



COMMUNICATIONS
AUTHORITY OF KENYA



A GUIDE TO CHILD ONLINE PROTECTION



Child Online Protection Guide

1. What Is Child Online Protection?

The internet is one of the most powerful communication and education tools ever invented and many people around the world are gaining access to it. Like with anything that powerful, there are some negative effects to it.

Protecting children online is a global problem that requires concerted efforts of parents, guardians, government, organizations that are children centric among others. Children are a vulnerable group and there have been many cases of children unknowingly getting into dangerous situations that sometimes have detrimental effects to them.

The Authority as the ICT Regulator is mandated to protect consumers of ICT services and this includes children. To that end, the Authority has developed this Child Online Protection Guide to create awareness on how we can all ensure children are safe online.

2. What the Law says about Protecting Children

Article 29 (D) of the Kenya Constitution states that 'Every person has the right to freedom and security which includes the right not to be subjected to torture in any manner, whether physical or psychological. The Constitution in Article 46 (C) on Consumer Protection states that 'Consumers have the right to the protection of their health, safety and economic interests.

The Children's Act No.8 of 2001 makes provision for parental responsibility, fostering, adoption, custody, maintenance, guardianship, care and protection of children. This provision extends to protecting children in the cyber space.



3. Types of Online Crimes (Definitions)

The internet is a global tool and therefore people from all over the world, people from all walks of life and people with varying intentions have access to this tool.

The online society has different types of crime that occur and just like in the physical society; we need to protect ourselves and those we care for from the crimes.

We have highlighted different types of cyber-crime below. Of importance to note is that as the internet becomes more accessible, the nature and complexity of crimes are also evolving.

A Solicitation of a Minor

Solicitation of a minor involves asking or engaging in a conversation with a minor and during the course of that conversation, asking the minor for a physical meeting. The intentions of these meeting could be to lure the child to commit crimes, engage in sexual acts or to kidnap the children and seek ransom.

Criminal befriend children and establish an emotional connection with the motive of lowering the child's protective instincts in preparation for exploitation.



B Cyberbullying

Bullying is a vice where children or teenagers harass, threaten, insult, tease and blackmail other children. Cyberbullying is the same behavior extended to the online platforms such as mobile phones, websites, blogs and chat rooms.

Cyberbullying can be an extension of face-to-face bullying, or it can be a form of retaliation by victims of face-to-face bullying.

Cyberbullying takes many forms and sometimes the bullies will use someone else to do their dirty work and this could involve adults. Cyberbullies can also directly attack their victim by sending them insulting, threatening and blackmailing messages, impersonating them online, posting distasteful information on blogs, websites and chatrooms about the victim.

Unlike face-to-face bullying where one can get away, cyberbullying is harder to control as it can be carried out anonymously. It also spreads wider faster, has a greater degree of publicity, the content is available 24 hours a day and can invade the victim's privacy even in 'safe' places like their homes.

Research shows that children and teenagers rarely tell adults about their experiences of online bullying and do not fully capitalize on the tools provided by communication technologies to prevent future incidents.



C Identity Theft and Online Fraud

The internet is largely unregulated and it has become easy for criminals to steal someone's identity. Online identity can be stolen through various ways including intentionally sending a virus to user's devices which enable criminals to retrieve personal information, fake online sales and auction and phishing e-mails that claim to be from official entities. Methods of identity theft are constantly evolving and users need to be careful at all times.

Once an identity is stolen, it can be used by the criminals to carry out all manner of online crimes referred to as online fraud. Online fraud takes many forms including:

- * **Criminal identity theft** - assuming ones identity with the aim of committing crimes such as threatening national security or committing acts of terrorism. Victims of criminal identity theft have been apprehended and arrested wrongfully.
- * **Financial identity theft** - assuming someone else's identity to obtain credit, goods and services. Others run up huge amounts in debts then file for bankruptcy in their victim's name ruining the victim's credit history and financial reputation.
- * **Identity cloning** - using someone else's information to assume his/her identity in daily life. Using the identity to write e-mails, post on social media, apply for official documents such as passports, social security and bank accounts.
- * **Medical identity theft** - using someone else's identity to obtain medical care or drugs.

Children are exposed to these kinds of crimes when they go online and cyber criminals can trick children into giving personal information about themselves, their parents or other adults in their lives. This information is then used to commit various crimes both online and offline.



D Child Pornography



The internet has created opportunities for sexual abuse and exposure to pornographic content and this has harmful impact on children.

Pornography refers to images, films and, writings depicting sexually explicit activities. Child pornography refers to images, films and in some cases, writings depicting sexually explicit activities involving a child. It can be carried out in various forms including;

- * **Nudity** - images or films of naked or semi-naked children in inappropriate settings.
- * **Erotic Posing** - deliberately posed for pictures or films of children fully, partially clothed or naked in sexualized or provocative poses.
- * **Explicit sexual activity** - Refers to pictures or films that depict sexual activities involving children.

The Internet has escalated child pornography by increasing the amount of material available, the efficiency of its distribution and the ease of its accessibility. This is made worse by the fact that this material can be accessed anonymously and can be shared.

Child pornography can have devastating physical, social, and psychological effects on children. Parents and guardians are responsible for protecting their children against sexual exploitation. The Children's Act No. 8 of 2001 part II Article 15 states that:

"A child shall be protected from sexual exploitation and use in prostitution, inducement or coercion to engage in any sexual activity, and exposure to pornographic materials. Anyone found engaging in activities contrary to this shall be imprisoned for a term not exceeding 12 months."

4. Internet Addiction

In as much as the internet is a good platform for communicating and learning, it is also highly addictive. Internet addiction is described as an impulse control disorder and is very similar to pathological gambling. Individuals, children or adults, can get addicted to the internet and this has an effect on their lives as well as relationships with people in the real world.

There are some tell-tale signs of someone who is addicted to the internet that we can look out for.

Signs of Addiction

- * Rising amount of time spent on the internet
- * Time management problems
- * Problems in school (or work) life such that they experience difficulties in doing everyday lives such as studying or working
- * Health problems such as lack of sleep

- * Arising conflict with family members and co-workers as they are easily irritated when not online or when they feel their online activities are being interfered with
- * More priority on cyber world than real world - dependence on online relationship
- * Feel depressed when internet use is reduced
- * Most of them think they are not addicted and become defensive when this is mentioned

Stages of Addiction

Internet addiction, just like any other type of addiction, occurs in stages ranging from mild to chronic. The three stages are highlighted below;

- * **Curiosity** - the individual starts off by visiting various websites, social media sites, gaming sites and others out of curiosity then this becomes a habitual access
- * **Substitute satisfaction** - The individual has increased expectation to use the internet and they pursue their life's satisfaction online. They have very strong online presence and good relationships online. In case of addiction to gaming, one gains respect due to their excellence in the game.
- * **Escape from real world** - in the chronic stages, the individual is fully immersed in the cyberworld and they want to be connected to the internet through out. The individual is also in denial of real life social order such as working, studying and relating to real people.

Guidelines to Prevent Online Addiction:

1. Do not turn on the computer without a specific purpose. In case of the mobile phone, switch off the data and only put on to do something specific.
2. Set internet access time through a family discussion and stick to what has been agreed
3. Make a habit of keeping a log on time and use of the computer or mobile. There are time management software and applications available if unable to control the use of the Internet.
4. Spend more time on outdoor activities and other hobbies instead of using the Internet.
5. Do not skip meals or break regular bed time due to excessive internet use.

Safe Online Tips for Children

Remember, always respect parental and adult controls that have been put in place to protect your online safety. Listen to their guidance on which sites you should visit, how long you spend online and how you can use the sites you visit, obey age limits on sites. Finally, don't believe all the information you read or see online. Ask your parents, your teachers or trusted adults if you're in doubt.

Using the Internet is fun and you can do a lot of great things. Enjoy it most by keeping yourself safe by following these **SMART** rules:

BE SMART ONLINE

S Set Your Limits

1. Take care of your privacy and that of your family and friends. You might have the feeling of being anonymous online but collecting information from various sources can reveal too much private information about yourself or others you are close to, including your family.
2. If you join a social networking site use the privacy settings to protect your online profile so that only your friends can see it. Use a nickname that your real friends will be able to recognize.
3. Think twice before you publish or share anything online. Once you post information, photographs or any other material on the Internet, you may never be able to remove it or prevent other people from using it. You can never know for sure where it might end up.
4. Always double check the information from other reliable sources.
5. You have rights and you, as well as other people, should respect them. You should never accept harassment or bullying by other people.

**M Meeting Online/
Friends Offline**

1. Think twice before meeting an online friend in real life. If you still would like to meet an online friend offline, you should always ask your parent or another trusted adult to join you to avoid any trouble in case the meeting turns out to be a disappointment.
2. Bear in mind that people lie and your online friend might turn out to be a different kind of person than you thought he or she would be.

**A Accepting
Invitations/
Friendships**

1. Through online connections you can connect with people previously unknown to you. You may get requests by strangers who want to be included in your contact list and see your profile, but it is not wise to accept them. If you are not sure about an invitation, there's nothing wrong with declining.



R React

1. Protect yourself from inappropriate content by not visiting such pages or sharing such content with others. If you see something that bothers you, talk about this with your parents or an adult you trust.
2. Ignore bad behaviour and leave unpleasant conversations or sites with inappropriate content.
3. Block anyone approaching you using rude, intruding or threatening emails or comments.
4. Always be alert if someone, especially a stranger, wants to talk to you about sex or anything that makes you uncomfortable. You should tell a trusted adult and block or ignore the person.
5. If you have been lured or tricked by someone into engaging in sexual activities or transmitting sexual images of yourself, you should always tell a trusted adult in order to receive help and also report it. No adult has a right to request things of that particular nature from a child or a young person.



T Tell Someone About Your Concerns

1. If you have any concerns or problems while online, you need to tell someone you can trust. Your parents or some other trusted adult can help and give you good advice. No problem is too big to be solved!
2. You can report harmful or inappropriate content or activities on the websites to the abuse e-mail of the host of the site.
3. You can report illegal content to an Internet Hotline or to the police.
4. You can report illegal or possibly illegal activities to the local police.
5. In addition to taking good care of yourself, you should also take care of your computer or mobile device



Safe Online Tips for Parents/Teachers or Guardians



KEY AREAS FOR CONSIDERATION	
Safety & security of your personal computer	a. Keep the computer in a common room b. Install firewall and antivirus software
Rules	a. Agree on house rules about using the Internet through the computer and other devices and giving particular attention to issues of privacy, age inappropriate places, bullying and stranger danger b. Agree on rules about use of mobile devices
Parents', Guardians' and Teachers' education	a. Parents, guardians and teachers should be familiar with the Internet sites used by their children and should have a good understanding of how children spend their time online b. Parents, guardians and educators should understand how children use other personal devices such as mobile phones, games consoles, MP3 players, PDAs, etc c. There are basic ways to monitor activities being carried out on the internet such as sites visited. There are also software's and applications available to monitor internet activities including time spent online.
Children's education	a. Educate your children on the risks associated with sharing personal information; arranging face-to-face meetings with a person/s met online; posting photographs online; making use of the webcam; etc.
Communication	a. Communicate with your children about their online experiences

5. What to do when you encounter Online Abuse?

Should you encounter any form of online abuse report through the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) through the contact below:

Website: <http://www.ke-cirt.go.ke>

Email: incidents@ke-cirt.go.ke

Tel: +254-20-4242000/446 or +254-20-4242000/446

Telephone Hotlines: +254-732-444274/276/581/582/721 or +254-703-123897/890/841/846/850



CHILDLINE KENYA
Lower Kabete Rehab Centre
Website: <http://www.childlinekenya.co.ke>
P. O. Box 100003-00100, Nairobi
Email: info@childlinekenya.co.ke
116@childlinekenya.co.ke
Telephone: 0727-637076/0735-813344
or 020 2059722



THE CRADLE - The Children Foundation
Swiss Cottages (Apartment No. 1)
Riverside Ring Road, Kileleshwa, off Riverside Drive
Website: <http://www.thecradle.or.ke>
P. O. Box 10101-00100, Nairobi
Email: info@thecradle.or.ke
Telephone: 0722-201805/0734-798199
or 020 3874575



KENYA ASSOCIATION OF
PROFESSIONAL COUNSELLORS
2nd Avenue Parklands, off Limuru Road
Website: <http://www.kapc.or.ke>
P. O. Box 55472-00200, Nairobi
Email: nairobi@kapc.or.ke
Telephone: 0721-296912/0733-761242
or 020 3741051/3741056/3741123



DEPARTMENT OF CHILDREN SERVICES
NSSF Block A and C
P.O. Box 40326 - 00100, Nairobi
Telephone: 020 2729800
Email: info@labour.go.ke
watotoidara@gmail.com



What Have You Learnt Today:



In partnership with:

