E-SAFETY EDUCATION TOOLKIT FOR YOUNG PEOPLE IN UGANDA

Follow!

NEWS

hi!

230

Internet Society
Uganda Chapter

Content:

About The E-Safety Education Tool Kit

This Toolkit has been developed to guide young people on how to stay safe online in Uganda. The internet and other technologies have drastically changed the way children interact with their world thus becoming a major part of nearly every aspect of our lives. Today's children have access to the internet at very young ages; they are comfortable with it and able to interact with it easily. While the internet is full of learning opportunities, it also allows access to inappropriate content and a wide range of things that can place children at risk.

Social networks and web based communication tools allow people to interact by sharing information on a variety of platforms, has changed the way we communicate. Some of the most popular social networking applications young people are using to communicate include- Facebook, Twitter, Instagram, Snapchat, and WhatsApp. While the sites themselves are not harmful, the atmosphere of perceived anonymity created by non-face-to-face communication can become dangerous to children and young adults since they are more likely to engage in risky behaviour not normally considered in actual face-to-face situations.

The good news is that if armed with the right information and skills, children and adults can safely use technology, avoid risks and respond effectively to unsafe situations. Adults who recognize the risks will be better prepared to intervene and lessen the potential negative impacts.

This Toolkit created in collaboration with child online experts helps provide information needed to keep young people safe. This E-Safety toolkit has been developed to sensitise young people on how to stay safe online and offline and to prevent their online victimisation.

Toolkit Goals

1 Educate young people on how to recognise online and offline potential risks.

2 Engage young people in a two-way conversation about online and offline risks.

3 Empower young people to help prevent themselves from being exploited online, or to report victimisation to a trusted adult.

4 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 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:

1 **Online Safety Resources:** Guides that include full descriptions of online safety resources as well as an overview of the primary online safety risks.

2 **Online Safety Pledges:** Hangouts for nursery, primary and secondary students that outline clear, simple guidelines for safer Internet use.

3 **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 Uganda Chapter 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- **info@internetsociety.ug**

REMINDER!

Please log onto the Internet Society Uganda Chapter toolkit page 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 for young people

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 cyber bully

Cyberbullying

Technological advances have increased the unmonitored access that young people 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 for a long.

Cyberbullying is the use of Internet and mobile technologies to harass others. It includes spreading mean rumours, posting embarrassing images, impersonating others, and sending threatening messages.

Cyberbullying usually involves a victim, one or more bullies, and one or more bystanders. Victims of cyberbullying may react in a number of ways. Some kids and teens shrug it off; others are more severely affected. They may have low self-esteem, get bad marks, avoid going online or going to school, and change schools.

If you're being cyberbullied

- Don't respond.
- Block the bullies.
- Save any evidence.
- Report to the website.
- Remember you're not alone! Talk to friends and an adult you trust.

If you're thinking about cyberbullying

- Stop! Think about how being cyberbullied would make you feel.
- Calm down. Try talking to a friend or trusted adult.
- Consider the consequences. You could get in trouble at school or with the law.

If you're a bystander

- Don't share or like cyberbullying comments or images.
- Support the victim. For example, send or post a kind message.
- Report cyberbullying.

How to Deal with Cyberbullying

1. Do not respond to rude and harassing e-mails, messages, and comments
2. Keep a record of the harassment, including the date, time, and description of each call, message, text, or e-mail
3. 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)
4. Keep personal information private and share passwords only with parents/guardians.
5. Change your passwords often and make sure it's STRONG not easily readable.

Discussion Prompts

1. Do you think cyberbullying is a problem in your school/ community? Why or why not?
2. How do you think people who are cyberbullied feel?
3. Have you ever witnessed any one being cyberbullied? What did you do?
4. Have you ever made a report about cyberbullying? What happened next? Did you feel like the problem was solved?
5. Brainstorm some ways your school/community can fight cyberbullying.

SAVE
Any evidence of the bullying & show an adult.

BLOCK
Messages or the person. DO NOT Respond to them.

LOG OFF
The site where the bullying is happening.

TALK
Talk to someone you trust about it.

Source: Get2ICT Kids computing club

Digital Ethics

Digital ethics is about following the online rules – even if no one is there to catch you breaking them. One of the most important online rules is respecting content posted by other people. This includes not pirating (stealing) copyrighted content like movies and music; and giving credit to the creators of any text, images, or music that you use

If you quote an online article in a paper, **you should credit the author. Failure to do so is called plagiarism – which is a type of cheating.** The Internet has made it easier to plagiarize and cheat in other ways, such as posting homework solutions online and texting each other test answers. Sometimes the line between cheating and using the Internet for "help" may seem blurry, so it is important to talk to teachers about their expectations for each assignment.

Discussion Prompts

1. **How can you tell if something you've read online is true?**
2. **Have you ever read something online you thought was true, only to find out later it wasn't?**
3. **What would make you suspicious of a website?**
4. **Name three clues that can help you tell if a website is trustworthy.**
5. **Have you ever filled out an online offer form promising a free item? What happened next?**

Inappropriate Content

You can find almost anything online – from videos about kittens to mature content with violent, hateful, or sexual themes. A lot of this mature content is inappropriate for young people under 18.

It can be especially disturbing for younger children, but even older teens may be bothered if they come across this content unintentionally. **It is important to remember that it is not your fault if you accidentally come across inappropriate content online.**

Try to avoid inappropriate content by double checking the URLs you type and being careful about clicking on unknown links.

In addition to encountering inappropriate content online, kids and teens may also share and post inappropriate comments and images. While it is best to refrain from illegal or inappropriate actions in the first place, some people have gotten into more trouble by sharing comments or images about them online.

TIP! If someone shares or asks you to share inappropriate content, consider blocking that person and reporting them to the website or an adult.

Think before posting:

1. Drinking and drug use
2. Hate speech
3. Vulgar or offensive gestures
4. Profanity
5. Revealing or suggestive images
6. Threats

Discussion Prompts

1. **Have you ever come across any content online that bothered you?**
2. **Who would you talk to if you came across content online that bothered you?**
3. **Would anyone be embarrassed or hurt by the information you share online?**
4. **Have you ever seen any posts from friends that changed the way you thought about them?**
5. **What do you think the information you've shared online says about you?**

Online Privacy

Many people share information about themselves online through comments, images, and text messages. But once you put information online, it's easy to lose control of it. Anyone with access to your social media accounts may copy, share, and alter the information. That's why it's important to take precautions to keep your information safe online. Create strong passwords (and don't share them), consider friend requests carefully, and only accept people you know you can trust.

Those who reveal too much personal information online have become targets for identity theft, scams, computer hacks, and other trouble. **Before sharing personal information, it is important to check websites for signs that they are trustworthy.** For example, before entering financial information like a credit card number on a website, check the URL for "https" or the lock symbol.

Think before posting:

1. Addresses
2. Financial information
3. Passwords
4. Phone numbers
5. Personal Schedules
6. Social security numbers

Discussion Prompts

1. **What do you do to keep your online information private and secure?**
2. **How do you decide who to add to your friends' list?**
3. **When do you think it's OK to share personal information online?**
4. **How frequently do you change your passwords?**
5. **Have you ever had anyone steal a password? What happened next?**

TIP!
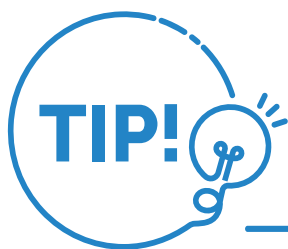
A strong password MUST have a Capital letter, small letter, number and special character like !#*&

Unwanted Sexual Requests

While online, young people may receive unwanted requests from adults asking them for nude images, to have a sexual conversation, or to meet offline for sex. These requests may come from people they've met online or know in real life. They may also come from their peers or young adults.

Most kids and teens are smart about dealing with sexual requests. They remove themselves from the situation, ask the people to stop, or change their personal information. But receiving these requests can still be distressing. **You should never respond to any requests you receive. Instead, report them to the website and an adult you trust immediately.**

In some cases, adults may target kids and teens for months before making a request. These adults are often called "online predators." They use a process called "grooming" to gain their victims' trust and form a relationship with them.

Adults should not pursue any kid or teen romantically. If an adult acts interested in a romantic relationship with you or your peers, it's a red flag signalling they cannot be trusted. **You should not engage them, refuse to talk to them about sex or meet them offline and tell an adult you trust.**

Someone trying to groom kids and teens may:

1. Flatter them.
2. Talk to them about sex.
3. Send them gifts, such as cell phones or bus tickets.
4. Ask them to keep secrets.
5. Try to isolate them from family and friends.
6. Share or ask them to share revealing images.

Discussion Prompts

1. **Do you know anyone who has received an unwanted sexual request? How did they respond?**
2. **Why do you think teens are tempted to meet offline?**
3. **Who would you tell if you received an unwanted sexual request?**
4. **What advice would you give a peer who received an unwanted sexual request?**
5. **Would you be bothered by an unwanted sexual request? Why or why not?**

TIP!
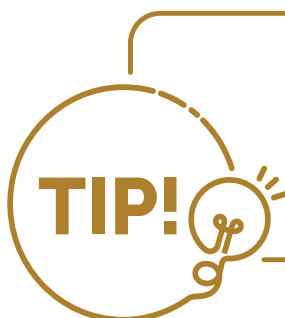
Report unwanted sexual request to the school or trusted adult.

Sexting

Sexting is when minors (those under 18) share sexual images of themselves or other minors online and by cellphone. Most minors share these images to flirt or because they were asked to by a boyfriend or girlfriend. However, sometimes they are pressured into sharing these images even when they do not want to.

- No one should pressure anyone else into sexting.
- No one has the right to make someone else share sexual images – not even a significant other.

It's illegal to share sexually explicit images of minors. However, many minors caught sexting are not charged with a crime. They may be ordered to attend educational programs or perform community service. They may also get in trouble at school and experience social consequences, such as being judged or excluded by their peers and communities.

ONCE YOU **HIT SEND**, YOU **CANT'T CONTROL** WHERE THE IMAGE GOES!

SEND

Before sending one, THINK

1 How would I feel if this image got out?
2 Can I really trust that the person I am sending it to will keep it private?
3 How could sending it affect my relationships with, classmates, parents, teachers, e.t.c.?

Before forwarding one, THINK

1 How would I feel if someone shared a photo of me?
2 What consequences could i face for forwading this?

Discussion Prompts

- **Do you think kids and teens feel pressured to sext? Why or why not?**
- **What would you tell a friend who was thinking about sexting?**
- **What advice would you give a friend who received a sext?**
- **Do you think people should get in trouble for forwarding sexts? Why or why not?**
- **Do you think sexting can be harmful for minors? Why or why not?**

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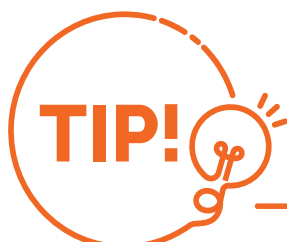
Find out how you can stay in control and what to do if your photo has fallen into the wrong hands.

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.

How to look for and identify a potential online predator

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

TIPS!   Tips for dealing with online predators

1. Never download images from an unknown source. Images could be sexually explicit.
2. Consult a trusted adult – teacher/parent/IT admin on how to use email filters.
3. Tell a trusted adult immediately if anything that happens that online makes them you uncomfortable or frightened.
4. Consider choosing a gender-neutral screen name that does not contain sexually suggestive words or reveal personal information.
5. **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.
6. **STOP** any email communication, instant messaging conversations, or chats if anyone starts to ask questions that are too personal or sexually suggestive.
7. 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.

Risks of Revealing Too Much

1. Anyone can access your personal information and may use it to harm you.

2. Cyberbullies may use your personal information as a weapon to spread rumours, distribute incriminating photos or conversations, or impersonate you.

3. Scammers may identify children who reveal personal information as targets for manipulation.

Tips to Help Children Avoid Revealing Too Much

1. **DO NOT** post e-mail addresses or cell phone numbers on your social networks.

2. **DO NOT** share with anyone apart from trusted adult.s

3. **DO NOT** talk about sex or other provocative subjects online.

4. **DO NO**T respond to emails or messages requesting personal information.

5. Delete e-mails from unknown senders.

6. Utilize privacy settings to block out any one you do not know in Person.

Online Safety pledge for primary and secondary students

ONLINE SAFETY PLEDGE

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: _____

ONLINE SAFETY PLEDGE
INTERMEDIATE

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 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 with anyone I have met online.

3   I will tell people I meet online **"No"** if they ask me for personal information or pictures of myself! It's OK for me to stand up for myself!

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

SIGNED: _____

SIGNED: _____

ONLINE SAFETY PLEDGE
SECONDARY

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 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 and home phone numbers, home address, sexual messages and inappropriate pictures and videos.**

2

I WILL RESPECT OTHER PEOPLE ONLINE, **I WILL NOT:**

Post anything rude, offensive or threating, send or forward images and information that might embarras, 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:**

1. Ask my parent or guardian's permission.
2. have a parent or guardian accompany me.
3. 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, gurdian or another trusted adult, report to the website, cell phone company, cybertipline.com or the police.

SIGNED: _____

SIGNED: _____

SMART RULES TO HELP YOU!

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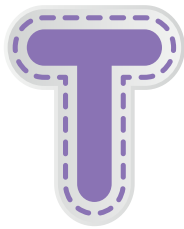
RELIABLE:
Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or trusted adult. If you like chatting online it's best to only chat to your real world friends and family.

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.

ALWAYS REMEMBER TO THINK
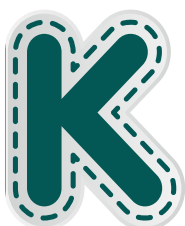
T   IS IT **TRUE?**

H   IS IT **HELPFUL?**

I   IS IT **INSPIRING?**

N   IS IT **NECESSARY?**

K   IS IT **KIND ?**

Additional Resources

Children's activity on internet security: -Budd:e (https://budde.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.

Acknowledgment

This Tool Kit was complied with support from:

CONTACT US:

📍 Plot 10 Kenneth Dale Drive, Kamyokya
P.O. Box 32330, Kampala

📞 +256 312202393

✉️ info@internetsociety.ug

f Internet Society Uganda Chapter

🐦 @ISOCUg

Internet Society
Uganda Chapter