

## Introduction

Use of the Internet in Kenya has increased significantly in recent years and, as a result increasing numbers of children now have unsupervised access to it (via a personal computer at home, at friends' houses, at school, at libraries or in cyber cafés; or via mobile-phones). While children can derive great benefit from Internet access, it also renders them vulnerable to certain risks.

## Activities of children on the web

Contrary to the wishes of the majority of parents, most of whom expect their children to access the Internet for educational purposes, research has revealed that most children use the Internet for entertainment. Girls commonly visit sites offering information on; television, music and celebrities, while boys tend to visit those offering information on sports and games.

## The risks posed by the Internet to children

The use of the Internet by children poses the following risks:

### The risk of exposure to on-line enticement

The anonymity of Internet users allows certain ill-intentioned adults to 'pose' as children and thereby lure children or teenagers into 'virtual relationships by means of professions of 'friendship' or shared interests.

### The risk of exposure to websites containing illegal and/or harmful content

Children can also be exposed to; 'identity theft', 'hate- or cult-websites', the unwitting purchase/vending of stolen goods, information on alcohol, online gambling, suicide-sites, sites selling weapons, hacking sites, and sites offering information on such topics as bomb-making or drugs. They can also be exposed to the risks inherent in the viewing of, possession of, taking of, and/or distribution of potentially indecent, abusive or pornographic images.

### The risk of exposure to online molestation

As a result of unregulated use of both the Internet and the mobile-phone, children can be exposed to belligerent, demeaning, or harassing messages or bullies.

### The risk of exposure to viruses and 'hackers'

Via use of the Internet children can unwittingly download destructive computer viruses or make it easier for 'hackers' to access such information as will jeopardize the privacy and safety of the family/educational unit.

### Exposure to financial/legal risk

Using the Internet, a child may inadvertently execute such actions as will expose it/the family to negative financial consequences by, for instance, credit-card information to third parties, some of whom may be fraudsters.

## Sexual, violent and illegal content

Unsupervised access to the Internet can result in children being exposed to information and images of a sexual, violent or illegal nature. Parents are advised to contact their Service Provider for information on how to bar their children's phones from accessing such material.

## Exposure to un-moderated 'chat rooms'

'Chat rooms' are sites where like-minded respondents can exchange virtual 'chat'. Typically interest/topic-based, such sites can provide loop-holes for the discussion of other (unsolicited and negative) topics. Although 'intended' for children or teenagers, such sites can also be visited by



ill-intentioned adults 'posing' as children with the intention of promoting illegal or sexual exchanges.

## Exposure to newsgroups forums and 'bulletin boards'

Typically, these are sites upon which children can read/'post' messages and/or download or upload personal files. Unlike chat rooms, they are not 'live' or operational in 'real time' and can be used to post computer programs, images and unsuitable content. Illegal newsgroups also exist, which display content of a violent or sexually-explicit 'adult' nature, which may be both textual and visual.

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

The existence of unsuitable content on the Internet is not, necessarily, a reason to preclude its access by children, particularly since the majority of the content offered is of educational or entertainment value. It is, however, strongly recommended that the use of the Internet by children be supervised/regulated by their parents/guardians or mentors; and that open discussions should be held between both parties regarding the risks posed and the safeguards on offer.

## Protection against the risks posed by illegal or harmful websites

A number of services are offered, which are designed to 'rate' websites and 'filter out' unsuitable content. Facilities also exist for blocking access to sites that are deemed inappropriate for children. For further information on such topics, parents/guardians are advised to contact their Internet Service Providers (ISPs).

## Safe search

Most search engines permit a 'safe search' mode, which automatically preclude access to inappropriate sites. While not 100% accurate, this is effective in denying access to most inappropriate material – particularly when the 'strict filtering' mode is selected.

## Parental responsibility

Parents/guardians are advised to: provide their children with a firm foundation of moral and ethical behavior with regard to the Internet; to encourage discussion and feed-back; encourage children to tell them immediately about any worrying communications; and advise them NEVER to respond to any messages that are suggestive, obscene or threatening.

### Common-sense procedures

Parents/guardians wishing to ensure the optimum safety of their children's Internet use should:

- Spend time with their children on the Internet, share positive online experiences and 'stay in touch'.
- In the event of children sharing concerns about their having received disturbing or otherwise inappropriate content via the Internet, parents/guardians are advised NOT to blame the child for this but, rather, to offer help and advice.
- Seek advice from their Service Provider regarding the activation of protective measures such as barring, filters and other such preventative measures. A directory of such programmes is available at: [www.getnetwise.org/](http://www.getnetwise.org/) tools.
- Remember that the use of the above is not a substitute for parental guidance and supervision.