll down to the bottom of the list and change the ‘Log On’ options to anonymous. This may prevent you from accessing some password-controlled sites, but will be of general help in increasing your privacy.

If you need to log on to password protected sites, you can do so by making sure that your security setting is on Automatic Logon only in Intranet Zone. You will then be prompted for passwords as needed, rather than being rejected by the site.

Having completed these tasks, there are just two more privacy tasks to undertake. These are both found in the Personal Information section of the Content tab in Internet Options. Click on the Auto Complete button and deselect ‘User names and passwords on forms’. This will ensure that all passwords have to be entered and will help you be certain that passwords are only entered when you are around. In this way you can monitor access and

also make certain that you are entering sites that are not likely to be invading your privacy to any great extent – which might be the case for a chat room, for instance.

The final privacy setting is the My Profile section. Just make sure that each section has no entries whatsoever. You will need to put a blank space in for the name; otherwise you cannot close the My Profile section. However, once you do, the amount of information available to any snoopers is considerably reduced.

Ensuring your email address is kept secret

Once you have completed the privacy tasks for Microsoft Internet Explorer you should also pay some attention to your email system. This is because your email address can be sent via your browser to people who request it, even though you do not send them an email. To be sure that this doesn't happen, make sure your email program does not have a 'reply to' address. Anyone you send an email will be able to reply, as your address will be sent with your message. However, the address cannot be found by online snooping activities.

Another way of keeping email addresses secret, particularly those of your children, is to use nicknames rather than real ones. Also don't use age identifiers or anything that shows the email address belongs to someone other than an adult. It's also worthwhile explaining to children that they should only give out their email address to people they know and trust – anyone else should require your permission. If you want to make sure your children are even more protected you can use a new service from Zero Knowledge Systems that provides the highest level of privacy available anywhere. You can find out more at:

http://www.zks.net

Using privacy settings in Netscape Communicator

Netscape Communicator has fewer privacy controls than Microsoft Internet Explorer, yet you can still be comparatively private. The settings you need to change are in the Preferences command on the Edit menu. Select 'Navigator' in the panel on the left and make sure the History expiration is set to zero. Then select Identity in the Mail and Newsgroups section in the left panel. Clear any entries so that you become anonymous. Now select the 'Advanced' options in the left hand panel and click for warnings when cookies arrive. You should also click on the Cache option under Advanced and reduce the cache size by about half.

Preventing browsers from displaying certain web sites
Although in their early stages, web browsers now include rating systems, much like video age categories. These are used by web sites to alert you to material and whether or not you might think it is suitable for children. The driving force for such rating systems is PICS – the Platform for Internet Content Selection. This uses a system that enables web developers to add small pieces of code that signal to web browsers the type of content that will be displayed if the page is loaded. Naturally, the system depends upon web developers actually using the PICS system and being honest. However, PICS is run by W3C the 'World Wide Web Consortium'. This is the organisation that sets the protocols for the operation of the web; these are not hard and fast rules, but the web industry tends to adhere to them. As such, therefore, PICS is run by an organisation that is central to the success of the web and carries some weight as a result. You can find out more about PICS at the following web site.

http://www.w3.org/PICS/

However, on its own, PICS will not help you. You need to set your browser to pick up PICS data, interpret it and let you know the rating of the material on offer. To do this you need to change the settings on your web browser.

Using PICS settings in Microsoft Internet Explorer
To enable PICS settings in Microsoft Internet Explorer you need to visit the Internet Options, available from the Tools menu and select the Content tab. Click on the Settings button and you can then adapt the various rules to your own requirements. Microsoft Internet Explorer comes with the Internet Content Ratings Association (RSACi) system for rating web pages. You can find out more from:

http://www.icra.org/

However, you can add other ratings systems if you wish, since some web sites would choose to register with other organisations. You can go to the following web site to add further ratings systems to Microsoft Internet Explorer.

http://www.microsoft.com/windows/ie/ratings.asp

One of the other main suppliers is Safe Surf. This can be found at:

http://www.safesurf.com/

You can add this to Microsoft Internet Explorer to provide even greater control. An automatic system for doing this is available at the Safe Surf web site.

Using the Content Adviser section of the Internet Options panel in Microsoft Internet Explorer means you can limit the type of web material that is viewable by your children. You can also boost the system by adding approved sites to a list. However, there are two problems when using rating systems in browsers. The first is that many sites are not yet rated and there is no compulsion for them to do so – hence you can easily miss many sites. The second problem is that it can slow you down or stop adults from viewing legitimate sites – the only way out of that is to change the Internet Options settings each time you use the computer. That's not very practical, so it may be easier to get the children their own, restricted use computer.

Changing the ratings settings in Netscape Communicator
To set up Netscape to adopt ratings you need to go to the following web site:

http://home.netscape.com/communicator/netwatch/

You then click on the set up button and follow the instructions. Netscape's NetWatch system uses the RSACi and the Safe Surf ratings systems.

Arranging encryption to enhance security
Encryption is the process whereby data from your computer is scrambled and can only be read by another computer that is capable of deciphering the mess. This system means that many people who might be able to find out about your children and their online activities would be prevented from knowing anything.

For children who simply use the web, you can arrange encrypted browsing using the Anonymizer service:

http://www.anonymizer.com

If you sign up for the service, you can browse the web and no one will know where you have been or who you are. The Anonymizer programme costs less than $50 a year so could well be worth it for the sake of your children.

However, this form of encryption is only suitable for web surfing. For using newsgroups or email, you would need some other forms of encryption to code the information being sent by your children. Anonymizer does have an email system that provides privacy, but it can take up to two days for messages to

be sent – hardly useful. To gain the most from the Anonymizer encryption system you need to use the company as your Internet Service Provider, which is only available to people in the USA. If you want full encryption protecting all aspects of your child's activity online you need Freedom from:

http://www.freedom.net/

This provides encryption of all the information leaving your computer. You can also buy encryption programs that code all the material leaving your computer. Popular ones include:

Absolute Security

http://www.pepsoft.com/absec/intro.html

Data Safe

http://www.authentix.com

Norton Internet Security

http://www.symantec.com/sabu/nis/index.html

Pretty Good Privacy (PGP)

http://www.pgp.com/asp_set/products/tns/intro.asp

Adding a digital signature to your browser

A further enhancement to your browser is a digital signature. This allows you to encrypt data sent from your computer via email. You can add a digital signature via the following web site:

http://www.trustwise.com/welcome.html

All you need is a 'Class 1 Personal Certificate' and you can add encryption to your email and browser. You will need to import the certificate into Microsoft Internet Explorer or Netscape Communicator. Full instructions for doing this are provided when you sign up for the Trustwise service.

Improving security in newsgroups you're your browser
One of the best ways of allowing your child to view newsgroups anonymously is to ensure they do not use a newsreader program, like Outlook Express. Instead, get them to access the newsgroups via a service like Deja. This ensures your child's email address remains hidden from others. You can access newsgroups at:

http://www.deja.com/usenet_home.epl

However, every newsgroup is available – unlike some British Internet Service Providers who block some sites, Deja allows them all. This means although your child can remain anonymous and send messages using encryption, they can also access many newsgroups you would rather they avoided. To gain complete control over newsgroups you need to sign up to use the internet with AOL. You can download the special AOL browser from:

http://www.aol.co.uk/try/

Even so, the safest way for youngsters to use newsgroups is with a parent present. Encouraging good web surfing and selecting appropriate sites is ultimately more beneficial.

Thinking about your browsing habits
Whichever internet browser program you use, the security and privacy options available are limited. You will restrict your children somewhat, but not completely. If you use all the methods outlined in this chapter to their full extent you will also restrict an adult's use of the internet. For this reason you may need to consider using two different browsers – not two copies of the same browser. You can then set up one browser with rating systems and high security measures for use by children. The other program can then be restricted to adult use. You can ensure this happens by password protecting the 'adult' browser and the folders associated with it. To do this you can use a password program – many are available at:

http://www.softseek.com/Utilities/Encryption_Security_and_Passwords/Security_and_Access_Control/

Chapter 5

Using Specialist Software to Set Boundaries

One of the ways in which you can improve online security for children is to buy a separate program that acts as a filter. With varying degrees of success these programs can prevent unsuitable web sites from being displayed, thus helping to ensure your youngsters do not view anything that is potentially damaging. However, it is important to remember that such filter programs are no substitute for real parental controls; neither are they completely successful – sometimes they can prevent your children from successfully completing their homework as they can block out appropriate sites. Setting up these filtering programs can also take some time and often you need constant maintenance to ensure that sites continue to be blocked. Whilst they are an excellent idea and will be very useful to many parents, these filtering programs should only be seen as part of the solution to internet safety for children, not the complete answer.

The filtering programs available include:

- Cyber Patrol
- CYBERsitter
- KidDesk
- Net Nanny
- Norton Internet Security
- Surf Watch

Using Cyber Patrol

Cyber Patrol is a comprehensive program providing filtering capabilities for the entire internet, not just the world wide web. You can find out more at:

http://www.cyberpatrol.com

The core of the program is the concept of a CyberLIST. There are various lists but there are two of particular interest to parents:

1. Cyber Patrol Kids' List
2. CyberNOT

The Cyber Patrol Kids' List is set up by parents or teachers to guide youngsters to the most appropriate sites. You can add various web sites to the Kids' List, or even remove some of those suggested by the program. In this way you can create a customised list of suitable web sites.

CyberNOT is a regularly updated list of web sites that cannot be accessed when Cyber Patrol is running. These are completely blocked by Cyber Patrol. However, you can adjust the degree of filtering and apply different filters for up to nine different users. In this way you could block all sites that contain any degree of sexual material from an infant school child, but allow teenagers, say, to be able to see sex education material, but not pornography. As a result, Cyber Patrol is an excellent tool for providing parents and teachers with a good degree of control for when they are not around. In addition, Cyber Patrol has a timer facility that limits a child's overall time spent on certain kinds of sites, or the internet as a whole. This could be useful if you would rather your child complete their homework, rather than spend hours chatting online! According to ZD Net – an online review service – Cyber Patrol is the most comprehensive filtering program of its kind[xx]. However, it does take some set up time and you need to pay an annual fee to keep using the updated CyberLIST service.

Controlling access with CYBERsitter

CYBERsitter is an award-winning program and unlike some similar internet filters, you do not have to pay an annual fee. One of the reasons for the award is probably the fact that CYBERsitter filters out much more than pornography or violence. For instance, you might think your child has just had too much of Pokemon and CYBERsitter would allow you to do just that as you can block sites containing any words you like. Another advantage of CYBERsitter is its varying degrees of blocking – you can either completely block particular sites, allow them to be seen but provide you with a report of when they were viewed and for how long, or simply provide you with an alert that particular sites were requested. In this way you can control older children who may not appreciate a heavy-handed total block approach but would limit their activities, as they would know they were 'being watched'. Another advantage of CYBERsitter is the fact that it supports the World Wide Web Consortium's PICS system of rating web sites. This impressive array of features has made CYBERsitter the 'Editor's Choice' of PC Magazine[xxi]. As if this were not enough to recommend it, CYBERsitter only takes a minute to install and supports all forms of Microsoft Windows and all the main web browsers, including that from AOL.

One other useful feature of CYBERsitter is the fact that it also blocks

unsuitable material leaving your computer as well as entering it. In this way you can prevent your children from submitting dubious email messages themselves or even using words in chat rooms that you would rather they didn't!

If you want to know more or download a trial copy, go to:

http://www.solidoak.com/cyberinfo.htm

Deciding how to use KidDesk

KidDesk Internet Safe is not exactly a filtering program, but it provides a means of filtering out material you would rather they did not see. The program works by you constructing a 'desktop' that is suitable for your particular child. On this desktop you place all the internet sites you elect for them to access. In this way they can only go to parts of the net that you already approve. In addition, because KidDesk uses its own desktop, your youngsters can't fiddle with the remaining computer settings – helping boost your system stability and your privacy. The problem with KidDesk is that you have to act as the filter – deciding what's appropriate or not. At the same time, your children could access unsuitable sites, as they may be able to be led through various links from the sites you choose. The whole point about the web is it's non-stop spreading nature – the 'world wide web'. Choosing suitable sites may be fine, but the nature of the web means that children could click through a range of links to visit somewhere nasty. You can find out more information about KidDesk at:

http://www.edmark.com/prod/kdis/

As you will see on this web site the screen shots of KidDesk are 'junior' and would be resented by older children. As a result KidDesk would probably not be suitable for teenagers.

Making the most of Net Nanny

Net Nanny is one of the most well known internet filtering programs and is extremely popular. However, according to the reviewers at PC Magazine, Net Nanny is quite difficult to set up, leading to the possibility that no blocking would occur at all[xxii]. This should be cleared up when a new version is produced, however if you buy or download anything less than Version 4.0 you could face the same difficulties as the PC Magazine reviewers. Even so, Net Nanny is widely reputed as being able to block almost anything. The program monitors all internet activity, not just web browsing, and blocks anything that a parent or teacher decides is inappropriate. Net Nanny also provides a list of unsuitable sites that you can adapt or add to. In addition you can set the

program up so that it only allows access to your list of predetermined sites. This means that even if a child clicks through to an unsuitable site, it will be blocked, as it is not on your suitability list.

An added benefit of Net Nanny is the fact that it also provides privacy options, allowing you to prevent your child's email address, for instance, from being distributed. You can also set up Net Nanny with different levels of filtering for up to 12 different children, or classes. You can find out more at:

http://www.netnanny.com/

You will find Net Nanny particularly useful if your child visits a lot of chat rooms, since it can block information in two directions. This will help ensure you child 'behaves' on line and also maintains their privacy. If you want to find more information on behaving on line, see the following web site for a discussion of 'netiquette':

http://www.albion.com/netiquette/

Using Norton Internet Security

Norton Internet Security provides much more than filtering software for children. The program provides virus protection and a range of other features including a 'firewall' to protect your computer from attacks by anyone connected to you via the net and privacy settings. As such, Norton Internet Security provides complete protection. Part of that fortification includes filtering software to prevent your children from accessing certain parts of the internet. Computer Shopper magazine reviewed the package and claimed one of its advantages was the fact that you could completely block particular kinds of internet activity, such as entering chat rooms[xxiii]. However, the filtering system for blocking web sites was seen as a shotgun approach – sometimes blocking out suitable sites. The more refined approaches of the dedicated filtering programs may therefore be more suitable.

Norton Internet Security comes with a year of updates and is backed by the Norton Antivirus software, one of the leading antivirus products. For this reason you may wish to use the program to provide that all round protection. You can find out more details at:

http://www.symantec.com/sabu/nis/index.html

Gaining protection with Surf Watch

Surf Watch is another filter program that blocks sites according to word patterns. However, the core of the program blocks only a limited range of

material such as sexually explicit material, violence, hate, gambling and drugs/alcohol. This means that anything else you need to add to the customisation filters, which could be a long job. Even so, Surf Watch is regarded as a highly usable and has received a range of awards for its tough filtering capabilities. An added feature of Surf Watch is the fact that it comes in a 'professional edition' that can be used by system administrators to set up filtering. This means the product is excellent for use in schools where small networks exist. Find out more at:

http://www.surfwatch.com

Comparing the programs
You will find a useful comparison of a range of filtering programs at:

http://microweb.com/pepsite/Software/filters.html

This web site lists all the main programs, compares the features and provides links to the publishers. You can also compare the various programs by downloading demonstration versions from the various web sites. In this way you can test them to find out which is best for you and your children. Only test one at a time, otherwise you will not be able to work out which filter is actually blocking anything. Once you have installed one of the demonstration programs, try visiting a web site that you know has content you would rather a child did not see. You could try the following sites, for instance:

http://www.sexworld.co.uk/

http://www.heinnie.com/

http://www.williamhill.co.uk/

If your test filters block these sites you will have effectively curbed your child from looking at porn, at knives and at gambling opportunities. You will want your tests to be more rigorous, of course, but you should check similar sites to these. If your filter program does not block these sites, you may need to adjust the settings; doing this will enable you to see how 'user friendly' the program is. Once you have selected your preferred program, set it to use, buy the full version and make sure you know how to use it.

Using age verification systems
Another way of limiting use of the internet is an age verification system. Many 'adult' sites use this method to prevent children from accessing their pages. Essentially you need to prove you are an adult to an independent age

verification system. You are then issued with a password that the adult site checks before giving you access to the material within. Whilst this is a great idea and works well, many sites do not require age verification. Hence, there is a considerable amount of material that children can gain access to, since no password entry is required. There are many different age verification systems, but you can find out more about the world's largest system, Adult Check, at:

http://www.adultcheck.com/

You may wish to obtain an age verifier for yourself. In this way you can surf adult sites and your children would be unable to visit any of your pages stored in 'History' or as 'Favourites' unless they knew your age verification password. This does not provide complete protection, but is added insurance if you do visit adult material on the web.

Using other software to set limits

You do not have to use a commercial program to set limits. There are plenty of shareware offerings available to curb your child's activities. You can, for instance use a logging application to check up on your youngster's surfing activities. You can find possible programs at:

http://www.softseek.com/Utilities/Encryption_Security_and_Passwords/Usage_Monitoring_and_Logging/

You can also use various web access controllers, found at:

http://www.softseek.com/Internet/Web_Browsers_and_Utilities/Privacy_and_Access_Control/

Whichever program you use to set limits for your children, though, it is important to remember they are only part of the answer to the problem, not the complete solution. You need to use all of the other features and enhancements mentioned elsewhere in this book. Do not rely on filtering programs in isolation. They cannot and do not block every unwanted activity on the internet.

Chapter 6
Finding out more about protecting children

One of the strengths of the internet is its speed and its ability to disseminate a message to a wide audience. In the past, parents would often have to rely on gossip and chance meetings to be able to find out about local dangers to children. Now, with the internet there is a real opportunity to keep up to date on all matters of child protection. Indeed, you can use the internet to contribute to the debate and report worrying incidents to help warn other parents or teachers. The internet provides you with a range of opportunities that were not easily available in the past. These include:

- Finding out about problems that face children
- Learning about ways to protect children
- Publicising situations that are potentially harmful
- Providing advice to children themselves

Looking up the latest information

The internet may be stuffed full with pornography, violence and the like, but it is also policed by a dedicated group of volunteers as well as government agencies. The result is that information on areas of concern is publicised almost as soon as the problem arises. In addition, any illegal or completely vile web sites are switched off by Internet Service Providers shortly after they go live. In this way, the internet is being cleaned up constantly, though it will never be completely free of problems. No one person or agency owns the internet; anyone can connect to it at any time and publish anything they like. This is why you need to keep constantly aware of what's going on. Using some of the following web sites will be of help.

CyberAngels

CyberAngels is a spin off from the American protection organisation, Guardian Angels. You can see the comprehensive web site at:
http://www.cyberangels.org/
CyberAngels is the world's largest online safety organisation and its web site should be on the Favourites list of every parent and teacher. The material available is detailed and mostly up to date. However, some pages are clearly old, which does not instil confidence. For instance, the 'international' page talks about meetings that have 'just' happened – in 1998! Even so, the CyberAngels site provides more depth and more information than any other site on child safety. You will also find on this site the Net Patrol team – providing details of the volunteer 'police force' that keeps its eye on internet activities. CyberAngels also includes an online newsletter, called Trumpet, as

well as a series of links to safe sites. The only problem with CyberAngels is the design of the web site. It is cluttered and looks less professional than other sites. If you can cope with this, you will find this site invaluable.

GetNetWise
This web site is produced by the Internet Education Foundation, an American non-profit making organisation dedicated to promoting the internet as a valuable medium. GetNetWise provides concise information on child safety and has a handy glossary of terms. There is a handy list of Quick Tips as well as a directory of suitable sites for children. It's all basic information, but should prove helpful. You can check out this site at:
http://www.getnetwise.org/

Internet Watch Foundation
This is a British site and is by far the most comprehensive and most professional of all the child safety sites that provide up-to-the minute details on online protection. You should certainly make this one of your favourites:
http://www.iwf.org.uk
Of particular interest is the news section that provides the most recent details of child protection online. There are also several links and downloadable reports. Altogether an excellent site.

Kid Shield
This site is brief, but includes a series of Safety Net tips that could prove useful. There is also a news section providing the latest information. There are also some links to suitable sites for children as well as a list of filtering products. You can see this site at:
http://www.kidshield.com/

Net Family News
This site is aiming to bridge the gap between computer literate children and their not so 'savvy' parents. The idea is to provide a range of information that will support parents and teachers in helping youngsters get the best out of the internet. Because this is a news-based site, you will be able to keep up to date with everything that is going on in the world of child safety on line. You can also sign up to a regular newsletter that will be delivered via email to you. This contains the most recent information. This site is straightforward, easy to use and has plenty of links to other child safety sites. For more information visit:
http://www.netfamilynews.org/

Net Parenting
This site includes basic safety information as well as a 'book of the week' on child related issues. The information is of general help, but the design of the site is not as good as it could be. For instance, the text runs into the navigation bar. There are a few links and information on software. Providing

you enter your email address, you are also provided with a list of child friendly sites. Once you enter your email address you are subscribing to a newsletter, but you can't get to the list of child friendly sites without doing this. You can see this site at:
http://www.netparenting.com/

NetParents
The NetParents web site is another American offering providing a host of information that would be useful to any parent, no matter which side of the Atlantic they live. This site provides a range of lessons that help you and your child understand more about the internet and online safety. There is also a series of useful links to child friendly sites. The site is at:
http://www.netparents.org/
You will discover that it is professional and fast, but limited in the range of material provided.

Safe Kids
This site is a bright and breezy set of pages that provide links to a host of information and resources on child safety. Of particular interest is the series of articles and links to publications that provide information on the risks faced by youngsters online. You can find out more at:
http://www.safekids.com/index.html
This site also includes 'pledges' for parents and children. These include various rules and objectives which a parent or child signs. You can then put the documents near the computer to show your dedication to safety. This is an interesting concept and one you might find useful.

Smart Parent
Smart Parent is a comprehensive and professional site that includes the latest internet news to help you keep up to date. The site is at:
http://www.smartparent.com/
The Smart Parent site is easy to use, has a host of information and has a monthly newsletter to help you keep informed. You can also see the archives of newsletters from previous months. These newsletters are comprehensive and an excellent source of information. They are delivered each month via email and should be of real value to teachers. There is a wide range of links and information on filtering software. This is one of the better information sites around and well worth a visit.

Surf Monkey
This site is a well-designed, fast and easy to use resource that is crammed full of information. The home page provides you with the latest news, so that you can quickly see the most recent information related to child safety online. You can visit this site at:
http://parents.surfmonkey.com/

The Surf Monkey also provides a range of links and tools to help you make your child's experience on the internet a positive one.

Reporting potential problems

If you discover something untoward on the internet, knowing where to turn can be a problem. Just whom do you tell to make sure the problem is dealt with? Equally, how can you publicise the situation to warn other parents? Thankfully there are several reporting facilities that are available.

In the UK, your first stop should be the Internet Watch Foundation:
http://www.iwf.org.uk

This is run with the co-operation of the police, the government, various Internet Service Providers and a range of safety and educational organisations. The web site has a 'hotline' section that enables you to make a report about problems you discover. These problems are then investigated by the Internet Watch Foundation and resolved in a number of ways. Sometimes the Internet Service Provider blocks the offending material. On other occasions the police are brought in and make further investigations.

If you discover child pornography online you should report it directly to the police. To find out how to do this, go to:
http://www.met.police.uk/police/mps/mps/mis/ocg.htm

This page discusses the situation regarding child pornography and tells you to phone 0808 100 0040 if you want to report a problem.

Another report you should make is to CyberAngels. This site has a reporting service at:
http://www.cyberangels.org/netpatrol/index.html

You can make reports on child pornography as well as other issues that could affect youngsters.

A further site you can make reports to is SafetyEd at:
http://www.safetyed.org/

This site will use its TRACE service to help police the web and newsgroups to alert the police and other authorities to problem areas. Other child safety sites also sometimes include reporting services, but SafetyEd, CyberAngels and the Internet Watch Foundation are the three main agencies to consider, as well as the police.

If you detect a problem also report it to your Internet Service Provider who may be able to take action to block the material. It is also worth reporting it to the host of the site. To find out who this is, go to:
http://www.domainsearch.com/

Then enter the name of the problem site – leave out the 'http://www' and any text after the name, such as .com or .co.uk. In other words, just type the name, such as 'domainsearch' using the example of this web site itself. You will then get a list of all the web sites that include this name. You can then click on the information button that appears next to your problem site's address in the list. This will open up a window that discloses who owns the site and who registered the name. The details will also show where the site is hosted. You can then contact the hosts and complain.

Providing advice to children

You can use the resources of the internet to provide advice to your children so that they get the best out of the web and newsgroups. Many of the sites already outlined in this chapter, as well as those discussed in Chapter 3, provide resources that help your children understand how they can use the internet safely. In the UK, an excellent list of tips for children is provided at Child Line:

http://www.childline.org.uk/factsheets/surfing1.cfm

This provides a series of five tips for youngsters in an easy to understand format that will help them get the best out of the internet. This page also comes with a printable version, allowing you to produce a mini poster that you can pin by the computer to keep your children reminded of the best way to use the internet. You can also find some excellent tips for children at:

http://www.yahooligans.com

It is worthwhile remembering that the more your children know about safe surfing, the less control you will have to exert and the less policing you will need to perform. Hence, using these child focused resources is an excellent way of ensuring that your children help themselves to stay safe.

Chapter 7

The Online Safety Charter

You can enable the greatest family enjoyment of the internet if you adopt the following 'charters'. One is for parents the other is for children. Teachers will also find these charters useful.

The Parent's Online Safety Charter

1. Children should be warned about the dangers they face online.
2. Children should be given clear instructions to report any problems they face straight away
3. Children should be guided towards safe and child friendly sites
4. Children should be encouraged to explore and use the internet for its huge educational benefit
5. Children should be accompanied online by parents from time to time, but particularly if they are young
6. Parents should monitor their child's online activity to ensure that the 'rules' are being kept
7. Children should be prevented from certain activities by filtering and blocking software
8. Parents should keep all passwords and usernames secret and hidden from children
9. Parents should report all problem areas to the key internet policing authorities
10. Parents should keep up to date with the technology and related safety information.

The Child's Online Safety Charter

1. The internet is a great place to learn and communicate and I should get the most out of it I can
2. Some parts of the internet are not aimed at children and I should avoid

these areas if I can

3. Whenever I see something on the internet that troubles me I shall tell a parent or teacher

4. When I am online I will never give out any details that will tell people where I live or who I am

5. I will only send emails to people I know

6. I will never meet anyone I chat to online, unless I already know them and if my parents are with me

7. I will keep all my passwords secret and never tell anyone, except a parent

8. I will always try to use the sites recommended to me by parents and teachers

9. I will use the internet for a purpose and will not stay online for a long time just because I like it

10. I will tell parents and teachers about the good things I find on the internet so they can tell other children

Glossary of internet terms

……..

Access provider The company that provides you with access to the internet. This may be an independent provider or a large international organisation such as AOL or CompuServe. See also **internet service provider**.

Adobe Acrobat A type of software required for reading PDF files ('portable document format'). You may need to have Adobe Acrobat Reader when downloading large text files from the internet, such as lengthy reports or chapters from books. If your computer lacks it, the web page will prompt you, and usually offer you an immediate download of the free version.

Address book A directory in a web browser where you can store people's email addresses. This saves having to type them out each time you want to email someone. You just click on an address whenever you want it.

Adult check An age verification system that only allows the over 18s to enter adult web sites.

Age verification Commercial systems that prevent minors from accessing adult oriented web sites

AltaVista One of the half dozen most popular internet search engines. Just type in a few key words to find what you want on the internet.

AOL America On Line, the world's biggest internet service provider, with more than 20 million subscribers, and now merged with Time Warner. Because it has masses of content of its own - quite aside from the wider internet - it is sometimes referred to as an 'online' service provider rather than internet service provider. It has given away vast numbers of free CDs with the popular computer magazines to build its customer base.

ARPANET Advanced Research Projects Agency Network, an early form of the internet.

ASCII American Standard Code for Information Interchange. It is a simple text file format that can be accessed by most word processors and text editors. It is a universal file type for passing textual information across the internet.

Ask Jeeves A popular internet search engine. Rather than just typing in a few key words for your search, you can type in a whole question or instruction, such as 'Find me everything about online investment.' It draws on a database of millions of questions and answers, and works best with fairly general questions.

ASP Active Server Pages, a filename extension for a type of web page.

ASP Application Service Provider – a company that provides computer software via the internet, whereby the application is borrowed, rather than downloaded. You keep your data, they keep the program.

Attachment A file sent with an email message. The attached file can be anything from a word-processed document to a database, spreadsheet, graphic, or even a sound or video file. For example you could email someone birthday greetings, and attach a sound track or video clip.

Avatar A cartoon or image used to represent someone on screen while taking part in internet chat.

Bandwidth The width of the electronic highway that gives you access to the internet. The higher the bandwidth, the wider this highway, and the faster the traffic can flow.

Banner ad This is a band of text and graphics, usually situated at the top of a web page. It acts like a title, telling the user what the content of the page is about. It invites the visitor to click on it to visit that site. Banner advertising has become big business.

Baud rate The data transmission speed in a modem, measured in bps (bits per second).

BBS Bulletin board service. A facility to read and to post public messages on a particular web site.

Blue Ribbon Campaign A widely supported campaign supporting free speech and opposing moves to censor the internet by all kinds of elected and unelected bodies.

Bookmark A file of URLs of your favourite internet sites. Bookmarks are very easily created by bookmarking (mouse-clicking) any internet page you like the look of. If you are an avid user, you could soon end up with hundreds of them! In the Internet Explorer browser and AOL they are called 'favourites'.

Boolean search A search in which you type in words such as AND and OR to refine your search. Such words are called 'Boolean operators'. The concept is named after George Boole, a nineteenth-century English mathematician.

Bot Short for robot. It is used to refer to a program that will perform a task on the internet, such as carrying out a search.

Browser Your browser is your window to the internet, and will normally supplied by your internet service provider when you first sign up. Itis the program that you use to access the world wide web, and manage your personal communications and privacy when online. By far the two most popular browsers are Netscape Communicator and its dominant rival Microsoft Internet Explorer. You can easily swap. Both can be downloaded free from their web sites and are found on the CD roms stuck to the computer magazines. It won't make much difference which one you use - they both do much the same thing. Other browsers include Oracle and NetCaptor.

Bulletin board A type of computer-based news service that provides an email service and a file archive.

Cache A file storage area on a computer. Your web browser will normally cache (copy to your hard drive) each web page you visit. When you revisit that page on the web, you may in fact be looking at the page originally cached on your computer. To be sure you are viewing the current page, press **reload** or **refresh** on your browser toolbar. You can empty your cache from time to time, and the computer will do so automatically whenever the cache is full. In Internet Explorer, pages are saved in the Windows folder, Temporary Internet Files. In Netscape they are saved in a folder called 'cache'.

Certificate A computer file that securely identifies a person or organisation on the internet.

CGI (Common Gateway Interface) This defines how the web server should pass information to the program, such as what it's being asked to do, what objects it should work with, any inputs, and so on. It is the same for all web servers.

Chat talking to other people live online by typing into a special web page window. You can see the replies of others and take part in a group 'conversation'.

channel (chat) Place where you can chat with other internet chatters. The name of a chat channel is prefixed with a hash mark, #.

click through This is when someone clicks on a banner ad or other link, for example, and is moved from that page to the advertiser's web site.

Client This is the term given to the program that you use to access the internet. For example your web browser is a web client, and your email program is an email client.

Closed areas Those areas of a web site that only registered users can enter.

Comic Chat A Windows client for IRC which shows chatters as cartoon characters.

Community The internet is often described as a net community. This refers to the fact that many people like the feeling of belonging to a group of like-minded individuals. Many big web sites have

been developed along these lines, such as GeoCities which is divided into special-interest 'neighbourhoods', or America OnLine which is strong on member services.

Compression Computer files can be electronically compressed, so that they can be uploaded or downloaded more quickly across the internet, saving time and money. If an image file is compressed too much, there may be a loss of quality. To read them, you uncompress – 'unzip' – them.

Content Articles, columns, sales messages, images, and the text of your web site.

content services Web sites dedicated to a particular subject.

cookie A cookie is a small code that the server asks your browser to keep until it asks for it. If it sends it with the first page and asks for it back before each other page, they can follow you around the site, even if you switch your computer off in between.

crash What happens when a computer program malfunctions. The operating system of your PC may perform incorrectly or come to a complete stop ('freeze'), forcing you to shut down and restart.

cross-posting Posting an identical message in several different newgroups at the same time.

cybercash This is a trademark, but is also often used as a broad term to describe the use of small payments made over the internet using a new form of electronic account that is loaded up with cash. You can send this money to the companies offering such cash facilities by cheque, or by credit card. Some Internet companies offering travel-related items can accept electronic cash of this kind.

cyberspace Popular term for the intangible 'place' where you go to surf - the ethereal and borderless world of computers and telecommunications on the internet.

Cyberstalker An individual who pursues you or your children using email, chat rooms and newsgroups. Often attempting to arrange a meeting with children.

Dial up account This allows you to connect your computer to your internet provider's computer remotely.

Digital Based on the two binary digits, 1 and 0. The operation of all computers is based on this amazingly simple concept. All forms of information are capable of being digitalised - numbers, words, and even sounds and images - and then transmitted over the internet.

DCC Direct client connection. Not normally recommended.

directory On a PC, a folder containing your files.

DNS Domain name server.

Domain A domain is a specific area on the internet and identifies to the computers on the rest of the internet where to access particular information. Each domain has a name. The domain for Internet Handbooks for instance is: www.internet-handbooks.co.uk

DotUK One of the largest UK 'talkers'.

Download 'Downloading' means copying a file from one computer on the internet to your own computer. You do this by clicking on a button that links you to the appropriate file. Downloading is an automatic process, except you have to click 'yes' to accept the download and give it a file name. You can download any type of file - text, graphics, sound, spreadsheet, computer programs, and so on.

ebusiness The broad concept of doing business to business, and business to consumer sales, over the internet.

E-cash Short for electronic cash. See cybercash.

ecommerce The various means and techniques of transacting business online.

Email Electronic mail, any message or file you send from your computer to another computer using your 'email client' program (such as Netscape Messenger or Microsoft Outlook).

email address The unique address given to you by your ISP. It can be used by others using the internet to send email messages to you. An example of a standard email address is:

mybusiness@aol.com

emoticons Popular symbols used to express emotions in email, for example the well known smiley:
:-) which means 'I'm smiling!'

Emoticons are not normally appropriate for business communications

Encryption Encoding for security purposes. Email and any other data can now be encrypted using PGP and other freely available programs. Modern encryption has become so amazingly powerful as to be to all intents and purposes uncrackable. Law enforcers world wide are pressing their governments for access to people's and organisation's passwords and security keys. Would you be willing to hand over yours?

Excite A popular internet directory and search engine used to find pages relating to specific keywords which you enter. See also Yahoo!.

E-zines The term for magazines and newsletters published on the internet.

FAQ Frequently Asked Questions. You will see 'FAQ' everywhere you go on the internet. If you are ever doubtful about anything check the FAQ page, if the site has one, and you should find the answers to your queries.

Favorites The rather coy term for **bookmarks** used by Internet Explorer, and by America Online.

File A file is any body of data such as a word processed document, a spreadsheet, a database file, a graphics or video file, sound file, or computer program.

Filtering software Software loaded onto a computer to prevent access by someone to unwelcome content on the internet, notably porn. The well-known 'parental controls' include CyberSitter, CyberPatrol, SurfWatch and NetNanny. They can be blunt instruments. For example, if they are programmed to reject all web pages containing the word 'virgin', you would not be able to access any web page hosted at Richard Branson's. Virgin Net! Of course, there are also web sites that tell you step-by-step how to disable or bypass these filtering tools.

finger A chat command which returns information about the other chat user, including idle time (time since they last did anything).

Firewall A firewall is special security software designed to stop the flow of certain files into and out of a computer network, e.g. viruses or attacks by hackers. A firewall would be an important feature of any fully commercial web site.

flame A more or less hostile or aggressive message posted in a newsgroup or to an individual newsgroup user. If they get out of hand there can be flame wars.

folder The name for a directory on a computer. It is a place in which files are stored.

Form A means of collecting data on web pages, using text boxes and buttons. For example quite a few commercial sites will ask you to register by completing an online form.

Forums Places for discussion on the internet. They are rather like usenet newsgroups and allow you to read, post and reply to messages. See also **bulletin board services.**

Frames A web design feature in which web pages are divided into several areas or panels, each containing separate information. A typical set of frames in a page includes an index frame (with navigation links), a banner frame (for a heading), and a body frame (for text matter).

freebies The 'give away' products, services or other enticements offered on a web site to attract registrations.

freespace An allocation of free web space by an internet service provider or other organisation, to its users or subscribers.

freeware Software programs made available without charge. Where a small charge is requested, the term is **shareware**.

front page The first page of your web site that the visitor will see. FrontPage is also the name of a popular web authoring package from Microsoft.

FTP File transfer protocol – the method the internet uses to speed files back and forth between computers. Your browser will automatically select this method, for instance, when you want to download your bank statements to reconcile your accounts. In practice you don't need to worry about FTP unless you are thinking about creating and publishing your own web pages: then you would need some of the freely available FTP software. Despite the name, it's easy to use.

GIF A graphic information file. It is a compressed file format used on web pages and elsewhere to display files that contain graphic images. See also JPEG.

Graphical client A graphical client typically uses many windows, one for each conversation you are involved in. Each window has a command line and status bar.

GUI Short for graphic user interface. It describes the user-friendly screens found in Windows and other WIMP environments (Windows, icons, mice, pointers).

hacker In the sense used by the mass media, it means someone who makes or seeks to make an unauthorised entry into someone else's computer system or network. Programmers use the word hacking to refer to editing programs (hacking an unruly mess into a beautiful form, like a gardener working on a hedge). Programmers call the vandals by various other names, including 'crackers', but most of the names are unprintable.

History list A record of visited web pages. Your browser probably includes a history list. It is handy way of revisiting sites whose addresses you have forgotten to bookmark - just click on the item you want in the history list. You can normally delete all or part of the history list in your browser. However, your ISP may well be keeping a copy of your history list (see **internet service providers**, above).

hit counter A piece of software used by a web site to publicly display the number of hits it has received.

Hits The number of times a web page has been viewed.

home page This refers to the index page of an individual or an organisation on the internet. It usually contains links to related pages of information, and to other relevant sites

Host A host is the computer where a particular file or domain is located, and from where people can retrieve it.

HotBot This is a popular internet search engine used to find pages relating to any keywords you decide to enter. 'Bot' is short for robot. In internet terms it means a piece of software that performs a task on the internet, such as searching.

HTML Hyper text markup language, the universal computer language used to create pages on the world wide web. It is much like word processing, but uses special 'tags' for formatting the text and creating hyperlinks to other web pages.

HTTP Hyper text transfer protocol. It is the standard way that HTML documents are transferred from host computer to your local browser when you're surfing the internet. You'll see this acronym at the start of every web address, for example:

http://www.abcxyz.com

With modern browsers, it is no longer necessary to enter 'http://' at the start of the address.

Hyperlink See **link**.

hypertext This is a link on an HTML page that, when clicked with a mouse, results in a further HTML page or graphic being loaded into view on your browser.

Infoseek One of the ten most popular internet search engines.

Internet The broad term for the fast-expanding network of global computers that can access each other in seconds by phone and satellite links. If you are using a modem on your computer, you too are part of the internet. The general term 'internet' encompasses email, web pages, internet chat, newsgroups, and video conferencing. It is rather like the way we speak of 'the printed word' when we mean books, magazines, newspapers, newsletters, catalogues, leaflets, tickets and posters. The 'internet' does not exist in one place any more than 'the printed word' does.

internet account The account set up by your internet service provider which gives you access to the world wide web, electronic mail facilities, newsgroups and other value added

Internet Explorer The world's most popular browser software, a product of MicroSoft and rival to Netscape (recently taken over by America OnLine).

Internet service providers ISPs are commercial, educational or official organisations which offer people ('users') access to the internet. The well known commercial ones in the UK include AOL, CompuServe, BT Internet, Freeserve, Demon and Virgin Net. Commercial ISPs may levy a fixed monthly charge, though the world wide trend is now towards free services. Services typically include access to the world wide web, email and newsgroups, as well as others such as news, chat, and entertainment. Your internet service provider will know everything you do on the internet - emails sent and received, web sites visited, information downloaded, key words typed into search engines, newsgroups visited and messages read and posted. This is why many of them are willing to offer their services free. What do they do with all this data? How long do they store it? Do they make it discreetly available to enforcement agencies? Do they allow the police private access? There are some major issues of personal privacy and data protection in all this, at both a national and European level, and state surveillance is expanding fast. At the very least, check out your service provider's privacy statement – but it may have very little value.

intranet A private computer network that uses internet technology to allow communication between individuals, for example within a large commercial organisation. It often operates on a LAN (local area network).

IP address An 'internet protocol' address. All computers linked to the internet have one. The address is somewhat like a telephone number, and consists of four sets of numbers separated by dots.

IRC Internet relay chat. Chat is an enormously popular part of the internet, and there are all kinds of chat rooms and chat software. The chat involves typing messages which are sent and read in real time. It was developed in 1988 by a Finn called Jarkko Oikarinen.

ISDN Integrated Services Digital Network. This is a high-speed telephone network that can send computer data from the internet to your PC faster than a normal telephone line.

JavaScript A simple programming language that can be put onto a web page to create interactive effects such as buttons that change appearance when you position the mouse over them.

JPEG The acronym is short for Joint Photographic Experts Group. A JPEG is a specialised file format used to display graphic files on the internet. JPEG files are smaller than similar GIF files and so have become ever more popular - even though there is sometimes a feeling that their quality is not as good as GIF format files. See also MPEG.

keywords Words that sum up your web site for being indexed in search engines. For example for a cosmetic site the key words might include beauty, lipstick, make-up, fashion, cosmetic and so on.

Kick To eject someone from a chat channel.

LAN Local area network, a computer network usually located in one building.

Link A hypertext phrase or image that calls up another web page when you click on it. Most web sites have lots of hyperlinks, or 'links' for short. These appear on the screen as buttons, images or bits of text (often underlined) that you can click on with your mouse to jump to another site on the world wide web.

Linux A new widely and freely available operating system for personal computers, and a potentially serious challenger to Microsoft. It has developed a considerable following.

Listserver A listserver is an automated email system whereby subscribers are able to receive and send email from other subscribers to the list.

Log on You may be asked to 'log on' to certain sites and particular pages. This normally means entering your user ID in the form of a name and a password.

Log on/log off To access/leave a network. In the early days of computing this literally involved writing a record in a log book.

Lurk The slang term used to describe reading a newsgroup's messages without actually taking part in that newsgroup. Despite the connotations of the word, it is a perfectly respectable activity on the internet.

Macros 'Macro languages' are used to automate repetitive tasks in Word processors.

Mail server A remote computer that enables you to send and receive emails. Your internet access provider will usually act as your mail server.

Mailing list A forum where messages are distributed by email to the members of the forum. The two types of lists are discussion and announcement. Discussion lists allow exchange between list members. Announcement lists are one-way only and used to distribute information such as news or humour. A good place to find mailing lists is Listz (http://www.liszt.com). You can normally quit a mailing list by sending an email message to request removal.

Marquee A moving (scrolling) line of text on a web site, normally used for advertising purposes.

Mayhem One of the largest UK 'talkers'.

Media player Software on a personal computer that will play sounds and images including video clips and animations.

Metasearch engine A site that sends a keyword search to many different search engines and directories so you can use many search engines from one place.

meta tags The technical term for the keywords used in your web page code to help search engine software rank your site.

modem This is an internal or external piece of hardware plugged into your PC. It links into a standard phone socket, thereby giving you access to the internet. The word derives from Modem MOdeulator/DEmodulator.

moderator A person in charge of a mailing list, newsgroup or forum. The moderator prevents unwanted messages.

MOO Multi-object…. (AUTHOR ???)

MPEG The file format used for video clips available on the internet. See also JPEG.

MP3 An immensely popular audio format that allows you to download and play music on your computer. See http://mpeg.org for further technical information, or the consumer web site www.mp3.com.

MUDs Multi-User Dungeons, interactive chat-based fantasy world games. Popular in the early days of the internet, they are in now in decline with the advance of networked arcade games such as Quake and Doom.

multi-phased medium The internet is a multi-phased medium. In other words, it can be used in many different ways to do many different things.

navigate To click on the hyperlinks on a web site in order to move to other web pages or internet sites.

Net A slang term for the internet. In the same way, the world wide web is often just called the web.

Netiquette Popular term for the unofficial rules and language people follow to keep electronic communication in an acceptably polite form.

Netmeeting This Microsoft plugin allows a moving video picture to be contained within a web page. It is now integrated into Windows Media Player.

Netscape After Internet Explorer, Netscape is the most popular browser software available for surfing the internet. An excellent browser, Netscape has suffered in the wake of the rise of Microsoft's Internet Explorer, mainly because of the success of Microsoft in getting it pre-loaded on most new PCs. Netscape Communicator comes complete with email, newsgroups, address book and bookmarks, plus a web page composer, and you can adjust its settings in all sorts of useful ways. Netscape was taken over by American Online for $4 billion.

nettie Slang term for someone who likes to spend a lot of time on the internet.

newbie Popular term for a new member of a newsgroup or mailing list.

Newsgroup A Usenet discussion group. Each newsgroup is a collection of messages, usually unedited and not checked by anyone (‘unmoderated’). Messages can be placed within the newsgroup by anyone including you. It is rather like reading and sending pubic emails. The ever-growing newsgroups have been around for much longer than the world wide web, and are an endless source of information, gossip, news, entertainment, sex, politics, resources and ideas. The 50,000-plus newsgroups are collectively referred to as Usenet, and millions of people use it every day.

News reader A type of software that enables you to search, read, post and manage messages in a newsgroup. It will normally be supplied by your internet service provider when you first sign up, or preloaded on your new computer. The best known are Microsoft Outlook, and Netscape Messenger.

News server A remote computer (eg your internet service provider) that enables you to access newsgroups. If you cannot get some or any newsgroups from your existing news server, use your favourite search engine to search for ‘open news servers’ - there are lots of them freely available. When you have found one you like, add it to your news reader by clicking on its name. The first time you do this, it may take 10 to 20 minutes to load the names of all the newsgroups onto your computer, but after that they open up in seconds whenever you want them.

Nick Nickname, an alias you can give yourself and use when entering a chat channel, rather than using your real name.

Nominet The official body for registering domain names in the UK (for example web sites whose name ends in .co.uk).

online The time you spend linked via a modem to the internet. You can keep your phone bill down by reducing online time. The opposite term is offline.

Op A chat channel operator.

open source software A type of freely modifiable software. A definition and more information can be found at: www.opensource.org

OS The operating system in a computer, for example MS DOS (Microsoft Disk Operating System), or Windows 95/98.

Packet Term for a small piece of data sent or received over the internet on your behalf by your internet service provider, and containing your address and the recipient's address.

Paedophile An adult who has sexual desires for children

ParaChat - ParaChat offers Java-based web chat rooms to any webmaster who wants to use it. http://www.parachat.com/

PC Personal computer.

Ping You can use a ping test to check the connection speed between your computer and another computer.

Off-portalling

Online Being connected to the internet.

Pentium The name of a very popular microprocessor chip in personal computers. The first Pentium IIIs were supplied with secret and unique personal identifiers, which ordinary people surfing the net were unwittingly sending out, enabling persons unknown to construct detailed user profiles. After a storm of protest, Pentium changed the technology so that this identifier could be disabled. If you buy or use a Pentium III computer you should be aware of this risk to your privacy when online.

PGP Pretty Good Privacy. A method of encoding a message before transmitting it over the internet. With PGP, a message is first compressed then encoded with the help of keys. Just like the valuables in a locked safe, your message is safe unless a person has access to the right keys. Many governments (as in France today) would like complete access to people's private keys. New Labour wanted access to everyone's keys in the UK, but dropped the proposed legislation after widespread protests. Unlike in many countries, there is no general right to privacy in the UK.

Plugin A type of (usually free and downloadable) software required to add some form of functionality to web page viewing. A well-known example is Macromedia Shockwave, a plugin which enables you to view animations.

Plugin chat A form of internet chat which depends on your downloading and installing additional software for your web browser.

PoP Point of presence. This refers to the dial up phone numbers available from your ISP. If your ISP does not have a local point of presence (i.e. local access phone number), then don't sign up - your telephone bill will rocket because you will be charged national phone rates. All the major ISPs have local numbers covering the whole of the country.

Portal site Portal means gateway. A portal site includes the one that loads into your browser each time you connect to the internet. It could for example be the front page of your internet service provider. Or you can set your browser to make it some other front page, for example a search engine such as Yahoo!, or even your own home page if you have one.

Post, to The common term used for sending ('posting') messages to a newsgroup. Posting messages is very like sending emails, except of course that they are public and everyone can read them. Also, newsgroup postings are archived, and can be read by anyone in the world years later. Because of this, many people feel more comfortable using an 'alias' (made-up name) when posting messages.

Privacy. You have practically no personal privacy online. Almost every mouse click and key stroke you make while online is being electronically logged, analysed and possibly archived by internet organisations, government agencies, police or other surveillance services. You are also leaving a permanent trail of data on whichever computer you are using. But then, if you have nothing to hide

you have nothing to fear… To explore privacy issues worldwide visit the authoritative Electronic Frontier Foundation web site at www.eff.org, and for the UK, www.netfreedom.org.

Protocol Rules. It is the technical term for the method by which computers communicate, for example http (hyper text transfer protocol) or ftp (file transfer protocol). It's not something to worry about in ordinary life.

Protocol Technical term for the method by which computers communicate. A protocol is something that has been agreed and can be used between systems. For example, for viewing web pages your computer would use hypertext transfer protocol (http). For downloading and uploading files, it would use file transfer protocol (ftp).

proxy An intermediate computer or server, used for reasons of security.

Quicktime A popular free software program from Apple Computers that will play sounds and images including video clips and animations on both Apple Macs and personal computers.

rank Your place on the list of web sites produced by a search engine, as a result of someone doing a search.

Real-time web chat Form of chat in which a web page is continually reloaded. You can only see the last few lines of the conversation at any one time.

refresh, reload The refresh or reload button on your browser toolbar tells the web page you are looking at to reload.

Register You may have to give your name, personal details and financial information to some sites before you can continue to use the pages. Site owners may want to produce a mailing list to offer you products and services. Registration is also used to discourage casual traffic.

Registered user Someone who has filled out an online form and then been granted permission to access a restricted area of a web site. Access is usually obtained by logging on, in other words entering a password and user name.

Residency The saving of a 'talker' is referred to as residency.

Search engine A search engine is a web site you can use for finding something on the internet. Popular search engines are big web sites and information directories in their own right. There are hundreds of them; the best known include Alta Vista, Excite, Google, Infoseek, Lycos and Yahoo!.

Secure servers The hardware and software provided so that people can use their credit cards and leave other details without the risk of others seeing them online. Your browser will tell you when you are entering a secure site.

secure sockets layer (SSL) A standard piece of technology which ensures secure financial transactions and data flow over the internet.

server Any computer on a network that provides access and serves information to other computers.

Shareware Software that you can try before you buy. Usually there is some kind of limitation to the game such as a time limit, or limited features. To get the registered version, you must pay for the software, typically $20 to $40. A vast amount of shareware is now available on the internet.

shell account

Shockwave A popular piece of software produced by Macromedia, which enables you to view animations and other special effects on web sites. You can download it free and in a few minutes from Macromedia's web site. The effects can be fun, but they slow down the speed at which the pages load into your browser window.

Signature file This is a computer file in which you can place your address details, for adding to email and newsgroup messages. Once you have created a signature file you can append it to your emails as often as you like.

Slashdot One of the leading technology news web sites, found at: http://slashdot.org

smiley A form of **emoticon**.

snail mail Popular term for the standard postal service involving post-persons, vans, trains, planes, sacks and sorting offices.**Spam** The popular term for electronic junk mail - unsolicited and unwelcome email messages sent across the internet. The term comes from Monty Python. There are various forms of spam-busting software which you can now obtain to filter out unwanted email messages.

Subscribe The term for accessing a newsgroup in order to read and post messages in the newsgroup. There is no charge, and you can subscribe, unsubscribe and resubscribe at will with a click of your mouse. Unless you post a message, no-one in the newsgroup will know that you have subscribed or unsubscribed.

Surfing Slang term for browsing the internet, especially following trails of links on pages across the world wide web.

sysop Systems operator, someone rather like a moderator for example of a chat room or bulletin board service.

Talk A form of internet chat, less used today. It was succeeded by Ntalk ('new talk') with which it was incompatible.

Talkers Servers which give users the opportunity to talk to each other. You connect to them, take a 'nickname' and start chatting. Usually, they offer some other features besides just allowing users to talk to each other, including Bulletin Boards, a 'world' such as a city or building, which you move around in. an opportunity to store some information on yourself, and some games.

TCP/IP Transmission Control Protocol/Internet Protocol, the essential technology of the internet. It's not normally something you need worry about.

telnet Software that allows you to connect via the internet to a remote computer and work as if you were a terminal linked to that system.

Textual client Textual clients run on a text screen (or window). They split it into a one-line command line at the bottom, a status bar just above that, and a chat message window in the rest of the screen.

theme A term in web page design. A theme describes the general colours and graphics used within a web site. Many themes are available in the form of readymade templates.

Thread An ongoing topic in a usenet newsgroup or mailing list discussion. The term refers to the original message on a particular topic, and all the replies and other messages which spin off from it. With news reading software, you can easily 'view thread' and thus read the related messages in a convenient batch.

traffic The amount of data flowing across the internet, or to a particular web site, newsgroup or chat room.

uploading The act of copying files from your PC to a server or other PC on the internet, for example when you are publishing your own web pages. The term is most commonly used to describe the act of copying HTML pages onto the internet via FTP.

UNIX This is a computer operating system that has been in use for many years, and still is used in many larger systems. Most ISPs use this operating system.

URL Uniform resource locator – the address of each internet page. For instance the URL of Internet Handbooks is http://www.internet-handbooks.co.uk

Usenet The collection of well over 50,000 active newsgroups that make up a substantial part of the internet.

virtual reality The presentation of a lifelike scenario in electronic form.

Virus A computer program maliciously designed to cause havoc to people's computer files. Viruses can typically be received when downloading program files from the internet, or from copying material from infected disks. Even Word files can now be infected. You can protect yourself from the vast majority of them by installing some inexpensive anti-virus software, such as Norton, McAfee or Dr Solomon.

web authoring Creating HTML pages to upload onto the internet. You will be a web author if you create your own home page for uploading onto the internet.

Webcrawler A popular internet search engine used to find pages relating to specific keywords entered.

Webmaster Any person who manages a web site.

web pages individual sets of information that can be viewed completely on one screen (though you may need to scroll down to see the whole page)

web site a set of web pages which are interconnected

Windows The hugely popular operating system for personal computers developed by Bill Gates and the Microsoft Corporation. The Windows 3.1 version was followed by Windows 95, further enhanced by Windows 98 and now Windows 2000.

Write A chat program called Write flashes a message on the screen of another user, named on the command line. The other user can then use the same command to write on the screen of the first user. By agreeing a few simple rules, it's possible to hold a workable conversation with another user.

WWW The world wide web. Since it began in 1994 this has become the most popular part of the internet. The web is now made up of more than one billion web pages of every description, typically linking to other pages. Developed by a British computer scientist, Tim Berners-Lee, its growth has been exponential and is set to continue so.

WYSIWYG 'What you see is what you get.' If you see it on the screen, then it should look just the same when you print it out.

Yahoo! Probably the world's most popular internet directory and search engine, and now valued on Wall Street at billions of dollars.

Zip/unzip Many files that you download from the internet will be in compressed format, especially if they are large files. This is to make them quicker to download. These files are said to be zipped or compressed. Unzipping these compressed files generally refers to the process of returning them to their original size on receipt. Zip files have the extension '.zip' and are created (and unzipped) using WinZip or a similar popular software package.

Web Site Index

Web Site	**URL**
Absolute Security	http://www.pepsoft.com/absec/intro.html
Access Control programs	http://www.softseek.com/Internet/Web_Browsers_and_Utilities/Privacy_and_Access_Control/
Action	http://www.action.com
Adult Check	http://www.adultcheck.com/
Anonymizer	http://www.anonymizer.com
AOL	http://www.aol.co.uk/try/
Boob Cruise	http://www.boobcruise.com
Bookmark Manager	http://www.cdml.com/OurSoft/ubm.htm
BT Trustwise	http://www.trustwise.co.uk/welcome.html
Center for Media Education	http://www.cme.org/children/kids_tv/violence.html
Childline	http://www.childline.org.uk/factsheets/surfing1.cfm
Classical Conditioning	http://www.as.wvu.edu/~sbb/comm221/chapters/pavlov.htm
Cookie Pal	http://www.kburra.com/cpal.html
Cyber Patrol	http://www.cyberpatrol.com
Cyber Surveillance	http://www.intelliquis.com/products/cyber.stm
CyberAngels	http://www.cyberangels.org
CYBERsitter	http://www.solidoak.com/cyberinfo.htm
Dakota	http://www.dakota-euro.com/

Deja	http://www.deja.com/usenet_home.epl
Domain Search	http://www.domainsearch.com/
Don't Forget	http://www.mousehook.com/dforget.htm
Filters Review	http://microweb.com/pepsite/Software/filters.html
Fletcher Research	(http://www.fletch.co.uk/)
Freedom	http://www.freedom.net/
Freezone	http://www.freezone.com
GetNetWsie	http://www.getnetwise.org/
Guide to Netiquette	http://www.albion.com/netiquette/
Halt Abuse	http://www.haltabuse.org/
Heinnie Knives	http://www.heinnie.com/
Internet 101	http://www2.famvid.com/i101/internet101.html
Internet Content Ratings Association	http://www.icra.org/
Internet Service Provider Association	http://www.ispa.org.uk
Internet Service Provider Association Members List	http://www.ispa.org.uk/members.htm
Internet Watch Foundation	http://www.iwf.org.uk
ISP Review	http://www.ispreview.co.uk
Jungle	http://www.jungle.com
KidDesk	http://www.edmark.com/prod/kdis/
KidShield	http://www.kidshield.com/

KZUK	http://www.kzuk.net
Learn the Net	http://www.learnthenet.com/english/index.html
Metropolitan Police Paedophile Report	http://www.met.police.uk/police/mps/mps/mis/ocg.htm
Microsoft Internet Explorer	http://www.microsoft.com/windows/IE
Microsoft Internet Explorer Ratings	http://www.microsoft.com/windows/ie/ratings.asp
Microsoft Windows 2000 upgrade compatibility	http://www.microsoft.com/windows2000/upgrade/compat/default.asp
Microsoft Windows Update	http://windowsupdate.microsoft.com
National Criminal Intelligence Service Paedophile Unit	http://www.ncis.co.uk/pa.html
Nestcape Communicator Smart Update	http://www.netscape.com/smartupdate/index.html?cp=dowdep1
Net Family News	http://www.netfamilynews.org/
Net Nanny	http://www.netnanny.com/
Net Parenting	http://www.netparenting.com/
Net Parents	http://www.netparents.org/
Net Patrol	http://www.cyberangels.org/netpatrol/index.html
NetLearn	http://www.rgu.ac.uk/schools/sim/research/netlearn/callist.htm

Netscape Communicator	http://www.netscape.com/download/index.html?cp=djudep2
Netscape Netwatch	http://home.netscape.com/communicator/netwatch/
Norton Internet Security	http://www.symantec.com/sabu/nis/index.html
Norton Internet Security	http://www.symantec.com/sabu/nis/index.html
PC World	http://www.pcworld.co.uk
Pipex Use Policy	http://www.unipalm.pipex.com/customerservices/usepolicy/
Police Law	http://www.policelaw.co.uk/internet.htm
Pretty Good Privacy	http://www.pgp.com/asp_set/products/tns/intro.asp
Privacy	http://privacy.net
Protecting children in cyberspace	http://www.childpsych.com/sample2.htm
Safe Kids Safe Surf	http://www.safekids.com/index.html http://www.safesurf.com/
SafetyEd ScamBusters	http://www.safetyed.org/ http://www.scambusters.com/index.html
Security Administrator	http://www.softheap.com/secagent.html
Security and Access Control Software	http://www.softseek.com/Utilities/Encryption_Security_and_Passwords/Security_and_Access_Control/
SexWorld UK	http://www.sexworld.co.uk/
Simon Wiesenthal Organisation	http://www.wiesenthal.com
Smart Parent	http://www.smartparent.com/

SoftSeek	http://www.softseek.com
Surf Monkey SurfWatch	http://parents.surfmonkey.com/ http://www.surfwatch.com
The Internet For Teachers	http://www.massnetworks.org/~nicoley/tutorial/index.html
The Jackson Laboratory	http://lena.jax.org/pubinfo/media/releases/eicher.html
The Web Adviser	http://www.the-web-adviser.com
Usage and Logging programs	http://www.softseek.com/Utilities/Encryption_Security_and_Passwords/Usage_Monitoring_and_Logging/
Web Monkey	http://hotwired.lycos.com/webmonkey/guides/
William Hill	http://www.williamhill.co.uk/
Window Washer	http://www.webroot.com/washer.htm
World Wide Web Consortium PICS	http://www.w3.org/PICS/
Yahooligans	http://www.yahooligans.com
Zero Knowledge Systems	http://www.zks.net

[i] The Observer, 6th June 1999

[ii] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905354804&rel=true

[iii] Sexual Addiction and Compulsivity Journal, March 2000

[iv] The Observer, 19th March 2000

[v] The Guardian, 9th December 1999

[vi] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905355382&rel=true

[vii] See: http://www.dawn.com/1998/19981227/int7.htm

[viii] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905354672&rel=true

[ix] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905355199&rel=true

[x] See: http://www.internetnews.com/ec-news/article/0,,4_134631,00.html

[xi] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905355006&rel=true

[xii] See: http://www.nua.net/surveys/index.cgi?f=VS&art_id=905355684&rel=true

[xiii] The Independent, Review Section, 28th August 1998

[xiv] Mass Media, Violence and Society, Howitt D and Cumberbatch G, London, Paul Elek, 1975

[xv] Daily Telegraph, 15th June 1999

[xvi] Hilgard's Introduction to Psychology, Edited by Rita L. Atkinson et al, Harcourt Brace College Publishers, Florida, 1996.

[xvii] http://www.nua.ie/surveys/analysis/weekly_editorial/archives/issue1no28.html

[xviii] http://www.crimelibrary.com/serial/pedophiles/4.htm

[xix] The Times, 27th April 2000

[xx] See: http://www.zdnet.com/products/stories/reviews/0,4161,398118,00.html

[xxi] PC Magazine, April 2000

[xxii] PC Magazine, 1999 also see: http://www.zdnet.com/pcmag/features/utilities99/parfilt06.html

[xxiii] Computer Shopper, April 2000