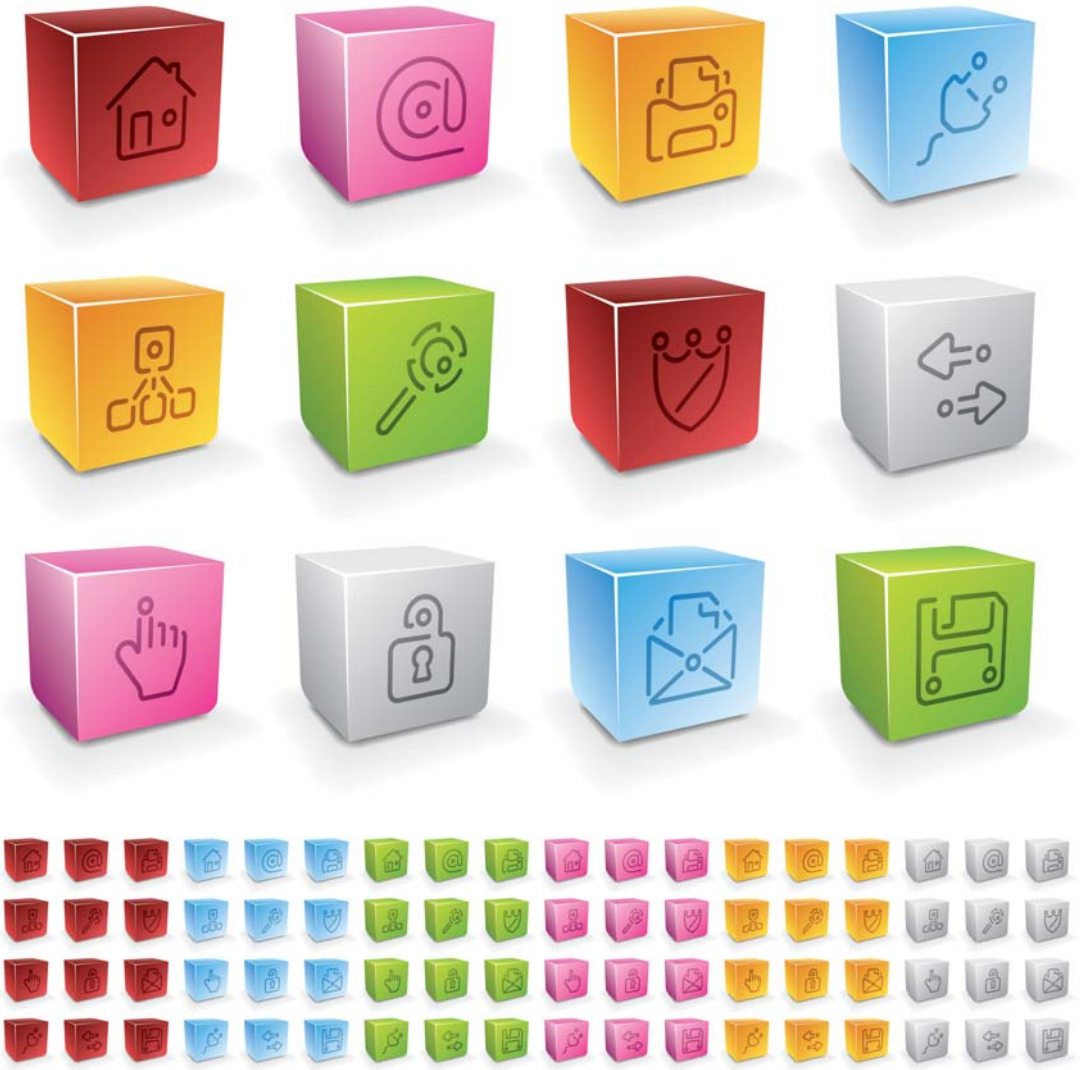
Safe Surfing

Guidelines for safe Internet use for young people and those who work with them



by
Youth Work Ireland
Drafted and Edited by Fran Bissett

Youth Work Ireland

Youth Work Ireland
20 Lower Dominick Street
Dublin 1
Tel: 01-8729933
Fax: 01-8724183
Email: info:youthworkireland.ie
Website: www.youthworkireland.ie

Contents:

ACKNOWLEDGEMENTS

We would like to acknowledge our appreciation to the following:

The members of the **National Youth Federation Youth Information Network** for their input and feedback in reviewing various drafts of the original guidelines.

Those agencies who gave us permission to adapt and reproduce some of their materials in the original guidelines.

Michelle Drumm, former **Irish YouthWork Centre** Administrator for her administrative support in the production of the original guidelines.

Gina Halpin, Youth Work Ireland National Office for her work on design, layout and desk top publishing of these revised guidelines.

Geraldine Moore, Youth Work Ieland National Office for her work in proofing this document.

COPYRIGHT PERMISSION

DISCLAIMER

INTRODUCTION

In 2003 Youth Work Ireland (then the National Youth Federation) developed a set of guidelines and poster campaign on Safe Internet Use for those working with young people called Safe Surfing. This document is an updated version of that set of guidelines.

These guidelines focus on general safe use of the Internet and email with a focus on chatrooms, newsgroups, bulletin boards etc and also provide supporting documentation and templates to assist with the provision of Internet access by youth organisations. However, these guidelines pre-dated the explosion in the use of social networking sites such as Bebo, MySpace, YouTube and Facebook and **do not cover the safe use of social networking sites.** However, in tandem with the updating of these guidelines, a separate companion set of guidelines has been produced - **Safe Social Networking Guidelines.**

The use of the Internet by children and young people is an emotive issue, which has generated much public debate in recent times. The increasing media reporting and publicity surrounding the potential exploitation of young people by paedophiles and child abusers, those promoting racial hatred, and exposure to pornographic and other inappropriate materials, has made many concerned parents and those who work with young people fearful of allowing young people access to the Internet.

However, we live in the era of information technology, where most young people now have access to a computer be it at home, school/college, via mobile phones and increasingly in the high street. We must accept that we cannot prevent young people using the Internet. Indeed it should be encouraged, as it is potentially a wonderful leisure, educational and developmental tool that can open up many opportunities and new worlds for young people at the touch of a button.

Our role should be to ensure, to the best of our ability, that young people are using and enjoying the Internet in a safe and responsible manner. These guidelines represent in a small way an attempt to assist this process. The document is not prescriptive and does not claim to have all the answers. It does attempt however to document a range of successful and practical measures and advice which can be used by those working with young people in helping them to use the Internet in as safe a manner as is possible.

Many of the sections contained in the document can be extracted and used as stand alone materials to suit either the setting you work in and/or the group of young people you are working with. Much of the information is standard but has been produced or written in different forms or language to suit a particular audience be it young person, parent or worker.

We would encourage readers to use whatever materials are relevant and appropriate to their setting or circumstances and disseminate the information contained as widely as possible.

We would also like to refer people to the partner document mentioned earlier, **Safe Social Networking Guidelines** also available as a downloadable document from www.youthworkirleand.ie OR www.iywc.com

SECTION ONE: Guidelines

Introduction

This section contains the main body of the guidelines and incorporates a number of areas that need to be considered when developing or drawing up a policy document or guidelines on safe use of the Internet and computers by young people.

The areas covered are by no means to be regarded as prescriptive or exhaustive but they do incorporate the main areas of concern identified during the development of these guidelines and in combination with the selection of template documents in Section Two and supporting information included in the Appendices section we hope they will provide readers with a comprehensive set of resources from which a coherent and extensive set of guidelines can be tailored to suit the needs of any centre or group's setting and circumstances.

The following areas are covered in this section:

- Online Safety Measures/Tools
- Responsibilities of Internet Service Providers
- Internet Service Providers' Responses to Complaints and Queries
- How to Check Internet Resources Accessed by a Computer
- General Safety Principles
- Using Websites, Chatrooms, Newsgroups and Email
- Guiding Principles for Young People
- Simple Tips for Young People
- Guidelines for Parents
- Computer Viruses

ONLINE SAFETY MEASURES / TOOLS

Acceptable Use Policies

Most Internet and online service providers take the issue of online safety seriously. For example, many Internet service providers (ISP's) have adopted Acceptable Use Policies (AUP'S), outlined in their service agreements, to ensure safety of their customers. These policies can be viewed at the provider's website, and are normally included with membership/subscription information.

They usually include guidelines covering libel, defamation, obscene/pornographic material, and threatening, abusive, or illegal behaviour online, as well as the use of the service to spread unsolicited e- mail, commonly known as "spam". Depending on the ISP, the consequences and penalties associated with this type of behaviour vary from minimal reductions in privileges to temporary suspension, or even permanent termination of service. An example of an AUP is included in the Sample Documents section.

Monitoring & Filtering Tools

Most Internet and online service providers also provide a range of online safety services to their customers either for free or at a discounted price. Potential customers should check with their ISP to determine what options are available to them and to determine the costs involved, which vary from one provider to another (or be free in some instances). There are a variety of different tools and services available. A number of such examples are listed below:

- **Browsers with child-safety features e.g. Microsoft Internet Explorer 5.0, which features child-safety and security features. Ratings are also available that can provide parents with the ability to create restricted sites and safe sites.**
- **Filtering software e.g. Cyber Patrol, Net Nanny or Surfwatch, which using a variety of methods (see below) allow for access to unsuitable and inappropriate materials to be blocked or filtered.**
- **General information and advice services e.g. Cruise Control an Internet guide for kids and families. It includes a Web site, CD-ROM, seminar series, and school teacher training program designed to encourage a safe Internet experience.**
- **Search engines, which allow children to search for content that is geared toward their interests and is safe.**

Blocking Access to Unsuitable & Inappropriate Material

For those concerned that their child may be reading or viewing material online that one considers unsuitable, inappropriate or harmful, one may want to think about filtering tools as mentioned above. There are numerous filtering tools available, and they do not all work the same way. Most of these tools filter based on one or more of the following kinds of information:

- **Filtering "Context Sensitive" Key Words: Analyses the language around key words such as 'breast' to avoid blocking "breast cancer" or "chicken breast" for example, but block sites of a sexual nature, which include the word 'breast' in the title.**
- **Filtering key words: Limits access to sites containing potentially inappropriate words like "sex" or "breast". Some of these filters block only the selective key words, not the text surround-**

ing them. Some filters apply to web sites, others to e-mail, chat, "instant" message systems, news groups, or a combination of them all. Most filters allow parents to turn off or edit the key word list.

- **Filtering on Approved/Pre-listed Web Site Addresses: Limits access to a specific list of websites that have been classified as inappropriate or unsuitable to be accessed by young people. Some companies decide what is filtered, some let parents select from a list of pre-set categories (e.g. graphic violence OK, sexually explicit material not OK). Some provide a "starter list" where a parent can add or remove sites. Also, some tools allow a parent to override the filter if they feel that the site is appropriate for their child to view, but others do not.**
- **Real Time Screen Monitoring: – This method involves the screen being scanned regularly for flesh colours (nude photographs/images). This method does not filter text and can also filter out colours similar to flesh such as pink or peach.**
- **Web Page Review and Classification: Some companies employ people e.g. an Internet Resource Manager to look at web pages that have been visited, and classify them, into different categories, which a parent may or may not choose to block. However, some such services will not offer such a choice and will automatically filter out sites they deem unsuitable or inappropriate.**

Resources

A listing of relveant agencies and useful websites is included in the Appendices Section, which provide information, advice and guidelines to parents, teachers, young people and those who work with them on issues of Internet safety.

RESPONSIBILITIES OF INTERNET SERVICE PROVIDERS

Most if not all ISP's provide some sort of service to users in terms of filtering or monitoring materials which is inappropriate or unsuitable for children and young people and many operate Acceptable Use Policies (see next section). However, as with most other issues relating to the use of the Internet, the legal position is vague. Currently, there is no specific legislation to cover the responsibility of an ISP regarding the material that can be accessed when using them as a service provider.

However, there have been some cases in Europe and the USA where providers have been taken to court and found to be liable or at least have a legal responsibility for the kind of material that can be accessed when using their service and given this some ISP's are responding by screening out unsuitable material at source. There have been no such legal cases in Ireland to date.

There are however, some clear legal provisions in this area. Stalking through electronic or physical means carries a penalty of up to seven years imprisonment in Ireland. Also, if an individual continually sends email to someone that is unwanted, explicit, etc. it can be regarded as a harassment offence under section 10 of the Non-Fatal Offences Against the Person Act (1997).

INTERNET SERVICE PROVIDERS (ISP'S) RESPONSES TO COMPLAINTS

As previously highlighted many ISP's provide filtering and monitoring products/tools. As part of such services many have sections within them whereby anyone can make suggestions regarding inappropriate sites, ask

questions regarding specific sites and seek general information, help and advice. This is the method that most ISP's will use to assist or refer their clients to when they have questions or complaints in relation to offensive or inappropriate sites that they or their children come across in using the Internet. An extensive listing of these filtering and monitoring tools is provided in the Appendices (see Appendix 2), as is a separate list (see Appendix 3) of sites that provide information, educational support and advice on Internet sites, which will assist users with such questions and queries. (See Reporting a Complaint)

As previously highlighted, many ISP's also operate Acceptable Use Policies (AUP) with their customers. If an ISP has such an AUP they can terminate the email account of their customer if they are found to be using their email account to send threatening/abusive emails or spam emails. It is possible to trace the source of an email back to the ISP whereby one can then report any inappropriate use of email. There is an excellent website for children called For Kids By Kids Online which goes through the process involved in tracing an email. The website address is www.fkbko.net

HOW TO CHECK INTERNET RESOURCES ACCESSED BY A COMPUTER

Checking the History Folder

There are a number of ways whereby it is possible to check exactly what material has been accessed on the Internet on a computer. The simplest option is the History folder. When you go online there is a History icon as one of the options, at the top of the screen usually. If you click on History, there will be normally be options to check what has been accessed within the day, last week, two weeks etc. If you click on any of these options you will get a list of the sites accessed over that period and they can be easily examined for their content by clicking on any of them.

However, it is relatively easy to clear out the History folder or set it up not to retain a list of sites visited for very long. If this is the case it becomes more difficult to check what sites have been visited, but not impossible. There are a variety of software packages available that include a facility whereby a record is kept of any website, chatroom etc that is accessed which can be checked at any time.

Saving and Downloading Information

If any website or file, picture, graphic, etc has been saved or any item has been downloaded on to a computer it is also possible to check by searching the hard drive for new items. Also, when a website or file, picture, graphic, etc, which has previously been saved or downloaded, is deleted from the computer it goes into the recycling bin. It will remain there until it is also removed from the recycling bin, and it can be easily accessed by simply clicking on the recycling bin icon.

GENERAL SAFETY PRINCIPLES

Physical Danger

One of the most serious potential risks faced when using the Internet involves the possibility of someone hurting or exploiting you because of information that you post or someone else posts about you online or because of somewhere you go as a result of what you encounter online. The numbers of young people who are abducted, or leave home as a result of contacts made on the Internet are thankfully relatively low, but it does happen and the results can be tragic.

Harassment

When you are online, especially in chatrooms, newsgroups or bulletin boards, there is a possibility that you will get messages that are harassing, demeaning, upsetting or nasty. A message such as this says a lot about the sender and should act as a warning. Ironically, even people who are nice in the "real" world can forget their manners when they go online.

The best thing to do if you encounter such messages or people in chatrooms who are behaving this way is to ignore them. Some messages, however, may constitute harassment. If someone sends you messages or images that are obscene, lewd, or indecent, intended to harass, abuse, annoy, or threaten you, report it to your Internet Service Provider, parent, teacher or leader, whoever you feel is most appropriate.

Hurting Others and Getting Into Trouble

Avoid doing anything that might hurt other people and risk getting you into trouble. You need to respect people's privacy and avoid taking any actions that annoy, harass, or hurt other people. You are responsible for your behaviour when you are online and this applies to giving out information about other people. Treat this information as if it were information about yourself and be as careful about sharing it as you would your own personal details.

Uncomfortable Situations and Inappropriate Behaviour

Not everything that can go wrong in cyberspace necessarily puts you in physical danger. However, there are sites, newsgroups, chat rooms, and other places online that contain material that could make you feel uncomfortable. It could be material that's sexual and/or violent in nature. It could be material expressing hateful attitudes or discussing activities that you find repulsive or unpleasant. It really doesn't matter what the material is. What is important is that you have the right, and the tools, to remove yourself from any site, chatroom, newsgroup etc. where you feel uncomfortable or unsure.

Financial Risk

The Internet, like so many other forms of media in this world, can be used by people who would try to take money from you or your family or just pester you with unwelcome advertising, promotions and marketing material. Be especially vigilant of "get rich quick" schemes that promise to help earn you lots of money for you on your own time. In most cases if something sounds "too good to be true", it probably is.

Safeteens.com

USING WEBSITES, CHATROOMS, NEWSGROUPS AND EMAIL

WEBSITES:

Introduction & Background

Websites give young people the opportunity to do many wonderful things; read newspapers, tour museums, check out libraries, play games, look at pictures, shop, or do research to help with homework. Children and young people can pursue their hobbies, plan holidays and trips abroad, and much more. There are millions of web sites on just about every topic imaginable.

Many web sites are excellent, but many others are silly or contain "adult" images and other material that children and young people should avoid. Other sites will contain violent, racist, sexist, and demeaning

information and images. Some of these sites contain material that can be disturbing, even for adults. If you wander into any of these sites, it is best to leave immediately by clicking on the Home icon, going to another site, or shutting down from the Internet altogether.

Giving Personal Information

In addition to displaying information, websites sometimes ask you for personal details. The site may ask for your name, mailing address, email address, and other information before letting you in. It may entice you to provide information in exchange for sending you a promotion or entering you in a contest. Never enter any personal information, if at all possible, and if necessary check with your parents.

When you enter information on a web site or anywhere on the Internet, you are giving up a bit of your privacy. Your name will inevitably end up in some database(s), and will be probably to be used to sell you something sooner or later. However this information can potentially be used to harm or exploit you. Just because a web site seems to be from a reputable organisation or individual does not mean that it necessarily is what it seems to be. Anyone can set up their own website and it is relatively easy and straightforward to do so. So be extremely cautious before divulging any personal information online. This is especially true with sites that contain adult material.

Some children and young people have their own web sites or post material to web sites maintained by their school or a youth group they are involved with. If you choose to post something on the web, be sure never to include your address, telephone number, or a photograph of yourself. If you do want people to be able to contact you through the web, just give an email address, preferably a central email address used by the school or youth group's website.

CHAT ROOMS:

Introduction and Background

Chat rooms allow people to engage in a live conversation with other people at their computer anywhere in the world. It has been compared to being on a party line, only you type instead of talk. Everyone in the chat room can see everything that is typed. The types of chat rooms vary depending on the service being used. Some chat rooms operate open conversations. Some rooms are moderated where there is a "speaker" who leads the discussion and participants. Some rooms have chaperons or monitors who are responsible for maintaining order, but even in some of these rooms what is typed is displayed immediately.

The monitor can eject someone out of the room that is acting in an inappropriate manner. However, he or she may be able to act only after the fact. The monitor cannot, however, prevent you from going off to a private chat area with a person who might do you harm or typing information that could put you in danger.

Chat rooms are widely regarded as probably the most dangerous area on the Internet as you have no reliable way of knowing whom you are chatting to or who is listening in, so never say anything in a chat room you would not say in public.

Online Relationships

It is not uncommon for people to make "friends" in chat rooms. You enter a room, start a conversation with someone who shares a particular interest with you and over time a relationship of sorts can often develop. These relationships in many cases are fine and very enjoyable for the participants. However people sometimes use chat

rooms to exploit others. Chat rooms are sometimes used by paedophiles to target victims. Adults or possibly older teenagers seeking to exploit children will obviously not tell the truth about who they are.

You might meet someone in a room who appears to be sympathetic and understanding and offers wonderful advice and friendship. If the relationship remains strictly online, that could be fine as long you are careful not to give out any personal information and you also let your parents (or school or youth group if using one of their computers) know that such a relationship has developed.

Meeting Up

The thought of getting together with someone you meet in a chat room and you like to 'chat' to is natural and can be exciting to look forward to, but remember people are not always who they seem to be. The basic rules for online safety apply to all areas of the Internet, but they are especially important in chat areas. Never give out personal information or arrange a face-to-face meeting with someone you meet in a chat room without first checking with parents

Be suspicious of anyone who tries to turn you against your parents, teachers, or friends or wants to meet you in secret.

Theme Based Chatrooms

Chat rooms are usually organised around a particular theme or topic, so avoid any topic area that makes you feel uncomfortable. Also just because a chat room is designed around a particular topic does not mean that other topics will not be discussed. Even if the room is "teens only," you have no way of knowing if everyone really is a teenager, so you still have to be on guard.

Be especially careful of chat rooms that get into subjects that might be associated with sex or cult groups that practice potentially dangerous rituals. It might seem interesting or even fun to discuss something that you might never consider engaging in, but some people who fantasise about things also like to try them out.

In some online services and web sites it is possible to enter into a private chat room where one can arrange to 'meet' friends. In some cases, but not all such chat rooms are truly private. They may be listed in a directory of rooms elsewhere and if this is the case other users can enter those rooms at any time.

A useful tip to avoid harassment, particularly for women and girls, is to choose a gender-neutral name e.g. your initials or a word to use in a chat room. Be careful with whatever name or words one chooses making sure it does not identify you or have any meaning or implication that might encourage others to bother you.

NEWSGROUPS, FORUMS, AND BULLETIN BOARDS:

Introduction and Background

Newsgroups (also called bulletin boards or forums) are places where users can read and post messages or download or upload files. Newsgroups do not operate in live or "real time" as chatrooms do. Messages are posted and they remain on the newsgroup for people to look at later. Newsgroups can also be used to post files including computer programmes, pictures, illustrations etc.

Newsgroups are again usually theme or subject specific, and they are often useful ways to get questions answered and share information about hobbies, sport, leisure, music or any others of interest.

Risk Factors

The primary risk attached to using newsgroups is posting a message that reveals information about you. Thus the basic principles previously discussed still apply of never revealing identifying information about yourself. The act of posting a message makes your email address public and available for people to send you email that you do not want. It should be noted that newsgroups are a particular favourite for people to send out junk mail ("spam"). Where possible use a central email address to post messages from and read replies.

There are newsgroups that contain sexually explicit or racist stories, illustrations, and photographs. In some cases this material may be illegal, especially if it contains images of people who are younger than the age of consent or certain other material that has been defined as obscene or contain materials aimed at inciting racial hatred. Some of this material can be disturbing and should be avoided. It is particularly dangerous to post anything in these types of groups as revealing your email address could reveal your identity.

E-MAIL:

Introduction and Background

Email is in its simplest explanation is a one-to-one form of communications system. As with postal mail, you write to someone who can then write back. Increasingly, people and companies are using email to send out messages to thousands of people at a time, for sales and marketing purposes, a process known as "spamming", which can be intrusive and annoying. Email is essentially free saving significant postal, staff, and time costs by sending out thousands or even millions of messages at the click of a mouse. Some also use 'spamming' to try to entice people to visit sexually explicit web sites.

Using Misleading Email Addresses

Each email message that you send and receive contains a return address. What many people do not realise is that the return address can be manufactured or disguised. So, just because you get a message from for example *'jenny@hotmail.com'* does not necessarily mean it is really from your friend Jenny. It could really be from another source using the email address to give a false impression of where or who it is coming from. Email can also contain other information called a 'header' that provides more information about who sent the message than where it came from. Understanding the header information can be difficult, but if you ever receive an email message that is aggressive, threatening, or contains material that makes you feel uncomfortable, you should report it to your Internet Service Provider and ask them to investigate where it came from.

Illegal Material

Material that appears to be illegal in nature should be reported immediately to the Internet Service Provider or an appropriate person such as your parent, teacher or youth leader, which will depend on where the computer you are using is located. Illegal material includes threats to your own safety, threats to others, child pornography, and evidence of other crimes.

Be careful how you respond to email from people you do not know. Remember, the sender may not be who he or she seems to be. Never send a photograph of yourself or any personal information to someone you do not know. Also, email can easily be copied and forwarded to others. Therefore, if you send personal information to friends, be sure that they are willing to respect your privacy.

In general, it is regarded as sensible and safer not to respond to spam mail or mail from someone you do not know. By responding you are verifying to the sender that you have a valid email address, and that information

can be used to encourage a person who may send inappropriate emails or get you on even more lists. If you receive a message that contains material that is sexually explicit, violent, or advocates something that is illegal or simply makes you feel uncomfortable, show it to your parents and report that message to your Internet service provider.

GUIDING PRINCIPLES FOR YOUNG PEOPLE

Educating Parents

Many parents will spend more than a decade educating you and teaching you about things they know. The Internet provides children with an opportunity to reverse the roles. Regardless of whether your parents are Internet novices or competent in using computers and the Internet, there are probably many things you know about the Internet that they will not. This is a great opportunity for you to explain them what you do online, reassure them and, in the process help them get more out of the Internet themselves.

Basic Rules of Online Safety for Children and Young People

The most important thing to remember is that when you are online in any kind of a public forum is that you are out in public and anyone can read whatever you post. You should never post anything on the Internet you would not want known to the public at large. You should also remember that people you meet in cyberspace may not be who they seem to be.

Keep Your Identity Private

If you are in any type of public forum, avoid giving out your full name, your mailing address, your telephone number, the name of your school, or any other information that could help someone detect your actual identity. The same applies to your family and friends. Also, never reveal any information about other people that could possibly get them into trouble.

Never Get Together With Someone You "Meet" Online

The biggest danger to your safety is if you get together with someone you have met online. Remember you never know for certain if people you meet online are who they say they are. If you do feel it is appropriate to meet with someone, discuss it with your parents and never go to the meeting by yourself. Arrange to meet in a public place, like a coffee shop or mall that you (not just the other person) are familiar and comfortable with, and never go alone. The safest procedure is to have your parents talk with the parents of the other person and for both of you to bring your parents along on the first meeting.

Do Not Respond to Unwelcome Emails or Chatroom Comments/Messages

It is not your fault if you get a message that you do not like, which upsets you or in any way makes you feel uncomfortable. If you receive such a message, whether it is en email or a comment or message in a chatroom or newsgroup, do not respond to it. Show it to your parents or a trusted adult to see if there is anything you can do to make it stop. Sending a response merely encourages the person.

NEVER RESPOND TO E-MAIL, CHAT COMMENTS, OR NEWSGROUP MESSAGES THAT ARE AGGRESSIVE, PERSISTENT, INAPPROPRIATE, OR IN ANY WAY MAKE YOU FEEL UNCOMFORTABLE.

SIMPLE TIPS FOR YOUNG PEOPLE

- **Remember – A million times before you've heard that honesty is the best policy. Many people do not believe that, though. So when you're out there in cyberspace, watch your- self. You never know when 5`6", blond and female could actually mean 6`3", hairy and male. Don't believe everything you see online.**
- **Be wary of those who want to know too much. There is no rule that says you have to tell them where you live, what your last name is, or anything else personal. Your business is your business. Let them stick to theirs. And trust your instincts. If someone makes you feel uncomfortable, leave.**
- **If you're planning on meeting up with somebody you met online, bring a friend, or even your parents, along with you and encourage your online acquaintance to bring theirs too. It sounds stupid but it is definitely the smart idea. At the very least discuss any possible meeting or request to meet with your parents, teacher or youth leader in advance and make sure they know what you're doing.**
- **If you get suspicious e-mails, files, or pictures from someone you don't know and trust, dump them just like any other junk mail. You could have a lot to lose by trusting someone you've never even met. The same goes for clicking links or sites that look suspicious – just don't do it.**
- **Avoid chat rooms or discussion areas that look sketchy or provocative, and do not let people on-line trick you into thinking of them as real-life friends if you've never met them in person. Just the same, don't let people goad you into online fights. If you go looking for trouble on the Internet, you'll find it, and things can get out of control really fast.**

GUIDELINES FOR PARENTS

Being a parent in the virtual world of the Internet is in essence not hugely different from being a parent in the real world. Many of the common sense principles, which a parent would employ to safeguard and protect their child from harm or unsuitable images or influences, can be utilised when attempting to protect one's child from unsuitable material on the Internet.

Listed below is a series of basic pointers and principles, which should greatly assist a parent to ensure safe use of the Internet by their child:

- **By taking responsibility for your children's online computer use, parents can greatly minimise and potential risks of being online.**
- **Take the trip together. Take the time to see what your kids are doing online and what their interests are. If you don't know how to log on, get your child to show you. Become familiar with all the things you can do online.**
- **Teach kids never to give out their personal information to people they meet online, espcially in public places like chat rooms and bulletin boards. Don't reveal home address, school name, and telephone number.**
- **Don't post photos of your children on web sites or newsgroups that are available to the public.**

- Avoid using your child's name and email address in any public directories and profiles.
- Tell your children never to give their password to anyone except their parents.
- Instruct your child never to plan a face-to- face meeting alone with online acquaintances without your permission. If a meeting is arranged, make the first one in a public place and be sure to accompany your child.
- Be very careful about any offers that involve you coming to a meeting, having someone visit your house, or sending money or credit card information.
- Tell your child not to respond when they receive offensive or dangerous email, chat, or other communications that make them feel uncomfortable. If your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy to your Internet service provider and ask for their assistance.
- If you become aware of the transmission, use or viewing of child pornography or illegal material while online, immediately report this to the Internet Service Provider and to the Police.
- If you become aware of the transmission, use or viewing of child pornography or illegal material while online, immediately report this to the Internet Service Provider and to the Police.
- Instruct your child not to click on any links or sites that are contained in emails from persons they do not know. Such links could lead to sexually explicit or otherwise inappropriate sites.
- Remind children that people they meet online may not be who they seem. Someone indicating that "she" is a "12 year-old girl" could in reality be a 40-year-old man.
- Be sure kids understand that they can come to you to explain things they find, and you will not be angry at them, though you may feel upset that they had to encounter something uncomfortable. Make sure kids know their rights, and that information about them and their family is private, and they don't have to give it out.
- Check "history" to see where your child has gone online. In Netscape Navigator you can check the history by going to the Window menu and clicking on the history command OR click the down arrow on the far right side of the location bar.
- Limit the amount of time children spend online. Don't let the Internet take the place of non-virtual chatting, reading, game playing and exploring.
- Be sure to make this a family activity. Consider placing your computer in the family room or another open area of your home where the entire family can see it, monitor the activity, and use it. This increases the likelihood of communication and discussion over computer issues.
- Get to know the services your child uses. If you don't know how to log on, get your child to show you. Find out what types of information it offers and whether there are ways for parents to block out objectionable material.
- Get to know their "online friends" just as you get to know all of their other friends
- Establish clear ground rules with your kids for Internet use – and consequences for breaking them (see Section 2: Sample Documents and Templates)
- Discuss these rules with your children and post them near the computer as a reminder

Finally check out blocking, rating and filtering tools As identified earlier, there are many services that rate websites for content as well as filtering programme browsers that empower parents to block the types of sites they consider to be inappropriate. These programmes work in a variety of different ways as discussed in Online Safety Measures/Tools earlier. Some block sites known to contain objectionable material. Some prevent users from entering certain types of information such as their name and address. Other sites are designed to keep children away from chat rooms or restrict their ability to send or read email.

Pages 11 – 16 include some adapted extracts and ideas from existing educational websites on safe Internet use such as Safeteens.com and For Kids By Kids Online among others. For a comprehensive list of such sites see Appendix 3 at the back of these guidelines.

COMPUTER VIRUSES

Definition & Effect

A computer virus is a programme that is designed to deliberately 'infect' or cause damage to a person's computer and its associated hardware and software. They are programmed in such a way that when they reach a computer, usually by email, they will damage or destroy the computers hardware, software, operating system etc. Computer viruses vary in the damage that they can inflict on your computer or network of computers if relevant. Some will damage or corrupt files or file areas whereas others can completely disable or destroy the hard drive and wipe out everything stored on the computer.

There has been a great deal of publicity in recent times about super computer viruses, which have been spread all over the world and caused untold damage. It is important, therefore, to be especially vigilant when checking and reading your emails, as this is the most common and easiest way to spread a computer virus. Some viruses are set up so that when they reach an individual or organisation's computer or network of computers (if relevant) they will automatically be sent to every email address that an individual or organisation has stored within its computer/network of computers.

Email

Be particularly careful when opening email and/or attachments to email from unknown or new sources. Where possible run an anti-virus software package (see below). If in any doubt do not open an email, simply delete it. If it is genuine and important the individual will usually follow up by another communication method if they do not receive a reply to the email.

Protection Against Computer Viruses

There are many software products and services available which can protect your computer or organisation from the dangers of computer viruses. It is advisable to seek the advice of an expert computer consultant as to what would be the computer anti-virus software best suited to your individual needs. One should bear this in mind when purchasing a computer.

Furthermore as with so much computer equipment be it hardware or software, anti-virus software dates very quickly, so one should get your anti-virus soft- ware checked at least twice a year if possible to ensure you have adequate protection and if not to get your anti-virus software upgraded accordingly.

SECTION TWO: Sample Documents and Templates

This section contains a number of templates which can be used by youth information centres and youth groups in other settings to assist in the development of a policy on Safe Internet Use for young people. The templates are generic and all of them can be adapted to suit the particular needs of the young people, staff, location and the setting.

The following template documents are contained in this section:

- Sample Youth Information Centre Internet Use Policy for Young People
- Generic Usage Policy for Youth Information Centres
- Sample Acceptable Use Policy (school/college based)
- Sample Parental Consent Form
- Sample Contract Between Parent and Child

SAMPLE YOUTH INFORMATION CENTRE INTERNET USE POLICY FOR YOUNG PEOPLE

Dún Laoghaire Youth Information Centre is pleased to offer Internet/Email access to children and young people. Both of these services are free. However, the centre does have guidelines, which it expects its users to follow. Failure to follow these guidelines could result in the user being denied access.

It is important to know that Internet use is neither private or secure. Anything you write, read, send or post on the Internet can be seen and read by others, and be traced back to the computer that first accessed or posted the information.

Guidelines for Internet Use

General

1) Internet sessions must be pre-booked. Email: 20 minutes, Internet browsing: 40 minutes
2) No more than two people allowed at a terminal at any one time.
3) Parental consent for children under 15 must be obtained.
4) Improper Use – improper use of the Internet could create liability on the part of yourself on the be half of the youth centre.

Internet Use

It is not permitted to open or download files without first checking them with the staff for possible viruses. If a virus is found, please contact a member of staff. Anyone who opens an infected file will be denied further use of the centre's computers.

The viewing of pornographic or violent material is not permitted. Anyone found viewing such materials will be denied further access to the centre's computers. It is not permitted to post any material that is blasphemous, profane, or insulting to any religious creed or opinion, any material that is sexist or demeaning to any person or persons, any pornographic material, or any material that is racist, or material damaging to young people.

Emails

1) Young people may set up an email account, using any one of the web based email providers e.g. hot mail.com / Ireland / com / yahoo.com etc.

This account is the property of the user and not of the information centre.

2) Use standard Netiquette guidelines for all mail. These include:
- **(i)** Limit the length of messages (be conservative in what you send, liberal in what you receive)
- **(ii)** Use subject headings in messages
- **(iii)** Respect the copyright of material you produce
- **(iv)** Never send chain letters on the Internet
- **(v)** Do not reveal any personal information on the Internet (either your own or some- one else's) when forwarding or re-for- warding a message
- **(vi)** Do not send any large amounts of unsolicited information to people
- **(vii)** Always be courteous

For more information on Netiquette check the Internet e.g.

www.ude.ie/~lis/elec.htm www.fau/edu/netiquette/net
www.cochran.com/sttartguide/Netiquette.html www.albion.com/netiquette

We can be contacted at:
Dún Laoighaire Youth Information Centre,
The Bell Tower,
Dun Laoghaire,
Co. Dublin.
Tel. No.: 01-2809363,
Fax No.: 01-2843799,
Email: yicdlys@iol.ie

USAGE POLICY/CONTRACT FOR YOUTH INFORMATION CENTRE

These two pages provide a generic template covering all of the areas that could be incorporated into a usage policy/contract for Youth Information Centres. Some of the sections may not be relevant or practical to operate in a particular YIC's depending on resources and staffing levels, access to and number of computers, physical location or local circumstances.

If it is deemed not to be practical or appropriate to have each young person read and sign a contract such as this, an alternative option is to have this information clearly displayed and for young people to read it and sign a simple log book which confirms that they have read and are aware of the conditions under which they use computers/access the Internet in the Centre.

NAME OF YOUTH INFORMATION CENTRE:

_____
_____
_____

NAME OF LOCAL YOUTH SERVICE:

_____
_____
_____

1. PURPOSE & OPENING HOURS

We are pleased to provide a Public Internet Access Service for our clients. This service is available at the following times:

_____
_____
_____

2. CONDITIONS OF USE

This service is provided as a privilege to the user and this Usage Policy/Contract provides an opportunity to educate the user on the conditions of use, and the responsibilities of the user.

3. ACCESS

There are _____ computers available for public use. Ask for assistance from a member of staff as to which computers are available and if in use when they will next become available.

A time slot can be booked in advance by phone or email. The client must be on time for any booked slot otherwise the slot will be given to another user

4. TIME

Computers can be booked/used for ___ at a time. Clients will only be able to book one session on a computer at a time in order to ensure others have the opportunity to avail of the facility.

5. USER RESPONSIBILITIES

1. Please use the computers in accordance with the conditions in this Policy/Contract.
2. Please be courteous and respectful in your email messages to others.
3. Do not degrade or damage computers and their equipment (printers, scanners, odems etc).
4. Do not change the data or trespass in the account of another user.
5. Do not gain access to inappropriate or unsuitable websites; chatrooms; newsgroups on the Internet
6. Do not use the computers to send inappropriate, unsuitable, offensive or threatening email.
7. Do not use the computers for illegal activity.

6. PERSONAL SAFETY

1. Report to a member of staff any unsolicited email, security problems, or information you gain access to that makes you uncomfortable or you feel is unsuitable.
2. Do not reveal your home address, phone number or personal details about yourself or about any of your friends.
3. Use school/youth organisation addresses and phone numbers only.
4. Please be aware that email you send is not guaranteed to be private.

7. INAPPROPRIATE USE

When using the computer you will be responsible for all your actions and any inappropriate or unacceptable uses of the computer and the Internet will result in the suspension of this service.

8. CONSENT

I have read this contract and am fully aware of the conditions of this contract and my responsibilities in using this Public Access Internet Service. Please indicate your agreement to this contract by signing here.

Client Signature:

_____

_____

_____

As the designated member of staff responsible for overseeing the use of this service I confirm that the named client has read and is fully aware of the conditions of this contract and their responsibilities in using this Public Access Internet Service.

Staff Member Signature:

_____

_____

SAMPLE ACCEPTABLE USE POLICY

SCHOOL/COLLEGE BASED

1. PURPOSE

We are pleased to provide network services for:

a) Student access to educational resources, to present information, and to work collaboratively with peers and experts internationally.

b) Faculty, staff, and administration access to professional development and research opportunities, educational standards and practices, collaborative opportunities, and successful teaching methods.

2. ACCEPTABLE USE POLICY

These services are provided as a privilege to the user and this Acceptable Use Policy provides an opportunity to educate the user on the school's expectations and the responsibilities of the user.

3. ACCESS

There are networked computers (networked meaning the computers that are connected to the Internet, email, personal and shared folders) accessible to students in classrooms, hallways, computer labs and libraries.

4. USER RESPONSIBILITIES – "DO'S AND DON'TS"

1. Do use the network in accordance with the school's code of conduct.
2. Do cite the sources of information properly.
3. Do use the network only for legal activity.
4. Do be courteous and respectful in your messages to others.
5. Do use appropriate language.
6. Do not swear, use vulgarities, or any other inappropriate language.
7. Do not degrade or disrupt equipment or sys- tem performance.
8. Do not intentionally waste finite resources or use them carelessly.
9. Do not change the data or trespass in the account of another user.
10. Do not gain unauthorised access to resources or entities

5. PERSONAL SAFETY

1. Use only your account and password and keep your password private.
2. Report to a system administrator, teacher or administrator any unsolicited email, security problems, or information that makes you uncomfortable.
3. Students: Do not reveal your home address, image, or phone numbers, or those of other students or colleagues. Use school addresses and phone numbers only.
4. Do know that electronic mail (e-mail) is not guaranteed to be private

6. INAPPROPRIATE USE

The network account holder is held responsible for their actions and activity within their account. Unacceptable uses of the network will result in the suspension or revoking of these privileges. Students will be referred to the dean of students and faculty will be referred to the head of their school.

7. CONSENT

Please indicate your consent and that your have read and are aware of the conditions of this policy by signing here.

Student Signature:

_____

_____

As the parent or legal guardian of the minor student signing above, I grant permission for my son or daughter to use school-networked computers. I have read the above stated rules and accept responsibility for setting and conveying standards for my child to use the Internet.

Parent/Guardian Signature:

_____

_____

_____

SAMPLE PARENTAL CONSENT FORM

Dún Laoghaire Youth Information Centre is pleased to offer Internet/Email access to children and young people. Both of these services are free.

The Internet is a vast information resource, which contains much useful information. At the centre we operate a policy of supervision of Internet access to avoid where possible accessing inappropriate material. Unfortunately it can still be possible to access inappropriate material in error.

Children under 15 cannot make use of our Public Internet Access without parental or guardian consent. Your child has requested access to our PC's. If, having read the above, you are happy to allow your child to access the Internet, please sign below.

We can be contacted at:
Dún Laoghaire Youth Information Centre,
The Bell Tower,
Dun Laoghaire,
Co. Dublin.
Tel. No.: 01-2809363,
Fax No.: 01-2843799,
Email: yicdlys@iol.ie

Parent/Guardian Signature:

_____

_____

Address:

_____

_____

_____

_____

_____

Name of Young Person:

_____

_____

Age:

_____

_____

SAMPLE CONTRACT BETWEEN PARENT AND YOUNG PERSON/CHILD

(a) I will not give out personal information such as my address, telephone number, parents' work address/ tele phone number, or the name and location of my school without my parents' permission.

(b) I will tell my parents right away if I come across any information that makes me feel uncomfortable.

(c) I will never agree to arrange to meet with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

(d) I will never send a person my picture or anything else without first checking with my parents.

(e) I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online services.

(f) I will not give out my Internet password to anyone (even my best friends) other than my parents.

(g) I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit.

(h) I will not access other areas or break these rules without their permission.

Child and Parent Signatures (optional)

_____
_____
_____
_____

SECTION THREE: Appendices

Appendix 1:
Resources

Appendix 2:
Reporting a Complaint

Appendix 3:
Health and Safety Issues/Use of VDU Equipment

APPENDIX ONE: RESOURCES

Irish Contact Agencies

Office for Internet Safety
The Office for Internet Safety has been established by the Government to take a lead responsibility for internet safety in Ireland, particularly as it relates to children, under the aegis of the Department of Justice, Equality and Law Reform
Office for Internet Safety
Floor 3, Block 2, Harcourt Centre, Harcourt Street, Dublin 2
Tel: 01 4086122
Email: internetsafety@justice.ie
Web: www.internetsafety.ie

Irish Internet Association
The Irish Internet Association is the professional body for those conducting business via the Internet from Ireland.
Irish Internet Association,
The Digital Hub, 101 James Street, Dublin 8
Tel: 01 5424154
Email: info@iia.ie
Web: www.iia.ie

ISPAI www.hotline.ie Service
The Internet Service Providers Association of Ireland aims to provide one voice for the Irish ISP industry at national, EU and International level. The Association is represented at many government initiatives and provides a public point of contact for the media. It established the www.hotline.ie service to combat illegal content, especially child pornography, being hosted and distributed on the Internet. ISPAI www.hotline.ie Service

ISPAI
Unit 24 Sandyford Office Park, Dublin 18
Tel: 1890 610710 Fax: 01 294 5282
Email: info@hotline.ie
Web: www.hotline.ie

NCTE
National Centre for Technology in Education is an Irish Government agency established to provide advice, support and information on the use of information and communications technology (ICT) in education.
NCTE,
Dublin City University,
Dublin 9
Tel 01 7008200 Fax: 017008210
Email: info@ncte.ie
Web: www.ncte.ie

Webwise
Webwise is the Irish Internet Safety Awareness Node managed by the NCTE. Webwise provides parents, teachers, and children with educational resources, advice and information about potential dangers on the Internet and empowers users to minimise or avoid these risks.
Web: www.webwise.ie

Useful Irish Based Resources

http://groups.google.ie/group/social-media-and-youth-work has a wide range of resources available to be downloaded including the following:

Exploring Bebo a Starter Guide for Youth Workers - *step by step tutorial on how to use bebo for youth workers*
Surfwise Educational Programme for Teachers - *manual for teachers from Webwise focuses on Internet use in general and not social networking and social media in particular*
Webwise 10 Tips for Parents - *list of dos and don'ts for parents focuses on internet use in general and not social networking and social media in particular*
Webwise Get With It: Parents Guide to Social Networking - *in-depth exploration of safety and social networking for parents in simple and easy to use language*
Webwise Personal Information Poster - *Awareness poster for young people to illustrate the dangers of posting photos of oneself*
Cyberbullying Poster - *poster providing info to young people on how to respond to text/cyberbullying*

www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-en
www.internetsafety.ie/website/ois/oisweb.nsf/page/publications-en
These two sections within the Office for Internet Safety website contain a range of downloadable documents on safe Internet use for both parents and children; safe use of mobile phones; social networking; protecting children online and cyberbullying.

Watchyourspace
Website aimed at raising awareness of Internet safety issues and promotes safe, responsible practice by young people when online. It is part of the NCTE's **Webwise** Internet safety initiative targeted at teenagers and young adults. The site is divided into 6 main areas containing clearly presented safety messages including a series of video clips of interviews with young experts using social networking sites, mobile phones and the Internet in general. It covers practical information and advice on a selection of online activities such as dealing with and reporting serious issues, online publishing and uploading images.
www.watchyourspace.ie

Webwise
Invaluable website which contains an extensive range of downloadable resources and publications, learning tools and a series of online training sessions with worksheets, handouts and posters for working with young people on different aspects of safe Internet use.
www.webwise.ie

Selected International Safe Internet Use Resource Websites

In addition to the safety information included in these guidelines there are a multitude of excellent safety resources available online from many dedicated websites. Listed below are just a few of them:

www.connectsafely.org

www.cyberbully.org

www.haltabuse.org

www.kidsmart.org

www.netsmartz.org

www.safekids.com

www.safeteens.com

www.wiredsafety.org

www.youngpeoplesafeonline.org

APPENDIX TWO: REPORTING A COMPLAINT

Reporting a Complaint

Office for Internet Safety

The Office for Internet Safety is an Executive Office of the Department of Justice, Equality & Law Reform. The Office for Internet Safety has been established by the Government to take a lead responsibility for Internet safety in Ireland, particularly as it relates to children. The Office for Internet Safety aims to build linkages and cohesion between all Departments and agencies to ensure that the State provides the best possible protection for the community and promotes internet safety, particularly in relation to combating child pornography.

The Office for Internet Safety will build on and oversee the current self-regulatory framework which is in place under the **Internet Service Providers Association of Ireland** (ISPAI) . Central to their relationship with ISPAI is an agreement to subscribe to a code of ethics and practice for the industry. As part of this agreement the industry supports www.hotline.ie which receives and processes reports of child pornography and other in appropriate Internet content.

www.hotline.ie

The www.hotline.ie service provides an anonymous facility for the public to report suspected illegal content encountered on the Internet, in a secure and confidential way. The primary focus of the Hotline is to combat child pornography. However, other forms of illegal content and activities that exist on the Internet can be reported using this service.

The Hotline, run by the Internet Service Providers Association of Ireland (ISPAI) since November 1999, is part financed by the European Commission's Safer Internet Plus Programme. It is supervised by the Department of Justice, Office for Internet Safety (OIS), in cooperation with An Garda Síochána and is a member of **INHOPE**, the International Network of Hotlines.

The **www.hotline.ie** service exists to combat illegal material on the Internet. All reports are assessed and where content is found to be illegal action is taken.

Members of the public can report content they suspect to be illegal when using any of the following services:

- **Websites (including sites for mobile WAP or equivalent).**
- **Unsolicited email (spam advertising illegal content).**
- **Peer-to-peer file sharing networks.**
- **Online forums, bulletin boards, blogs, *social networking sites.**
- **Newsgroups.**
- **Online chat rooms or instant messaging.**

*** Reporting complaint mechanism in relation to particular networking sites is dealt within the next section.**

If an individual is not sure if the material is illegal or not, it does not matter, report it to the Hotline and it will be assessed. Types of illegal content that should be reported are:

- **Child pornography**
- **Child grooming activities**
- **Child sex tourism**
- **Child trafficking**
- **Racism and xenophobia**
- **Incitement to hatred**
- **Financial scams (usually sent by spam)**
- **Other content (used to submit a query to the Hotline or notify about content not in above categories).**

Making a Report/Complaint

Upon entering the www.hotline.ie site there is a large **Click to Report** icon on the top right hand side of the page and this option is there on any page within the site that is visited. Clicking on this icon takes the user into a reporting template. The reporting template is straightforward and easy to complete and asks for the following:

- **Identify where the source of the complaint is.**
- **A description of the complaint.**
- **What is suspicious about the content (based on the above headings).**
- **An option to leave contact details or make the complaint anonymous.**

How the Hotline Processes a Report and the Information Provided Within It

The Hotline's operational process starts when a report is received from the public or from another international hotline. The submissions are generated through electronic forms that are available on **www.hotline.ie** and reports can be submitted completely anonymously.

When a report is received, the Hotline will send an acknowledgement where contact information has been given. The preference is to provide this reply by e-mail. The content of the report is then transferred to the Hotline operational Database, which is held in encrypted form for added security.

Under the legal system in Ireland, only a court of law can determine that a criminal offence has been committed and that material (i.e. child pornography) relating to that offence is actually illegal. Therefore, the Hotline can only determine that something is "probably illegal" with reference to the criteria given in the relevant Irish law. In the case of Child Pornography, for example, that is the **Child Trafficking and Pornography Act (1998)**.

Once the report has been logged, a trained Hotline Analysts will try to find the material on the Internet. If the subject content to which the report refers is found, it will then be assessed as to whether it is probably illegal under Irish law. If it is not illegal, no further investigatory action is taken. If the content is considered to be probably illegal under the relevant Act, the next step is to determine the location of the material as accurately as possible.

The Hotline staff use a suite of tools and their experience to attempt to trace and locate the source, be it a web host server, a peering node (P2P), an e-mail server or other Internet based service. If the reported material is traced to a server located in Ireland, or is found to have originated from an Internet user account provided by an Irish ISP, the ISP of that customer is identified.

The Hotline then issues notification to An Garda Síochána and simultaneously a "take down" notice is issued to the ISP, where they are a member of the ISPAI. The ISP is responsible for the timely removal of the specified probably illegal content from their servers to ensure that other Internet users cannot access the material. The decision to initiate a criminal investigation is a matter for An Garda Síochána.

If the content source is traced to another country, there are two possible actions. If an INHOPE hotline exists in that country, then details based on the original report, including the Hotline's findings, are forwarded to the other hotline for processing. If the material is located in a country having no INHOPE presence, the Hotline will attempt to have action taken by providing details to An Garda Síochána for transmission to the source country through international law enforcement channels.

In all the above cases, even if the person reporting has provided contact details, these are not provided to other parties. Only the details of the suspected content and the technical findings of the Hotline are transmitted.

Once this notification procedure is completed, the Hotline records the action that was taken in the database and closes the report.

Further Resources

The Office for Internet Safety produces occasional publications to advise and examine the role of the ISP in Ireland. The following is a list of their more recent publications which can all be downloaded free from the website (www.internetsafety.ie)

A guide to cyberbullying
Get With IT! Leaflet - Internet Safety for Parents
Get With IT - A parents' guide to social networking websites
Get with IT - A parents guide to filtering technologies
Get with IT - A parents guide to new media technologies

Contact Details:

Office for Internet Safety
Floor 3, Block 2, Harcourt Centre
Harcourt Street
Dublin 2
Tel: 01 408 6122 Fax: 0 4086142
Email: internetsafety@justice.ie
Web: www.internetsafety.ie

ISPAI www.hotline.ie Service
Unit 24, Sandyford Office Park
Dublin 18
Tel: 1890 610710 Fax: 294 5282
Email: internetsafety@justice.ie
Web: www.hotline.ie

APPENDIX THREE: SAFE & HEALTHY ISSUES` / USE OF VDU EQUIPMENT

There is another risk factor to be considered when young people are using computers and that is the issue of Health & Safety. There are very clear guidelines regarding the safe use of computers and visual display unit (VDU) equipment based on two pieces of legislation:

1. **The Safety, Health & Welfare at Work Act, 1989.**
2. **The Safety, Health and Welfare at Work (General Application) Regulations, 1993.**

Outlined below are the relevant sections from these pieces of legislation, which relate to the use of VDU equipment, the obligations of organisations towards their employees, and clients who use such equipment.

Work with Display Screen Equipment

The Regulations in this part give effect to Directive 90/270/FEC on the safety and health requirements for employees who habitually use display screen equipment (VDU's) as a significant part of their normal work.

Employers are required to evaluate health and safety at the workstations with particular reference to eyesight, physical difficulties and mental stress. Appropriate steps must be taken to control any risks identified. Employees are covered by these regulations:

Must be trained in the use of the workstation and be given information about health and safety factors.

Must also have periodic breaks or changes of routine, away from VDUs.

Are entitled to an appropriate eye and eyesight test (or may opt for either) before working with VDUs and at regular intervals. If at any time working with VDU employee experiences visual difficulties she/he has a similar entitlement.

If special corrective appliances (spectacles) are required exclusively for working at a display screen they must be provided at no cost to the employee. Should the spectacles be used also for other purposes the employer must cover the cost of the correction required for working with display screens.

Requirements are included about the various components of the workstation from chairs to the display screen etc. and as regards the general environment of the workstation, including lighting, noise levels, heat, radiation and humidity.

The duties in Part II, particularly as regards protective and preventive services, risk assessment, information, consultation & participation & training apply to the requirements in Part VII dealing with VDUs.

Regulation 29: Interpretation for Part VII

In this Part -

"display screen equipment" means any alphanumeric or graphic display screen, regardless of the display process involved;

"employee" means an employee who habitually uses display screen equipment as a significant part of his normal work; and
"workstation" means an assembly comprising display screen equipment, which may be provided with a keyboard or input device or software (or a keyboard or input device and software) determining the operator and machine interface, and includes optional accessories and peripherals such as a diskette drive, telephone, modem, printer, document holder, work chair and work desk or work surface and the immediate work environment of the display screen equipment.

The definition of "display screen equipment" (described in these Guidelines as VDUs) covers computer screens, microfiche readers and applies to both conventional cathode ray tube (CRT) display screens and other display processes such as liquid crystal displays. Display screens when showing films, videos, and television pictures or for surveillance purposes are not covered (please refer also to the exclusions under Regulation 30). However display screens capable of being used for a range of functions such as video viewing, as a television screen as well for word- processing or viewing of data and graphics will need to be assessed to establish the use of the screen and whether, if there is greater habitual use for data and graphics, it falls within the scope of the Regulations.

"Employee", as defined for this Part of the Regulations does not include employees engaged in maintenance or cleaning of VDUs. The following will help as regards deciding whether an employee is covered by the Regulations:

(a) If the employee has no choice but to the use the VDU to carry out her/his work.
(b) If the employee normally uses the VDU for continuous periods of more than one hour.
(c) If the VDU is generally used by the employee on a daily basis.

The definition of "workstation" is all encompassing and includes VDU and all the individual pieces of equipment, chair, desk and work environment, which can constitute a workstation. One of the most critical factors affecting the health of employees working at VDUs is the design and layout of the workstation. A badly arranged workstation can lead to the adoption of a bad working posture with consequent pains in muscles and joints and also visual problems. There are particular requirements on this in the 10th and 11th Schedules.

Regulation 30: Non-Application of this Part
The provisions of this Part do not apply to -

(a) Drivers' cabs or control cabs for vehicles or machinery;
(b) Computer systems on board a means of transport;
(c) Computer systems mainly intended for public use;
(d) Portable display screen equipment not in prolonged use at a workstation;
(e) Calculators, cash registers and any equipment having a small data or measurement display required for direct use of the equipment; and
(f) Typewriters of traditional design, of the type known as "typewriter with window".

This is a list of equipment to which the duties as regards VDUs do not apply. This does not dilute employers' general duties of care under the main pro- visions of the 1989 Act.

Regulation 31: Duties of Employer
(1) Every employer shall -

Perform an analysis of the workstations in order to evaluate the safety and health conditions to which they give rise for his employees, particularly as regards possible risks to eyesight, physical problems and problems of mental stress;

Workstations must be analysed to evaluate possible risks, which may give rise to visual or physical difficulties or to mental stress. This means examining each workstation taking account of the requirements, which are set out in Safety, Health and Welfare at Work Act, 1989 & Regulations. Any employee using a workstation should be given the opportunity to comment in the course of the analysis. This is in addition to the employer's general duty to consult employees on health and safety matters. Some common complaints, arising from working with VDUs which should be taken account of are as follows:

Upper limb pains and discomfort (WRULDs)

A range of effects on the arm, hand and shoulder areas linked to work activities is now described as work related upper limb disorders (WRULDs). These range from temporary fatigue or soreness in the limbs, to cramp, to ongoing pain in the muscles or nerves. These effects are probably due to a number of factors rather than any single cause. Holding a part of the body rigid for a long time such as the back, neck and head can cause discomfort in the muscles, bones and tendons. Awkward positioning of the hands and wrist relative to the work being carried out is another likely factor. These effects can be avoided by using proper equipment, suitable furniture, through training and changing the way in which the work is carried out.

Effects on the Eyes

Some employees may experience temporary eye fatigue, with such symptoms as failure to see clearly, red or sore eyes and headaches. Eye fatigue can also lead to employees adopting awkward postures, which can cause discomfort of the limbs. Medical evidence shows that using VDUS does not cause damage to eyes or eyesight; nor does it make existing defects worse. Eye fatigue can be caused by:

(a) Staying in the same position and concentrating for a long time;
(b) Poor positioning of the VDU;
(c) Poor legibility of the screen or source documents;
(d) Poor lighting, including glare and reflections;
(e) A drifting, flickering or uttering image on the screen.

While using a VDU does not cause eye damage, it may make employees with pre-existing vision defects, which are not corrected, more aware of them. Such uncorrected defects can make working with a VDU more tiring or stressful than would otherwise be the case.

Fatigue and Stress

The volume of VDU work to be carried out by employees can vary widely between different employments and activities. The work can range from air traffic control to accounting, stock recording and control, or documentation creation and revision. Some tasks may require a very high degree of concentration and vigilance. More routine tasks can even give rise to boredom. Some tasks can result in stress or fatigue.

Several symptoms, including fatigue, described by VDU users can also be caused by stress arising from broader aspects of their work. They are more likely to be caused by poor organisation of the work, lack of control by the employee over the pace of the work, under-utilisation of skills, high-speed repetitive work or working in

isolation. The onset of fatigue and stress can be minimised by careful design, selection and location of VDUs, good design of the workstation, its environment and the task involved as well as training, consultation and involvement of the employee.

Take appropriate measures to remedy any risks found, on the basis of the evaluation referred to in sub-paragraph and taking account of any additional or combined effects of any such risks so found;

Having examined each workstation in the light of the points raised in the 10th and 11th Schedules, the employer must take any necessary preventive measures to avoid risks to employees. Separate guidance is provided in both Schedules on each point. The requirements in the 10th and 11th Schedules are minimum standards. Employers may apply higher standards if they wish. The employee(s) should be informed of the steps taken following the assessment and be provided with training if necessary.

In making the analysis under subparagraph and in taking measures under subparagraph (b) for workstations already in service on or before the 31st day of December 1992, and in the interests of the health and safety of the employee, take account of the principles specified in the 10th Schedule;

The Regulations recognise the practicalities of coping with the many workstations already in use in employments. In the case of equipment already in use on 31 December 1992 the 10th Schedule contains broad specifications as regards the equipment and the environment surrounding the workstation to be taken into account when conducting the risk analysis and taking protective action. Employers must, when analysing workstations already in service before 31 December 1992, take account of the points set out in the 10th Schedule to the regulations.

Take appropriate steps to ensure that workstations first put into service after the 31 December 1992, comply with the minimum requirements specified in the 10th and 11th Schedules;

As well as complying with the 10th Schedule, all workstations first brought into use after 31 December 1992 must also comply with the 11th Schedule, which sets out more specific requirements on the equipment, the environment and the interface between employee and VDU. Please refer to Regulation 31 (2) as regards certain situations in which these requirements may not apply.

Take appropriate steps to ensure that workstations already in service on or before the 31 day of December 1992 are adapted not later than the 31st day of December, 1996 to comply with the minimum requirements specified in the 10th and 11th Schedules;

As well as complying with the 10th Schedule from the beginning of these Regulations, workstations must, following a period of grace to 31/12/1996, also meet the more specific requirements of the Eleventh Schedule as regards equipment, environment and the interface between employee and VDU.

Plan the activities of his employees in such a way that daily work on a display screen is periodically interupted by breaks or changes of activity, which reduce workload at the display screen;

Employers must plan work so that daily work at VDUs is interrupted periodically by breaks or changes in activity, which reduce the work at the screen. Although the Regulations set no frequency for breaks no single continuous period of work at a screen should, in general, exceed one hour. Equally, the Regulations do not

specify the frequency and duration of work breaks when working with VDUs, nor is there any generally accepted standard. In some countries, including Ireland there are employer / trade union agreements on work breaks at company level. The flow of work to a VDU user should be designed to allow natural breaks to occur. Alternatively a change in the pattern of work by combining VDU and non- VDU work could be introduced. However, rest breaks are essential where continuous VDU work, requiring sustained attention is likely to result in fatigue. Ideally, the length of the rest should reflect the intensity of the individual job. However, there are three very important points:

1. Rest breaks or changes in the pattern of work, where they are necessary, should be taken before fatigue sets in. Some employees suffer symptoms from the effort used to keep up performance while fatigued.
2. Short frequent rest breaks are more satisfactory than longer breaks taken occasionally.
3. Rest breaks should be taken away from the VDU. Other duties may be assigned during this period, provided they are not too intensive.

Without prejudice to the provisions of Regulation 11, provide information to his employees in relation to the measures applicable to workstations which have been implemented under subparagraphs (b) and (I) and Regulation 32; and In addition to the requirement on employers under Regulation 11 to provide information on safety and health matters to employees this paragraph puts a duty on employers to provide information on VDU workstations.

Employers must inform employees of any measures taken to protect eyesight, any risks to eyesight, physical effects or stress, as well as the arrangements for rest breaks in VDU work, or changes in work activity which are planned and also the results of any eye or eyesight tests which are conducted.

Without prejudice to the provisions of Regulation 13, provide training to employees in the use of workstations before commencing this work with display screen equipment and whenever the organisation of the workstation is substantially modified.

In addition to the requirement on employers under Regulation 13 to provide training on safety and health matters to employees, this paragraph puts a duty on employers to provide training in the use of the workstation before an employee commences work on a VDU and again should the organisation of the workstation be altered. Training should include:

(a) A general appreciation of the computer system to which the VDU may be linked;
(b) Appropriate induction training. Employees should understand how the work is organised so as to comply with these Regulations;
(c) Instruction on the general principles of ergonomics, the proper adjustment of furniture, screens, key board, lighting, etc. so as to suit individual employee's height, reach etc.

The requirements of the 10th and 11th Schedules apply only to the extent that the components concerned are present at a workstation and that the inherent requirements or characteristics of the work do not preclude such application.

The requirements of the 10th and 11th Schedules do not apply when analysing a workstation under Regulation 31 (c), (d) or (e) to a particular component if it is not normally part of a workstation or where the nature of the task makes compliance impossible. The following are examples where the need to fully comply with the 10th

and 11th Schedules may not arise:

(i) Where a VDU is part of a console in a plant control room and does not require a desk or, perhaps, a chair.
(ii) Radar screens used in air traffic control have characters with blurred "tails", which may be considered not to be well defined or clearly formed to indicate the movement of aircraft. Compliance in this case is not practicable.

The requirements specified in paragraph (1)(d) of the 11th Schedule shall not be construed as preventing the use of alternative suitable seating. There may be cases, for instance, in which an employee suffering from a back complaint, or perhaps in a wheelchair, may need to use a suitable alternative chair rather than one which complies with the 11th Schedule as regards adjustability etc.

Regulation 32: Provision of Eye Tests and Corrective Appliances

Every employer shall, taking into account any entitlement which an employee may have to any tests and appliances provided by the State and relating to eye- sight and appliances ensure –

(a) That an appropriate eye and eyesight test, carried out by a competent person, is made available to every employee -
  (i) Before commencing display screen work
  (ii) At regular intervals thereafter, and
  (iii) If an employee experiences visual difficulties which may be due to display screen work.

Eye and Eyesight Tests

Every employee who habitually uses a VDU as a significant part of normal work has a right to opt for an eye test and an eyesight test, which must be made available by the employer at his/her own cost, except where there may be a social welfare entitlement. While VDUs are now a common feature in many employments, this right applies only to employees with habitual and significant use. This could mean using a VDU for one continuous hour or more as part of every day work.

Eyesight Test (Visual Ability)

An eyesight test means a test of a person's ability to see (visual ability), to focus at various distances and to keep the two eyes coordinated. This can be carried out by a doctor or optometrist. It can also be carried out by a person (including a nurse) trained to use a vision-screening machine. The person operating the machine must know when to refer employees who do not pass the eyesight tests at the screening level to a doctor or optometrist. Problems with visual ability, which arise at any stage during life, may give rise to a need to wear spectacles.

Eye Test

An eye test means an examination of the eye itself using an ophthalmoscope normally carried out by a doctor or optometrist. Though entitled to an eye test and eyesight test, the first approach by an employee is likely to be to have an eyesight test. If the eyesight test results in the employee being referred on to a doctor or an optometrist, the who will probably do a further eyesight test as well as an eye test and will decide if the employee needs particular lenses for VDU work. While the tests should be available to all eligible employees, those suffering from visual difficulty or eyestrain either before or during work with a VDU should, in particular, avail of the option.

Combined Eye and Eyesight Test

The combined eye & eyesight test performed by an optometrist or doctor should include the following tests:

(a) Ability to read N6 print at between 30cm to 60cm.
(b) Either monocular vision or good binocular vision. In the latter case, heterophoria should be well compensated, with prisms if necessary. Diplopia is not admissible.
(c) No obvious central (+/- 20 degrees) visual field defects in the dominant eye.
(d) Normal near points of convergence and accommodation for the user's age.
(e) Clear ocular media. Absence of ocular disease.
(f) Normal colour vision is ONLY required if the V.D.U. work is unusually colour-dependant.
(g) Measurement and assessment of refractive error.

Schedule for Testing

Employees have the right to an eye and eyesight test before taking up work if it is habitual work with a VDU (one continuous hour or more every day) as well as at regular intervals. In determining the intervals, factors such as the ages of the employees and the intensity of VDU work should be taken into account in deciding the frequency of repeat tests.

That, if the results of a test under this Regulation show that it is necessary, an ophthalmological examination is carried out on the employee concerned:

Where complex problems are detected the doctor or optometrist will refer the employee to a specialist ophthalmologist for attention.

That, where the results of a test or an examination under this regulation show that it is necessary, and if normal corrective appliances cannot be used, the employee concerned is provided with special corrective appliances appropriate to his work.

Where eye tests carried out by the doctor or optometrist reveal that particular lenses are required for VDU work, the basic costs of providing the glasses (the special corrective appliances) or of new lenses where the employee already wears glasses must be borne by the employer, taking account of any social welfare entitlement that might apply. Where an employee already wears glasses to correct a visual defect (normal corrective appliances), and routine change of lenses arises, if these glasses are adequate also for VDU work, the employer is not liable as regards meeting the cost.

The cost of dealing with more general eye problems which are revealed as a result of the tests and which are not directly related to working with a VDU is a matter for the employee as part of his or her general health care, taking account of health care entitlements.

Tenth Schedule (Regulation 31): Minimum requirements for all VDUs

Many of these requirements are self-explanatory and guidance is provided only where necessary. It is expected that in due course, EU standards will cover these matters in detail.

1. EQUIPMENT

(a) General Use

The general use of the equipment shall not be a source of risk for employees. Workstations must be laid out and kept tidy so as to avoid any employee slipping, tripping or falling.

(b) Display Screen

(i) The characters on the screen shall be well defined and clearly formed, of adequate size and with adequate spacing between the characters and lines. The characters on the screen should be well defined and clearly formed so that letters and numerals may be easily recognised and clearly distinguished. The spacings between characters and between lines should also allow for an easily legible text on the screen. The legibility of characters, which depends mainly on the way they are created, their size and shape, is particularly important for avoiding eyestrain.

A minimum character height of between 3.1 mm to 4.2mm in the 350mm to 6OOmm viewing range – with a maximum viewing range of not more than 7OOmm – is recommended. Characters with a dot matrix of at least 7 x 9 dots are normally satisfactory when both upper and lower case letters are used. A 5 x 7 dot matrix is adequate for a character size of upper case letters and digits.

(ii) The image on the screen shall be stable, with no flickering or other forms of instability. In order to keep the characters visible on the screen, the signal must be continuously refreshed, i.e. regularly rewritten on the VDU. A flickering, swimming or shimmering effect which can arise may be minimised by operating VDUs at a recommended minimum 50 ertz refresh rate.

(iii) The brightness or the contrast (or both) between the characters and the back- ground shall be easily adjustable by the employee and easily adjustable to ambient conditions. The VDU should be capable of adjustment for contrast and brightness by the employee to obtain a suitable working condition. This will help avoid eyestrain and should help to maintain the quality of work produced. Excessive contrast between the characters and the general background on the VDU should be avoided.

(iv) The screen shall be free of reflective glare and reflections liable to cause discomfort to a user.

The display screen should be non-reflective and work surroundings should have a low reflective finish. See also paragraphs 2 (b) (ii) and (c) which follow.

(c) Keyboard

(i) The keyboard shall have a matt surface to avoid reflective glare.

(ii) The arrangement of the keyboard and the characteristics of the keys shall be such as to facilitate the use of the keyboard. The keyboard should be designed so that the employee can work efficiently in reasonable comfort. The position of the key board should allow sufficient resting space for the employee's hands arms to be supported. There should be no friction between the edge of the keyboard and the employee's wrist.

The keyboard should be detachable so that the employee can find a suitable working position and avoid straining hands and arms. It should be positioned so that the angle at the employee's elbow (when seated) between the forearm and the upper arm is in the range of 700 to 900. The employee should be able to look at parts of the keyboard used frequently without lowering the head. The keys should have low reflectance surfaces and should have concave tops to follow the contours of the fingertips.

(iii) The symbols on the keys shall be adequately contrasted and legible from the design working position. Modern keyboards on the market will meet these requirements based on current standards, for example

2. ENVIRONMENT

(a) Space Requirements

The workstation shall be dimensioned and designed so as to provide sufficient space for the user to change position and vary movements. There should be sufficient space for the employee to feel comfortable and to have room to stretch or reach arms or legs and to turn from side to side. There are general requirements as regards workspace in Regulation 7 (Workplace) and in the 2nd and 3rd Schedules (paragraph 9 in each case).

(b) Lighting

(i) Lighting (including room lighting, spot- lighting or work lamps) shall ensure satisfactory lighting conditions and an appropriate contrast between the screen and the background environment, taking into account the type of work and the user's vision requirements.

(ii) Possible disturbing glare and reflections on the screen or other equipment shall be prevented by co-ordinating the layout of workstations within the place of work with the positioning and technical characteristics of the artificial light sources. Correct lighting arrangements are essential if eye fatigue is to be avoided. Suitable background lighting is required for VDU work to provide an appropriate contrast between the screen and the background environment and to avoid problems of reflection and glare. As a general rule, a level of lighting of 300 – 500 lux should be appropriate. If more light is required for reading documents, local lighting should be used. However the light from a table lamp etc. must not shine on the VDU or the immediate surrounding area.

(c) Reflections and Glare

Workstations shall be so designed that sources of light, such as windows and other openings, transparent or translucid walls, and brightly coloured fixtures or walls cause no direct glare and, as far as possible, no distracting reflections on the screen. Reflections and glare can cause discomfort for the employee by making it difficult to see the information on the VDU. It is essential that VDUs should be positioned so that neither the screen nor the employee is facing a window. For greatest comfort the employee's line of vision should be parallel with the lines of overhead light fittings. Where fluorescent lights are used, they should be fitted parallel to the sides of the VDU and not parallel to the screen face. VDUs should not be positioned directly under overhead lights. Windows should be fitted with suitable blinds etc. that can be adjusted to reduce light and glare.

(d) Radiation

All radiation, with the exception of the visible part of the electromagnetic spectrum shall be reduced to negligible levels from the point of view of the protection of employees' health and safety. There is substantial evidence that concerns about radiation emissions from VDUs and their possible effects on pregnant women are unfounded. According to the World Health Organisation:

"The levels of ionising and non-ionising electromagnetic radiation which are likely to be generated by VDUs are well below those set out in international recommendations for limiting risk to human health created by such emissions and does not consider such levels to pose a significant risk to health. No special protective measures are therefore needed to protect the health of people from this radiation"

ELEVENTH SCHEDULE (REGULATION 31)

Minimum requirements for workstations first put into service after the 31st day of December 1992 and for all workstations after the 31st day of December 1996.

The following are requirements which are additional to those in the 10th Schedule and which apply as above. Some are self-explanatory and guidance is provided only where necessary.

(a) Display Screen

(i) The screen shall be able to swivel and tilt easily and freely to suit the needs of the user. Equipment on the market will in general be capable of being swivelled and tilted.

(ii) It shall be possible to use either a separate base for the screen or an adjustable table. To adjust the screen and the height or position of the employee, it should be possible to move the screen upwards or downwards as necessary. This is possible either by using a stand mounted on an adjustable arm, or a table, which is adjustable in height. Both are currently available.

(b) Keyboard

(i) The Keyboard shall be tiltable and separate from the screen so as to allow the user to find a comfortable working position, which avoids fatigue in the arms or hands. Keyboards which can be tilted and which are separate from but connected to the screen are currently available.

(ii) The space in front of the keyboard shall be sufficient to provide support for the hands and arms of the user. There should be sufficient space on the desk to place the lower arms and hands so as to avoid fatigue.

(c) Work desk or Work Surface

(i) The work desk or work surface shall have a sufficiently large, low-reflectance surface and allow a flexible arrangement of the screen, keyboard, documents and related equipment. The work desk, which should have a matt or semi-matt surface, should permit a flexible arrangement of the screen, keyboard and document stand. The desktop should be as thin as possible to allow for knee clearance but should be sufficiently strong. It should also be adjustable to allow adequate thigh clearance for the employee. Devices for adjusting the desk should be within easy reach of the employee when seated. Storage space for documents etc should be provided in the desk without interfering with comfortable use of the screen.

(ii) The document holder shall be stable and adjustable and shall be positioned so as to minimise the need for uncomfortable head and eye movement. Standard equipment available on the market meets this requirement.

(iii) There shall be adequate space for users to find a comfortable position. There should be clearances for thighs, knees, lower legs and feet under the work surfaces and between furniture components.

(d) Workchair

(i) The work chair shall be stable and allow the user easy freedom of movement and a comfortable position

(ii) The seat shall be adjustable in height

(iii) The seat back shall be adjustable in both height and tilt.

(iv) A footrest shall be made available to any user who requires one.

Work chairs should be stable and should allow the employee easy freedom of movement. The seat height of all chairs should be adjustable with backrests, adjustable in height and tilt. The support area produced by back rests

for the employee's lower back should be as large as possible so as to avoid undue pressure on the employee's thighs and spine. All employees using VDUs should be instructed in how to adjust chairs properly in order to find the best sitting posture to avoid long-term problems of muscular strain and backache.

2. ENVIRONMENT

(a) Reflections and Glare

Windows shall be fitted with a suitable system of adjustable covering to attenuate the daylight, which falls on the workstation. Vertical or venetian blinds or other coverings of a type used in offices will meet this requirement.

(b) Noise

Noise emitted by equipment belonging to a workstation shall be taken into account when a workstation is being equipped, in particular so as not to distract attention or disturb speech. Certain keyboards and printers, or numbers of them located near each other, may be sources of noise at computer work- stations. Noise can disrupt the employee's concentration particularly where a number of computer workstations are in operation. Noise can be reduced by the repositioning of printers and other equipment. Reflected sound can be reduced by the use of soundabsorbent partitions and suitable floor coverings. Where printers are installed near the employee suitable housings designed to reduce noise should be provided.

(c) Heat

Equipment belonging to a workstation shall not produce excess heat, which could cause discomfort to employees. VDU equipment and light sources discharge a certain amount of heat. Work areas should be well ventilated, kept at a comfortable temperature and free of draughts so as to avoid fatigue and discomfort.

(d) Humidity

An adequate level of humidity shall be established and maintained. Hot dry air will cause the eye surface to dry, creating eye irritation, which can lead to fatigue. The relative humidity in work areas with VDUs should be kept at an adequate level, not lower than 45%. Tests can be carried out using a wet and dry thermometer or other measuring equipment. This is particularly important where work is carried out in a relatively confined space or where there are several VDU workstations. Relative humidity can be easily increased e.g. by placing trays of water in the workplace.

3. EMPLOYEE/COMPUTER INTERFACE

In designing, selecting, commissioning and modifying software, and in designing tasks using VDUs, the employer shall take in to account the following principles;

(a) Software shall be suitable for the task;
(b) Software shall be easy to LI5C and, where appropriate, adaptable to the employee's level of knowledge or experience; no quantitative or qualitative checking facility may be used without the knowledge of the employees;
(c) Systems shall provide feedback to employees on their performance;
(d) Systems shall display information in a format and at a pace, which are adapted to employees;
(e) The principles of software ergonomics shall be applied in particular to human data processing.

The operation of VDU Systems should enable employees to work comfortably and without undue pressure or

stress. Software chosen should be appropriate to the particular task and not too complicated for the employee using it. There should not be any fear on the part of employees that hidden checks on performance are being carried out. VDU systems should have features, which indicate error messages, suitable assistance ("help") and messages about changes in the systems, malfunctions or overloading. Equipment on the market may provide these features. There are limitations on the capacity of individuals to process data on VDUs and the software must be adaptable to the employee capacities.

BIBLIOGRAPHY OF REFERENCES

Amárach Consulting, (2001), *Internet Downside Issues*, (Dublin: Amárach Consulting)

Health and Safety Authority, (1999) *Guide to the Safety, Health & Welfare at Work Act, 1989 and the Safety, Health and Welfare at Work (General Application) Regulations, 1993* (Dublin: Health and Safety Authority)

Jones, G., (2000), *Protecting Children on the Internet*, (Plymouth: Internet Handbooks)

Magid, L. J., (2001), *Teen Safety on the Information Highway*, Safeteens.com Website. (USA: Safeteens)

McConville, C., (2001), *Providing a Public Access Internet Service:* Input to NYF Youth Information Conference, (Dublin: Dun Laoighaire Youth Information Centre)

The Once Project, (2001), *For Kids By Kids Online*, (England: The Once Project)

www.hotline.ie, (2001), *Supervising the Internet: Working Together to Combat Child Pornography On- Line* (Dublin: www.hotline.ie)

Published by the Irish Youthwork Press
20 Lower Dominick Street, Dublin 1.

ISBN: 978 1 900416 68 9