

Children's and Young People's Safety on the Internet

Information & Guidance for Carers



April 2007

Introduction

These guidelines are for carers of looked after children, to assist them, advise, support and encourage the appropriate use of the Internet by children and young people.

The information and guidance provided should be read alongside Trust and/or Board Policies; which deal with the corporate responsibilities (for example) Information Technology and Health & Safety; Internet Access, E-Mail use, IT Security and Storing and Sharing of personal Information.

There are a number of web sites designed for and targeted at children & young people, these are included in the text and everyone should be encouraged to visit these because they provide useful, friendly advice and encourage safe usage.

The final page of the guidance sets out some basic rules for online safety. Each young person should be given a copy of it and asked to agree it as part of his/her Internet access.

Cyberspace," the "web," the "net," the "information highway."

Millions of people each day are now going online to exchange electronic mail (E-mail) and to communicate with others through participating in chat rooms, post, and read messages in newsgroups, and bulletin boards. "Surfing" the world wide web is now routine; and there are many online activities which assist us in our day-to-day living. Children and young people are more likely to be online than adults.

Access to the Internet is possible from a variety of locations: from personal computers at home; at a friend's house; in school; at a library; at a club; or at a cafe. Many game consoles can be connected to the Internet and used for chatting and other online interaction. It is also possible to access the Internet using mobile devices such as cellular telephones and other handheld devices. This means that children and young people are not always in the company of responsible adults when they use the Internet.

Even though Internet Service Providers (ISPs) and cellular telephone companies strive to provide their subscribers with an enjoyable, safe, and rewarding online experience, it is not possible for these companies to monitor everyone who uses their service. Once connected to the Internet you are able to exchange information with people who use other ISPs and online services.

There are no censors on the Internet

Anyone in the world — companies, governments, individuals, and organizations — can publish material on the Internet. An ISP links you to these sites, but it cannot control what is on them. It is up to individuals to make sure they behave in a safe and appropriate way. Obviously this creates potential risks for children and young people who may not have the maturity or experience to identify potential risks in situations.

Benefits of the Information Highway

There is a vast array of services available online. Reference information such as airline fares, encyclopaedias, movie reviews, news, sports, stock quotes, and weather are readily available. Children and young people find it particularly helpful when researching projects for school or completing a portfolio of work. Millions of people, including children and young people communicate through E-mail with family, friends, and colleagues around the world, or access chat areas to communicate with those who have common interests. The Internet can also be used to watch videos and listen to audio programmes produced by major media companies, businesses, organizations, and individuals.

It is however up to individuals to make sure they behave in a safe and appropriate way.

Where children are concerned, however, this requires that adults take steps to ensure their safe use of the Internet. As an educational and entertainment tool children and young people can learn about virtually any topic, visit a museum, take a college course, or play an endless number of computer games with other users or against the computer itself.

Most people who go online have mainly positive experiences. But, like any endeavour there are some risks and annoyances. Children and young people get a lot of benefits from being online, but they can also be the target of crime, exploitation, and harassment in this as in any other environment.

As an educational and entertainment tool users can learn about virtually any topic.....

It is important however that as adults we know what children are learning about and that it is age appropriate and non-threatening to them. Trusting, curious, and anxious to explore this new world and the relationships it brings, children and young people need supervision and common-sense advice regarding how to be sure their journeys into “cyberspace” are fun, appropriate, and productive experiences.

Putting the Issue in Perspective

There have been some highly publicized cases of exploitation involving the Internet, but that does not mean that every child or young person using it will experience major problems. The vast majority of those who use the Internet do not get into serious trouble, although some may experience minor irritations and frustrations.

Some people, including children, have been confronted with disturbing or inappropriate material. There are steps that parents and guardians can take to try to shield their children from such material, but it is almost impossible to completely avoid all inappropriate material. There are also a number of cases where children and young people have been victimized by serious crime as a result of going online. Parents and carers can greatly minimize the chances that children and young people will be victimized by teaching them to follow the safety rules at the back of this document. The fact that crimes are being committed online, however, is not a reason to avoid using these services.

....Instruct children and young people..to be 'street smart'...to better safeguard themselves...

A well-informed child is less likely to be harmed when using the Internet as he/she will select sites carefully and whistle-blow to parents and carers when anything untoward is accessed. Telling children and young people to stop using the Internet would be like telling them to forego attending school because students are sometimes victimized or bullied there. A better strategy is instructing them about both the benefits and dangers of "cyberspace" and for them to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

What Are the Risks?

There are a few risks for children who use the Internet or other online services. Teenagers are particularly at risk because they often go online unsupervised and are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. If you have a teenager in your family, or you are a teenager, check out Teen Safety on the Information Highway at:

www.kidsmart.org.uk

www.childnet-int.org

www.thinkuknow.co.uk

www.getnetwize.org

Some specific risks include:

- **exposure to inappropriate material:** children and young people may be exposed to inappropriate material considered to be sexual, hateful, or violent in nature, or material encouraging dangerous or illegal activities. Children may purposefully seek out such material, but they may also come across it on the web via chat areas, E-mail, or even instant messaging even if they are not looking for it;
- **physical molestation:** a child or young person might provide information, or arrange an encounter possibly risking his or her safety, or the safety of other family members. In some cases child molesters have used chat areas, E-mail, and instant messages to gain a child's confidence and then arrange a face-to-face meeting;
- **harassment and bullying:** children and young people might encounter messages via chat, E-mail, or their cellular telephones that are belligerent, demeaning, or harassing. "Bullies," typically other young people, often use the Internet to bother their victims; advice is available at:
www.bullying.co.uk
- **viruses and hackers:** a child or young person might download a file containing a virus that could damage the computer, or increase the risk of a "hacker" gaining remote access to it. This could jeopardize your family's privacy and safety;

- **legal and financial:** a child or young person could do something that has negative legal or financial consequences such as giving out a credit-card number or doing something violating another person's rights. Legal issues aside, children and young people should be taught good "netiquette" that is avoid being inconsiderate, mean, or rude on the Internet.

How to Reduce the Risks?

While children and young people need a certain amount of privacy, they also need adult involvement and supervision in their daily lives. The same general "parenting" skills that apply to the "real world" also apply online.

If you have cause for concern about a child's or young person's online activities, talk to them

Also seek out the advice and counsel of teachers, librarians, and other Internet and online service users in your area. In serious cases, also make contact with the Police.

Having open communication with children and young people in your care about using computer resources, and becoming familiar with the world wide web yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

If a child or young person tells you about an upsetting message, person, or web site encountered while online, do not blame them, rather help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and also teaches them how to deal with problems on their own.

Beyond these basic guidelines there are some specific things you should know about the Internet. For instance did you know there are chat areas, newsgroups, and web sites that have hateful or violent material or material otherwise considered to be inappropriate by parents or guardians? It is possible for children to stumble across this type of material when doing a search using one of the web sites specifically designed to help people find information on the Internet. Most of these sites,

called “search engines,” do not, by default, filter out material that might be inappropriate for children, but some offer a child-safe option and others are designed specifically for use by children and young people.

Remember, finding inappropriate material online can make people feel bad or upset

If your children end up in any of these areas, tell them to immediately leave by clicking on the ‘Home’ icon, going to another site, or shutting down the browser.

Check out the information for Safe Use of Chatrooms at:-

www.chatdanger.com

The Internet also contains newsgroups, web sites, and other areas designed specifically for adults who wish to post, read, or view sexually explicit material including pictures, stories, and videos. Some of this material is posted on web sites where there is an attempt to verify the user’s age and/or a requirement for users to enter a credit-card number on the presumption that children and young people do not generally have access to credit-card numbers. Other areas on the Internet make no effort to control access. If you or your children come across this type of material, immediately report it to the ISP and/or the Police and the child’s social worker. Your local CARE Unit may be able to assist; a list of their addresses can be found on the penultimate page of this guidance. You can also report concerns about or instances of abuse by using the Home Office sponsored: ‘Child Exploitation and Online Protection Centre [CEOP]

www.ceop.gov.uk

Some online services and ISPs allow parents, guardians or carers to limit their children’s access to certain services and features such as adult-oriented “chat rooms,” bulletin boards, and web sites. There may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised “chat room.” At the very least, keep track of any files that children or young people download to the computer (Trusts’ IT departments can assist you with this), and

consider joining your children when they are in private chat areas to assess the material they are accessing for yourself.

In addition, there are ways to filter or control what your children can see and do online. One type of filter, called a “spam” filter, limits unsolicited E-mail including mail promoting sexually explicit material. Some ISPs and E-mail services include filters as part of their service but, if not, there is software you can purchase that will help to limit this type of material getting through.

There are also ways to filter what a child or young person can see on the World Wide Web. Check with your service provider to see if they offer age-appropriate “parental controls.” If not, consider using a software programme blocking chat areas, newsgroups, and web sites known to be inappropriate for children. Most of these programmes can be configured to filter out sites containing nudity, sexual content, hateful or violent material or anything advocating the use of alcohol, drugs, or tobacco. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programmes at:

<http://kids.getnetwise.org/tools>.

Another option is to use a rating system that relies on web-site operators indicating the nature of their material. Internet browsers can be configured to only allow children and young people to visit sites rated at the level carers deem appropriate and specify. The advantage of this method is that only appropriately rated sites can be viewed. The disadvantage is many appropriate web sites have not submitted themselves for a rating and will, therefore, be blocked.

While technological-child-protection tools are worth exploring, they’re not a panacea. To begin with, no programme is perfect. There is always the possibility that something inappropriate could “slip through” or something appropriate will be blocked. Finally, filtering programmes do not necessarily protect children and young people from all dangerous activities. For example, some do not control instant messaging or chat services, which can put a child in instant communications with strangers. Also some filters do not work with peer-to-peer networks allowing

people to exchange files such as music, pictures, text, and videos. These peer-to-peer networks are sometimes used to distribute pornography, including pornographic images of children. File-sharing when in peer-to-peer networks may turn your personal computer into a server that shares your files, which can place you in legal difficulties or possibly allow others to gain access to your child's personal files on his or her computer. It is like giving someone you do not know the opportunity to know everything about you.

Filters are not a substitute for adult involvement and supervision of children's usage of the Internet

The best way to ensure that your children and young people are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with them while they are online. Have them show you what they do, and ask them to teach you how to use the Internet or online services. You might be surprised by how much you can learn!

Guidelines for Carers

By taking responsibility for children's and young people's online computer use, you can greatly minimize any potential risks associated with being online. Make it a rule to:

- never give out identifying information — home address, school name, or telephone number — in a public message such as chat or newsgroups, and be sure you are dealing with someone both you and your children know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, financial information, or marital status. Do not post photographs of children or young people in newsgroups or on web sites available to the public. Consider using a pseudonym, avoid listing a child's or young person's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used;
- get to know the Internet and any services a child or young person uses. If you do not know how to log on, get one of the children or young people to show you. Have them show you what he or she does online, and become familiar with all the activities available online. Find out if they have signed up to a free web based, E-mail account, such as those offered by some ISPs, also find out the other places, such as school and the library, where they can access those accounts;
- never allow a child or young person to arrange a face-to-face meeting with someone they first "meet" on the Internet without an adult's permission. If a meeting is arranged, **and this would be in very exceptional circumstances**, make sure the first one is in a public place, and be sure that you accompany the child or young person to any such meeting;
- never respond to messages that are suggestive; are obscene; are belligerent; are threatening; or make you feel scared, uncomfortable, or confused. Encourage the

children and young people to tell you if they encounter such messages. If you or child or young person receive a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance. Report the matter to your Trust's IT department and make a record of the event in either the fostering diary or residential log. Serious matters should be raised with the Police;

- instruct children and young people not to click on any links contained in E-mail from persons they do not know. Such links could lead to sexually explicit, or otherwise inappropriate web sites, or could be a computer virus. If someone sends you, or your children messages, or images that are indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, or if you become aware of the transmission, use, or viewing of pornographic images of children while online, immediately report this to the child's social worker and the Police immediately;
- remember people online may not be who they say they are because you cannot see or may not hear the person it would be easy for someone to misrepresent him/or herself. Thus someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man";
- remember everything you read online may not be true. Any offer that's "too good to be true" probably is. Be careful about any offers involving you going to a meeting, having someone visit your home, or sending money or credit-card information. Make sure your children are "street-smart" about the risk of a confidence trick too;
- set reasonable rules and guidelines for computer use. See "My Rules for Online Safety" at the back, discuss them with the children and young people, and post them near the computer as a reminder. There are two versions with a simpler one for younger children. Remember to monitor compliance with these rules, especially when it comes to the amount of time your children spend on the computer. Excessive use of online services or the Internet, especially late at night, may be

an indication that there is a potential problem. Remember personal computers and online services should not be used as electronic babysitters;

- check out blocking, filtering, and ratings applications to see if they will be of assistance to you;
- if children and young have a cellular telephone, talk with him or her about using it safely. The same rules that apply to computer use also apply to the use of cellular telephones.

Police Care Units – Contact Details

Ballymena C.A.R.E. Unit 26 Galgorm Road Ballymena BT43 5EX Telephone 028 2566 4014	Cookstown C.A.R.E. Unit 19 Molesworth Road Cookstown BT80 8NT Telephone 028 7939 9414
Enniskillen C.A.R.E Unit 48 Queen Street Enniskillen BT74 7JR Telephone 028 6632 1562	Maydown C.A.R.E Unit 4 Maydown Road Londonderry BT47 6SJ Telephone 028 7186 1355
Newry C.A.R.E Unit (Ardmore) 3 Belfast Road Newry BT34 1EF Telephone 028 3025 9211	Newtownards C.A.R.E Unit 36-40 John Street Newtownards BT23 4LX Telephone 028 9182 9007
Mahon Road C.A.R.E Unit 50 Mahon Road Portadown BT62 3SF Telephone 028 3831 5274	Portstewart C.A.R.E. Unit 59 Coleraine Road Portstewart BT55 7HP Telephone 028 7035 0990
Newtownabbey C.A.R.E. Unit 418 Shore Road Newtownabbey BT37 9RT Telephone 028 9025 9305	Lisburn Road C.A.R.E. Unit 276 Lisburn Road Belfast BT9 6GG Telephone 028 9025 9856
Willowfield C.A.R.E Unit 277 Woodstock Road Belfast BT6 8PR Telephone 028 9025 9831	Woodbourne C.A.R.E Unit 139 Stewartstown Road Belfast BT11 9NB Telephone 028 9025 9905

My Rules for Online Safety

- I will not give out personal information such as my address; telephone number; parents', carers or guardians' work address/telephone number; or the name and location of my school.
- I will not give out my Internet password(s) to anyone — even my best friends.
- I will tell my carer and/or key worker right away if I come across any information that makes me feel scared, uncomfortable, or confused.
- I will never agree to get together with someone I first “meet” online without checking with my carer and/or key worker. If they agree to the meeting, I will make sure it is in a public place and that I bring my carer and/or key worker along.
- I will never send a person my picture or anything else without first checking with my carer and/or key worker.
- I will not respond to any messages that are mean, or in any way make me feel scared, uncomfortable, or confused. It is not my fault if I get a message like that. If I do receive such information I will tell my carer and/or a trusted adult right away so they can contact the online service to put the situation right.
- I will talk with my carer and/or key worker and social worker so we can set up rules for going online. We will decide upon the time of day I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas, without their permission, or break these rules.
- I will practice good “netiquette” by not hurting other people or breaking the law.

SIGNED

Date: _____

Young Person

Carer

My Rules

- I agree to talk with my carers about the good and bad things that can happen when using the Internet
- I agree to my carers monitoring my use of the Internet
- I agree to tell my carers if, by mistake, I find a site that contains pornography, racism, sectarianism or extremism
- I will tell my carers if anybody says or sends me anything that makes me feel bullied, embarrassed or frightened
- I will not give out my address or any other personal information when using the Internet
- I will not allow anyone else to use my personal log-in and password
- I will not forget to log-off

Signed:

Date:

Young Person

Carer

There are some really cool things on the Internet, but a lot of bad stuff too. This means we have to be **SMART** when we are online

S	SECRET - Always keep your name, address, mobile number and password PRIVATE – it's like giving out the keys to your home if you don't act smart.
M	MEETING someone you have contacted in cyberspace can be dangerous. Only do so with your carer's permission, and then when they can be present and in a public place.
A	ACCEPTING e-mails or opening files from people you don't really know or trust can be hurtful – they may contain viruses or nasty messages
R	REMEMBER – someone online may be lying and not be who they say they are. Stick to the public area in chat rooms and if you feel uncomfortable, simply get out of there! Be smart, log off.
T	TELL your carer if someone or something makes you feel uncomfortable or worried