



Children Safety and Internet Use

This fact sheet has been developed for the Consumer Education Program by the Communications Commission of Kenya. It was compiled by studying material from various authoritative sources and adopting what is universally acceptable and relevant to the Kenyan situation. The fact sheet is intended to enable Consumers have a good understanding of the issues discussed and hence empower them when making decisions regarding ICT products and services.

Introduction

Millions of people are now going online to exchange e-mails and instant messages (IM), participate in chat groups, post and read messages in news groups which are sometimes called bulletin boards, surf the Wide World Web (WWW) and many other online activities. Children are no exception and are more likely to be online than adults. Children can go online from a personal computer (PC) usually located at home, at a friend's house, at school, at a library or at a cyber café. With advances in technology, it is also possible to access the internet on hand held devices such as cellular phones therefore have numerous opportunities to use the internet without the supervision of an adult.

While children can benefit immensely from online access, they are also vulnerable to crime, exploitation and harassment through this media. Parental/guardian supervision and common sense guidelines are therefore necessary to ensure that the activities and experiences of children on the internet are safe and productive.

Activities of children on the web

In general, majority of the children online are known to consistently visit a few well known sites. Girls commonly visit television, music and celebrity sites, while boys visit sports or games.

Research done in London for the National Opinion Poll Family, 2000 indicates that children consider the internet as the most valuable source of information. However, as opposed to parents, to children, information refer to, games, sports results and music releases. Contrary to the parent's objectives, children do not use the internet widely for education purposes.

Generally, emerging preferences for young people on internet content includes:

- Commercial and fan sites
- Entertainment and fan sites
- Communication or chat sites
- Picture and visually interesting sites more than printed text
- Games and interactive sites

Risks posed by the internet to children

a) Online enticement

The anonymity of the internet offers adults the chance to pose as children. Young teenagers, through emails and chat rooms, may be lured into virtual relationships with adults with ulterior motives. Such relationships may result to actual encounters.

A paedophile posing as young person with similar interests and hobbies, use the internet to establish online 'friendships'. These relationships may develop to a point where the paedophile gains the trust of a child to set up a face to face meeting.

Such techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

b) Exposure to illegal and harmful content - websites

Children may be at risk of identity theft or participation in hate or cult websites. They also risk involvement in buying and selling of stolen goods without their knowledge. The ease of access to online gambling, suicide sites, sites selling weapons, hacking sites, and sites providing recipes for making drugs or bombs, are also of great concern.

Unregulated use of the internet by young people can also make them become involved in the viewing, possession, making and distribution of indecent and/or child abuse/pornographic images.

c) Online molestation

A child may encounter belligerent, demeaning, or harassing messages via chat, e-mail, or their cellular phones. Additionally, "bullies," typically other young people, often use the Internet to approach their victims. While a young person may or may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological well-being.

d) Viruses and Hackers

A child could download a file containing a virus that could damage the computer or increase the risk of a 'hacker' gaining remote access to the computer, jeopardizing the family's privacy and the family's safety.

e) Legal and Financial

A child could do something that has negative legal or financial consequences such as giving out a parent's credit-card number. While children need a certain amount of privacy, they also need parental involvement.

f) Un-moderated chat rooms

Chat rooms are primarily topic- based but in other cases, they may be loop holes for other unsolicited side topics to be discussed. Similarly, even if the site is exclusively for teenagers, there is no way of telling whether every participant is a teenager. (we may need to qualify this statement so that it can show why involvement in these discussions is

g) Newsgroups Forums and Bulletin boards

These are places where children can read and post messages or download or upload files. Unlike chat rooms, these are not live or real time. They can also be used to post files including computer programs, pictures illustrations and stories. There are however newsgroups that contain sexually explicit stories, illustrations and photographs which are undesirable for children and even in some instances this material may be illegal.

Should children be allowed to access internet given the inherent risks?

The fact that crimes are being committed online is not a reason to stop children from using the internet for it would be like telling them to forgo attending school because students are sometimes victimized or bullied there.

The vast majority of children who use the Internet do not get into major problems even though there have been some highly publicized cases of exploitation involving the Internet.

There are steps parents can take to shield their children from material that is disturbing or inappropriate, although it is almost impossible to completely avoid all such material.

Parents can greatly minimize the chances that their children will be victimized by teaching their children to follow the safety rules discussed below and to instruct them about both the benefits and dangers of “cyberspace” and for them to learn how to be “street smart” in order to better safeguard them in any potentially dangerous situations.

How to ensure children’s safety on the internet

Illegal or harmful websites

Services are available that rate web sites for content, as well as filtering programs and browsers that allow you to block the types of sites you consider to be inappropriate. These programs work in different ways. Some block sites known to contain objectionable material. Some prevent children from entering certain types of information such as their name and address. Other programs keep your children away from chat rooms. Check with your ISP (Internet Service Provider) to see what is available and remember if you have older children, be honest and let them know why and how you are protecting them.



On most internet search engines you can turn on a 'Safe Search' mode which removes adult sites or sites containing explicit sexual content from search results. It's not 100% accurate, but using a safe search option does eliminate most inappropriate material. You should select Strict Filtering which removes adult content from both image and web search results.

Newsgroups Forums and Bulletin boards

Advise children to:

- Be aware that the biggest risk is that they post something that reveals information about them. In many cases, the mere act of posting something makes their email address public which then allows spammers to send them junk email, often of a pornographic nature, or individuals to send undesirable emails.
- Chose their newsgroups carefully.

Chat rooms

On the internet they should always remember that people they meet might not be who they seem.

Be suspicious of anyone who tries to turn them against their parents, teachers, or friends. They may have a hidden agenda.

Never get together with someone they "meet" online without knowing who they are. If they do feel it is appropriate to meet with someone, they should discuss it with you and never go to the meeting alone. The meeting should be in a public place, like a coffee shop, restaurant or shopping centre that they are familiar and comfortable with. The safest procedure is to have you talk with the parents of the other person and for both children to bring their parents along on the first meeting.

Be careful when they enter into a private chat area where they can arrange to meet friends they know. In some cases, those rooms are truly private. But in others, they may be listed in a directory of rooms, where there is nothing to stop others from entering.

If you have a daughter, she should choose a gender-neutral name - like your initials or a word - to use in a chat room. It is fine to be cute or funny with the name you choose, but they should be sure that the name does not identify them and does not have any meaning or implication that might encourage other users to bother them.

Spam e-mails

Never reply to a suspicious looking email or click on a web link contained in one. Replying to a spam email or taking an action based upon it confirms that the email



Child safety and internet use

address is live. The spammer will send more email and probably share their list with other spammers who will also send your child email.

Remember that spam (or other) email messages can appear to come from a fake address which may look harmless. So don't automatically trust an email because it appears to originate from a friendly source.

Respond carefully to email and never send personal information to someone you don't know.

It is a good idea to turn off automatic downloading of images as many spammers add a tracking image in the email which tells them you have read their email and then start the email deluge. In many email programs, it is possible to turn off the automatic downloading of images at:

Tools > Options > Security > Change Automatic Download Settings

You can add specific senders to your trusted senders as you receive messages so it's easy to use.

Be aware that email is not at all secure. Each email passes through many points and can be read easily.

Never send credit card information by email - either submit it through a secure website or use the phone. Extracting personal information from an email, especially credit card information where there is a fixed pattern (4 blocks of 4 numbers) is fairly easy.

Other safety measures include:

If you have cause for concern about your children'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.

Having open communication with your children, using computer resources, and getting online yourself will alert you to any potential problem that may occur.

If your child tells you about an upsetting message, person, or web site encountered while online, do not blame your child but 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 how they learn to deal with problems on their own.

Check with your service provider to see if they offer age-appropriate parental controls. If not, consider using a software program that blocks chat areas, newsgroups, and web sites that are known to be inappropriate for children. Most of these programs can be configured to filter out sites that contain sexually explicit content, hateful or violent material or that advocate 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 programs at www.getnetwise.org/tools. Always remember that filters or internet rating system are not a substitute for parental involvement.

The best way to be sure that your children are having positive online experiences is by staying in touch with what they are doing. Spend time with your children while they are online and have them show you what they doing.



Rules that children should observe

- Not to give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without parents' permission.
- Children should alert parents/guardians right away if they come across any information that makes them feel uncomfortable.
- Never agree to get together with someone they "meet" online without first checking with parents. If parents agree to the meeting, then it should be in a public place and the child must be in the company of the parent /guardian.
- Never to send a person their picture or anything else without first checking with parents.
- Not to respond to any messages that are mean or in any way make them feel uncomfortable. It is not their fault if they get a message like that, but if they do they will tell the parents right away so that they can take the appropriate action.
- To talk with their parents so that they can set up rules for going online. Decide upon the time of day that they can be online, the length of time, and appropriate areas to visit. Not to access other areas or break these rules without the parent's permission

For more information contact the Communication Commission of Kenya on the following address:

**THE DIRECTOR GENERAL,
COMMUNICATIONS COMMISSION OF KENYA
P.O. BOX 14448, NAIROBI, 00800**
Email: info@cck.go.ke
Website: www.cck.go.ke

Acknowledgement

This Fact Sheet was developed in partnership with Teknobyte (Kenya) for the Consumer Education Outreach Programme by the Communications Commission of Kenya.

Disclaimer

All attempts have been made in order to ensure that the information contained in this publication is accurate. However, the document is intended as guide only. Readers should ensure that they verify on their own any information contained in this document upon which they intend to rely as a basis for taking any action or making any decision. The Commission will not accept liability for the information contained



Child safety and internet use

in this document or for consequences of any actions taken or decisions made on the basis of the information provided.

© 2008 **Communications
Commission of Kenya**