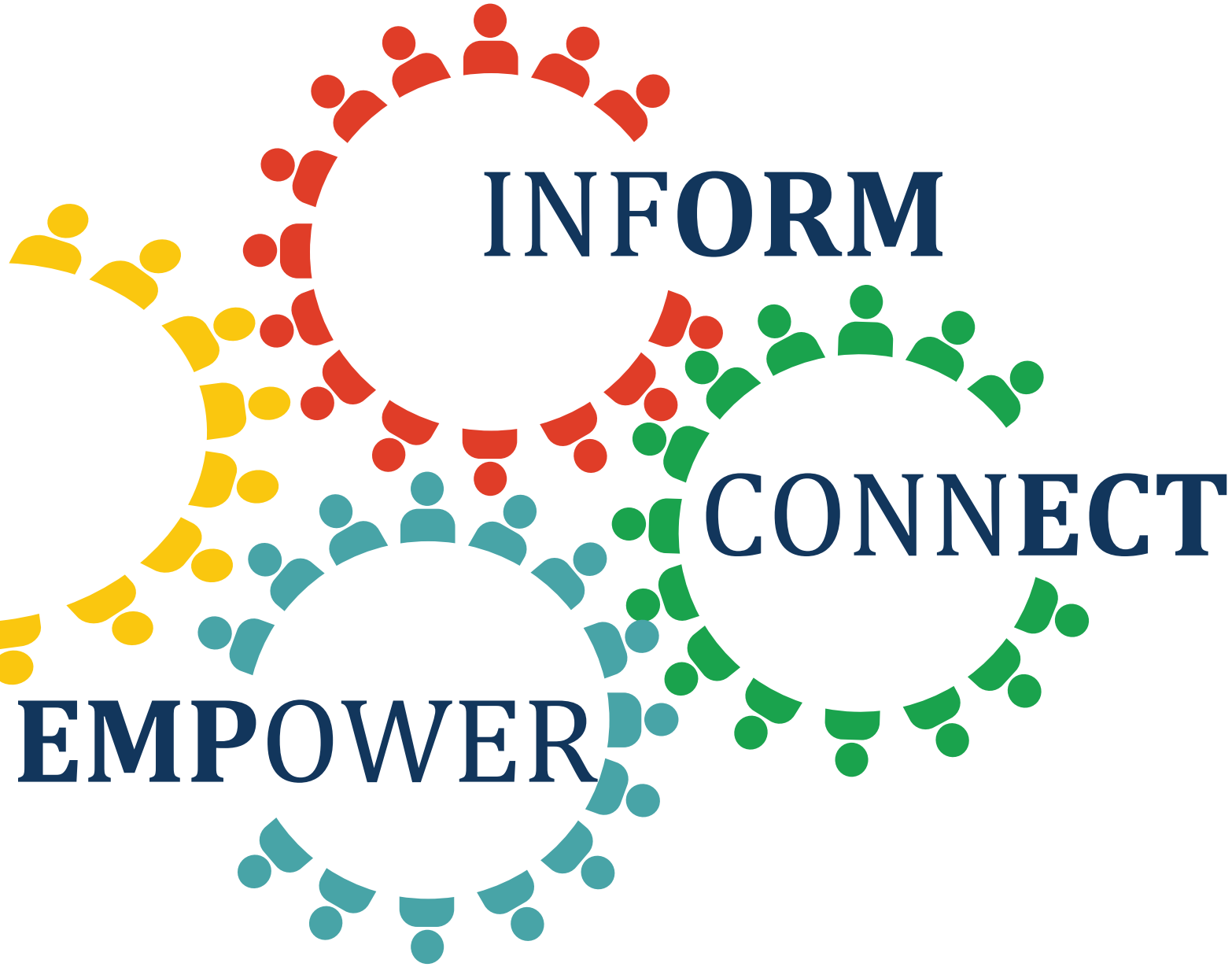


Online Safety Education Toolkit for Young People in Uganda

Internet Society Uganda chapter

TOOL KIT OUTLINE

a quick starter guide

2014

About The E-safety Education Tool Kit

We all must realise that the internet is used for many positive activities; however, children also face some serious risks, such as online predatory, cyber bullying and consequences from revealing too much personal information. Young children may encounter these risks during common online activities like school research, chatting with friends, or updating their social networking pages.

A crucial part of keeping children safer online is by teaching them about the online risks and how to make responsible decisions. This online Safety Education Kit has been developed to sensitise and prevent online victimisation of young children and youth by teaching them how to stay safer online and offline.

Toolkit Goals

- Educate students on how to recognise online and offline potential internet risks
- Engage children and the young adults in a two-way conversation about online and offline risks
- Empower children to help prevent themselves from being exploited online, or to report victimisation to a trusted adult
- Support and enhance community online safety education efforts

WHO SHOULD USE THIS KIT?

This kit is designed to be convenient and ready to use for young people in Uganda between ages of 5 -20 years. Whether you access internet at school, home, internet café or mobile phone, this kit has all of the tools you need to equip you with online safety tips.

WHAT RESOURCES DOES THE KIT CONTAIN?

Within this kit, you will find the following resources:

- **Online Safety Resources:** - Guides that include full descriptions of online safety resources as well as an overview of the primary online safety risks
- **Online Safety Pledges:** Hangouts for nursery, primary and secondary students that outline clear, simple guidelines for safer Internet use.
- **Online Safety Rules and Posters:** - Single-sided poster which displays the online safety rules

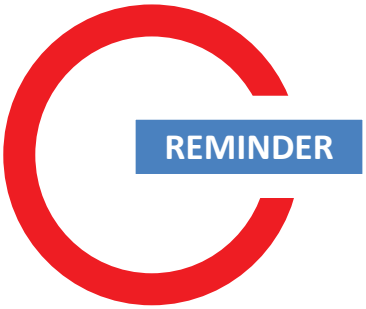
WHERE CAN I FIND MORE E-SAFETY MATERIALS?

On the Internet Society website (www.internetsociety.ug) you can find tips, talking points and expert advice to prepare you on how to stay safe while browsing the internet. You may also preview the other age-appropriate materials ISOC Uganda Chapter has developed for use with children in nursery, primary and secondary schools.

To promote a safer and more positive experience for your children, the ISOC Uganda Chapter has designed a dedicated page which does not link to any outside resources. Here, children can interact with characters play, and watch several animated videos.

CONTACT INFORMATION

For further assistance, please contact us by e-mail at :-info@internetsociety.ug



Please log on to ISOC Uganda toolkitpage to compare your evaluation of these resources. Your feedback will allows us to continue creating free, dynamic tools like this kit. Thank you for your support.

ONLINE RISKS AND SAFETY TIPS

All of the videos and activities for primary and secondary students are based on this tool kit's four rules of online safety. These rules address what children should do if they: -

- See or receive something inappropriate online
- Are asked to share personal information online
- Are asked to meet up offline after an online engagement with a stranger
- Encounter a cyberbully

Technological advances have increased the unmonitored access that youth have to one another. Bullying can now occur through a cell phone, a computer, or a webcam, as well as in person. This "cyberbullying" may be just as damaging as traditional bullying because the victimization does not end when the victim goes home. Taunting SMS texts, comments, e-mails, and instant messages (IM) may continue throughout the night, making the victim dread going to school the next day or interact with fellow peers.

Here are some Common Forms of Cyberbullying

- **Flaming and Trolling** -sending or posting hostile messages to "inflame" the emotion of others
- **Happy-slapping** - recording someone being harassed or bullied in a way that usually involves physical abuse, then posting the videos online for public viewing
- **Cyber stalking** - continuous harassment, including threats of physical harm. Cyberstalkers can be either strangers or people you know, and there are many different motives. The more determined or obsessive stalkers become, the more likely they are to move from one online channel to another until your online presence is fully intruded upon.
- **Identity theft/impersonation** - stealing someone else's password and/ or hijacking their online accounts to send or post incriminating or humiliating pictures, videos and information
- **Photoshopping** - doctoring digital images so that the main subject is placed in a compromising or embarrassing situation
- **Physical threats** - sending messages that involves threats to a person's physical safety
- **Rumour spreading** - spreading gossip through email, text messaging or social networking site like Facebook
- **Denigration**- posting mean comments online through e-mail, IM, chat rooms, online profiles, or websites set up specifically to make fun of someone

A cyberstalker relies upon the anonymity afforded by the internet to allow them to stalk their victim without being detected

- **Exclusion**- intentionally leaving someone out of an online group or community, such as IM buddy lists or friends lists on profile pages
- **Flaming**- online fighting, usually through e-mail, IM, or chat rooms where angry, rude, or offensive messages are exchanged
- **Cyber Harassment**- repeatedly sending malicious messages to someone online
- **Impersonation** - pretending to be other people when sending or posting content that makes them look bad, gets them in trouble, or puts them at risk
- **Outing-** sharing secrets about someone online, including private information,pictures, and videos
- **Trickery-** tricking someone into revealing personal information and then sharing it with others

How to Deal with Cyberbullying

- Do not respond to rude and harassing e-mails, messages, and comments
- Keep a record of the harassment, including the date, time, and description of each call, message, text, or e-mail
- Make a report to a trusted adult. This could be your teacher or guardian. In case of internet based bullying, contact your Internet service provider or telecom provider –incase of SMS and phone call or inform law enforcement authority (police).
- Keep personal information private and share passwords only with parents/guardians.
- Change your passwords often and make sure it is not easily readable

ONLINE PREDATORS

The Internet has significantly increased the opportunities young people have to explore the world and socialize. Since the Internet allows u to talk to many different people, children may encounter people who mean them harm while trying to meet new friends.

Online predators may employ a technique called “grooming” as a means to build trust with a child and eventually lead to an offline meeting.

Online predators usually find kids social networking, blogs, chat rooms, instant messaging, email, discussion boards, and other websites. Young people engaged in a combination of risky behaviours are most vulnerable to this enticement.

For example, children who share sexy photos and hang out in chat rooms talking about sex with unknown people are more likely to be groomed by a predator. Online predators usually

How to look identify a potential online predator

- He/she shows unwanted attention, affection, kindness or even sending online gifts
- Know the latest music, and hobbies likely to interest young people
- Listens to and sympathises with your problems
- Try to ease your inhibitions by gradually introducing sexual content into your conversations or by showing you sexually explicit material.

Tips for dealing with online predators:

- Never download images from an unknown source. Images could be sexually explicit.
- Consult a trusted adult – teacher/parent on how to use email filters.
- Tell a trusted adult immediately if anything that happens that online makes them you uncomfortable or frightened.
- Consider choosing a gender-neutral screen name that does not contain sexually suggestive words or reveal personal information.
- DO NOT reveal personal information about yourself (including age and gender) or information about your family to anyone online and DO NOT fill out online personal profiles
- STOP any email communication, instant messaging conversations, or chats if anyone starts to ask questions that are too personal or sexually suggestive.
- When you are approached online by someone suspicious, block them, DO NOT accept them as a friend, DO NOT meet them offline, and TELL A TRUSTED ADULT.

REVEALING TOO MUCH INFORMATION

Social Networking sites such as Face book, Instgram and MySpace can often be used as forums for revealing too much. These networks often include personal and identifying information such as real first and last names, phone numbers, names of schools, or one's age and gender. Even if users employ the sites' privacy settings, their profiles can still be accessed by those who are added to their friends' lists.

Young people can also reveal too much information while using a webcam or cell phone. Cell phones, for example, have become extensions of the computer because they allow Internet access. These technologies have increasingly been used to take and send inappropriate photos and videos. These images can then be sent to other users. This phenomenon is sometimes referred to as "sexting," and it may lead to criminal prosecution.

Sexting is when someone sends or receives a sexually explicit text, image or video on their mobile phone, usually in a text message. Examples include sending or receiving:

- naked pictures or 'nudes'
- 'underwear shots'
- sexual or 'dirty pics'
- rude text messages or videos

They can be sent from a friend, boyfriend, girlfriend or someone you've met online.

Tip! Find out how you can stay in control and what to do if a photo has fallen into the wrong hands.

If a minor takes a nude picture of another minor, even if it is of him or herself, it can be considered the production of child pornography. If the picture is sent to someone else, it can be considered the distribution of child pornography

Risks of Revealing Too Much

Anyone can access a your personal information and may use it to harm you
Cyberbullies may use your personal information as a weapon to spread rumours, distribute incriminating photos or conversations, or impersonate the you online
Scammers may identify children who reveal personal information as easy targets for manipulation

Tips to Help Children Avoid Revealing Too Much

DO NOT post e-mail addresses or cell phone numbers on your social networks
DO NOT share with anyone apart from trusted adults
DO NOT talk about sex or other provocative subjects online
DO NOT respond to emails or messages requesting personal information
Delete e-mails from unknown senders.
Utilize privacy settings to block out any one you do not know in person

Online Safety Tips for Primary and Secondary Students

My Rules for Internet Safety

Primary

The Internet is where I learn and play
But I have to be careful everyday
So I pledge to be safer online
And follow these rules all of the time:

1. I will tell my trusted adult if anything makes me feel sad, scared, or confused.

2. I will ask my trusted adult before sharing information like my name, address, and phone number.

3. I won't meet face-to-face with anyone from the Internet.

4. I will always use good netiquette and not be rude or mean online.

signed .....

signed .....

Internet Safety Rules

Secondary School

1 I WILL THINK BEFORE I POST.

I agree not to post information and images that could put me at risk, embarrass me, or damage my future, such as

- » cell & home phone numbers
- » home address
- » sexual messages
- » inappropriate pictures and videos

2 I WILL RESPECT OTHER PEOPLE ONLINE.

I will not

- » post anything rude, offensive, or threatening
- » send or forward images and information that might embarrass, hurt, or harass someone
- » take anyone's personal information and use it to damage his or her reputation

3 I WILL BE CAREFUL WHEN MEETING ONLINE FRIENDS IN PERSON.

I agree to

- » ask my parent or guardian's permission
- » have a parent or guardian accompany me
- » meet in a public place

4 I WILL PROTECT MYSELF ONLINE.

If someone makes me feel uncomfortable or if someone is rude or offensive, I will

- » not respond
- » save the evidence
- » tell my parent, guardian, or another trusted adult
- » report to the website, cell phone company, cybertipline.com, or the police

STAMP

STAMP

5: SMART rules

Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your e-mail address, phone number and password.

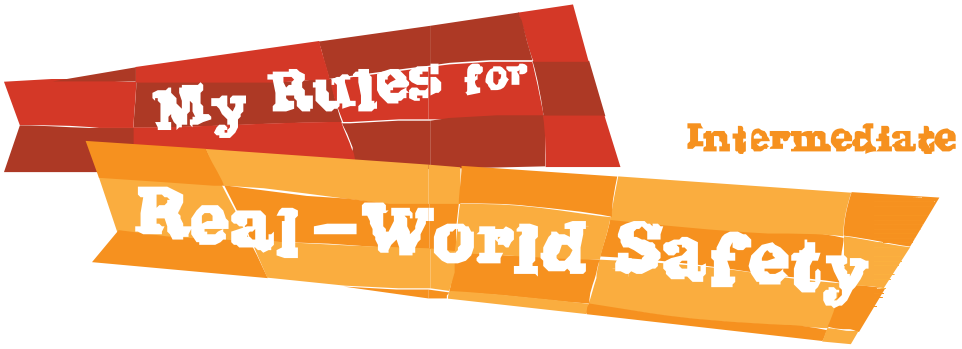
Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

Accepting: Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites,books or trusted adult. If you like chatting online it's best to only chat to your real world friends and family.

Tell: Tell your parent, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Online Safety for Intermediate & Middle School Students



Your School Logo Here

1 I will always check first with my parent, guardian, or other trusted adult before going anywhere, helping anyone, accepting anything, or getting into a car.

2 I will take a friend with me when going places or playing outside.

3 I will tell people "NO" if they try to touch or hurt me. It's OK for me to stand up for myself.

4 I will tell my trusted adult if anything makes me feel sad, scared, or confused.

signed .....

signed .....

Always ask a grown up before you use the internet. They can help you find the best thing to do.

Don't tell strangers where you live, your phone number or where you go to school. Only your friends and family need to know that.

Don't send pictures to people you don't know. You don't want strangers looking at photos of you, your friends or your family.

Tell a grown up if you feel scared or unhappy about anything.

Additional Resources

- Children's activity on internet security: -Budd:e (https://budd-e.staysmartonline.gov.au/primary/demo.html)
- Connect with Respect Quiz- take a test to find out how well you connect with respect:- http://www.sharetakecare.co.uk/
- Take the Connect with Respect Quiz: http://www.saferinternet.org.uk/safer-internet-day/2013/quiz
- Accidental Outlaw: - Quiz to test your knowledge about the law online http://accidentaloutlaw.knowthenet.org.uk/)
- Thinkuknow: -http://www.thinkuknow.co.uk/
- Cyber smart:- http://www.cybersmart.gov.au/

About the Internet Society Uganda Chapter

The Internet Society is a global organisation with over 100 organisational and more than 44,000 individual members in over 80 Chapters around the world. The organisation attracts individual and organisation members bound by a common stake in maintaining the viability and global scaling of the internet.
The Internet Society Uganda Chapter is a non-for-profit organization based in Uganda with the aim of promoting the open and transparent development on the internet in Uganda while working with different like –minded institutions Uganda.

Contact Us
Plot 10 Kenneth Dale Drive, Kamyokya
P.O. Box 32330, Kampala
Email:info@internetsociety.ug
Tel: +256791032473, +256312202393
Facebook:https://www.facebook.com/internetsociet-yug
Twitter: @ISOC-UG

2014