6. Advice children not to post or share personal information online.
7. Advice children not to meet online friends, offline without supervision.
8. Encourage children to inform them of any kind of abuse they experience online.

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

Acknowledgements: This brochure was developed as part of the Consumer Education Outreach Programme of the Communications Authority of Kenya, working in partnership with Teknobyte (Kenya).

CONSUMER AND PUBLIC AFFAIRS
COMMUNICATIONS AUTHORITY OF KENYA
P.O. BOX 14448, Nairobi, 00800
Email: chukuahatua@ca.go.ke
TEL – 020 – 44 55 555, 0714 – 444 555, 0737 – 44 55 55

CA/CPA/CEP/B/03/2014

Children and the use of the Internet

CHUKUA HATUA
Pata huduma ya mawasiliano unayostahili

COMMUNICATIONS AUTHORITY OF KENYA

This brochure has been developed for the **Consumer Education Program** by the **Communications Authority 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 brochure 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

Use of internet in Kenya has increased significantly in recent years and, as a result increasing number of children who now have unsupervised access to the internet (via personal computers or mobile phones.) while children can derive great benefit from internet access, it also renders them vulnerable to risks such as; exposure to fraudulent practices, exposure to unsuitable content and potential harassment from third parties.

Activities of children on the web

Research has revealed that most children use the internet for entertainment. The most visited websites by children include:

- Commercial and fan sites
- Entertainment 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. A paedophile posing as a young person with similar interests and hobbies, uses 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, buying and selling of stolen goods without their knowledge, 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, email, 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 Risks

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

f) Unmoderated chat rooms

Chat rooms are primarily topic- based but in other cases, there may be loopholes for other unsolicited side topics to be discussed. Predators and other criminals usually use chat rooms to lure young people and abuse them physically, mentally and sexually

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.

h) Addiction and Compulsive Behaviour

Young people may log in to websites that my expose them to addictions like gambling and gaming. Such content may incite the young people to aggressiveness and violence.

i) Sexual, violent and illegal content

Unsupervised access to the internet can result in children being exposed to information and images of a sexual, violent and illegal nature. Parents are advised to contact their service provider for information on how to bar access to this type of information.

j) Unmonitored commercial access to children

The Internet provides an unprecedented ease of access to children by a wide range of individuals and/or commercial bodies-most of it without the knowledge or consent of their parents. This can expose children to:

- Unsuitable sales or marketing information.
- Invitations to participate in competitions,betting,gambling
- Material of a frudulent or illegal nature
- Material of violent or sexual nature
- Unsolicited material (spam)

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. It is strongly recommended that the use of internet by children be supervised by parents/guardians and that open discussions should be held between both parties regarding the risks posed and the safeguards on offer.

How to ensure children's safety on the internet

Parents Should:

1. Spend time with their children on the internet, share positive experiences and stay in touch.
2. Be conversant with the internet themselves.
3. Seek advice from their Internet Service Provider (ISP) regarding the activation of protective measures such as filters. A directory of such programmes is available at: www.getnetwise.org/tools.
4. Report any kind of online abuse to the police and the CA.
5. Do not blame or reproach the child if you find them with inappropriate content. Instead, offer help and advice.