

KEEPING CHILDREN SAFE ONLINE:

Advice to parents and caregivers



**KEEPING
CHILDREN SAFE
ONLINE:
Advice to parents
and caregivers**



Contents

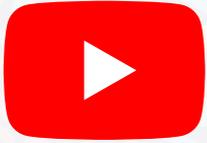
Introduction.....	iv
Creating a Balance: 'Opportunity' versus 'Risk'.....	1
What to do to keep children safe online.....	2
What are the risks children face online?.....	10
Child online safety talking points between parent/carer and a child.....	11
Four tips to help protect your children online.....	14





Dear Parent/Guardian/Educator/Teacher/Carer,

How digitally aware are you? Try answering by identifying the names behind the images below! No cheating please.







Y!









W





N













NCC Toll Free Line: 622

Cece Yara Foundation: 08008008001 (for children, toll free)
07007007001 (for adults, non toll free)



INTRODUCTION

Nations are presently grappling with the impact of COVID-19. For parents, there is the additional burden of keeping children occupied which can mean more screen time (offline/online).

The impact of the COVID-19 pandemic has created a new normal and a shift in the traditional ways of doing many things. This change has also moved education from the classroom to mobile phones, tablets, laptops, and desktops or a blend of both. The future has arrived for children all over the world, including Nigeria. Online activities have acquired a new meaning and become the reality of many Nigerian parents and children. Screen time and screen activities are the new normal. Parents are constantly searching for online learning platforms, TV stations are providing more child-based educational content and schools are teaching via Zoom, Google Classroom, and YouTube. Cyberspace, the internet, and online activities are here to stay. The future has arrived, welcome!

The fusion of children and the internet has now given birth to new concerns as is widely perceived, it has magnified the critical need for parents and caregivers to act responsibly. Concerns of safety and privacy have been with us from the beginning of time. What has changed, however, is the invisible and borderless nature of these concerns and the magnitude of the consequences of bad online parenting, when they occur.



Parents have to contend with the overwhelming and scary possibility of a child being hurt by faceless individuals while surfing the internet, and a perceived inability/incapability to protect the child.

The good news is that the internet is not all gloom and doom. The internet is a world of endless possibilities waiting to be explored by young, adventurous and impressionable minds. Undoubtedly, there are many great ways children can use connected devices to learn and play, but there are also risks. With the right tools and strategies, parents and caregivers have the opportunity to support and guide children to avoid online risks and have safer internet experiences.

The COVID-19 pandemic and its attendant change in the mode of operation have compelled all stakeholders, parents, caregivers, governments and industry players, to actively pursue, create and promote a safe online environment for children.

This handbook will provide practical online safety tips for parents, caregivers and children. It covers what to do before things go wrong, while children are online and if things go wrong.

The Nigerian Communications Commission (NCC), has taken into consideration the International Edition of Europol COVID-19 Global Online Safety Advice for, Parents and Carers, and the ITU's Keeping Children Safe Online during the COVID-19 Pandemic to develop this guide that will help Parents and Carers/Guardians during and beyond the COVID-19 pandemic.

CREATING A BALANCE: 'OPPORTUNITY' VERSUS 'RISK'

Child online abuse is a societal concern that has been exacerbated by the COVID-19 pandemic. Countries are developing measures to address and provide significant assurance of online safety for children, their families, and society at large. Let us be clear, online safety is not the non-existence of harm or risk, rather it is creating the atmosphere or opportunity to overcome the risks while enjoying the inherent benefits of using the internet.

Educating young children about cyber safety is complicated - young children often do not understand the social and technical complexities of the internet. This lack of understanding arises because the internet is virtual and cannot be experienced firsthand by sense. Computers and devices are usually in places children perceive as safe (homes, schools, cars, etc.). Therefore, the risks are not readily apparent to them. They do not understand that the computer is networked and connected beyond their safe places to a world that can be risky and dangerous. Young children and most adults do not realize that materials posted on the internet oftentimes, do not have external controls or standards to subscribe to.





NCC Toll Free Line: 622

Cece Yara Foundation: 08008008001 (for children, toll free)
07007007001 (for adults, non toll free)

WHAT TO DO TO KEEP CHILDREN SAFE ONLINE

To keep children safe online, parents and caregivers should:

1. Anticipate risks:

The anticipation of risks will lead to appropriate control measures being put in place before a child is allowed access to digital devices or the internet. Some of these anticipatory control measures include:

- **Parental education:** As a parent, stay informed and educated about the use of your devices and the devices your child has access to. Stay informed on various social network sites and what happens on them. Stay informed and better educated than your children and wards. Make them understand that you know as much or more than they do. This will make you their go-to person for information on what to do with the device you eventually give them access to.
- **Caregivers should be trained on how to guide children in online activities:** Schools have adopted the use of online platforms for education. Care must be taken to educate the teachers and prepare them for the avalanche of questions from children, on the use of various online applications or whatever information the children encounter online.



Teachers are major support pillars in the life of any child. Children take their words as law and often trust them as much as parents are trusted.

- **Install child-appropriate apps/search engines:** Before a device is given to a child, age-appropriate applications should first be installed. This will protect the child from inadvertently stumbling onto wrong sites that appear as pop-ups.
- **Install firewall:** Firewalls act as content filters. They help ensure non-age-appropriate content is filtered on the child's device.
- **Set timers on all devices used by the child:** This helps to create discipline and structure for the child. Ensure clear time boundaries are set.

2. Empower the child:

This is one of the most important steps any parent can take. There is a sense of privacy associated with being online. Parents will not always be there when children go online. Adopting a child-centric approach to the use of the internet prepares the child for unforeseen issues and assures the child of the trust and respect of his/her parent.

Children will enjoy the benefits and advantages of the internet when they know how to stay in control and not allow themselves to be victims of the platforms and devices. You can empower children by:

- Setting ground rules and instructions in collaboration with the child.

- Teaching children basic online safety skills and how to apply them.

3. Pay attention/be observant:

As children spend more time online, observe behavioral patterns and changes. Recognize unusual activities, actions, and reactions. Where any change is observed, calmly address those changes and allow the child sufficient room to talk without being judgmental. The home is a safety net and the best support system for children. The home allows an abused child to recover from the abuse and provides a healing cover for post abuse trauma.

Children need to know they can go to their parents with whatever concerns they encounter online.

4. Discuss and Engage your Children:

- Ask how your children use the internet. Make them show you some of their favorite sites and discuss with them, make them aware that there are things on the internet that may upset them and that they can always talk to you or any trusted adult.
- Make sure your child realizes that he or she should never give out personal details, such as name, address, school and telephone numbers, to online friends that they do not know in the real world.
- Tell the child to never respond to junk emails or open attachments that are from unknown sources.

- 
- Be aware of any changes in the way a child uses the internet, such as a change in the length of time spent online.
 - Encourage your child to report online bullying, by contacting you immediately it occurs.
 - Encourage children to use nicknames and login names that do not reveal any personal information about them.
 - Educate children on the possibility of people using fake names purposely to cheat, hurt or impersonate others.
 - Use the parental control settings on your browser, search engine and internet security package.
 - Work with your child to understand how search engines work so that they don't stumble on inappropriate content.
 - Consider using the filtering software that is available from your internet service provider or from retailers, these can help block inappropriate material. Check with your internet service provider to learn how to block sites you don't want children to see.
 - Gain the child's or young person's confidence by appealing to his or her interests, teach them to think twice before they upload or download anything online.

5. If your child is using online platforms or programs for schoolwork, ensure a healthy balance between non-school-related online activities and offline physical/fun activities.

Here are some helpful tips:

- During non-school hours, establish time limits around when and for how long your child can be online.
- Use the available technologies — parental controls and tools to monitor online time, allows parents to measure and set time limits on device use or internet access. Be honest and open about why you want to use these technologies.
- Turn off notifications for social media apps to help minimize distractions.
- Depending on your child’s age, establish a family tech agreement that balances time spent in front of screens with offline activities. You can find templates by searching online.
- Include ‘offline’ activities in your routine at home — this can include family exercise, reading time or board games.

6. Model good behaviour in your use of media and digital devices

Generally, children will imitate what they see in the influencers around them. Hence, Parents and caregivers must take active steps to set an ideal example for online behaviour, that children can follow.





We suggest some tips below:

- Set a time to your own media usage
- Where you use media or devices heavily due to work, it is important to explain this to children so they understand
- Do not forward content to your children that you have not verified
- Share lessons with children about other adults who have lost out on opportunities due to their online activities

7. Use parental controls and safe search options:

Parental controls are software tools that allow you to monitor and limit what your child sees and does online. They are used to filter harmful content, such as ‘adult’ or sexual materials, and to monitor, time-limit, or block your child’s use of connected devices and functions such as cameras. While parental controls can be effective tools to help control and limit what your child does online, they are not foolproof. There is no substitute for active parental engagement and supervision of a child’s online activities. Helping your child build good online safety habits is just as important as building physical safety habits.

How to use parental controls?

- Check if the family wi-fi router has software that enables parental controls across the family wi-fi network. Search online for reputable child-friendly wi-fi products using terms like ‘child-friendly routers’, ‘child-friendly wi-fi’, ‘family-friendly routers’, and ‘child safe wifi’.

- Check out the parental controls available on most tablets, smartphones, computers, TVs and gaming consoles. Look at: Windows, Mac OS, Apple (from iOS12), Android using Google Play, or Google Family Link.
- Use the PIN code locking feature on smart TVs or disconnect the TV from the internet if you are not using the 'smart' features.
- Use parental controls to limit your child's cellular/mobile data usage.
- Use the parental control measures on streaming services and gaming consoles to help manage gaming activity. Search for the streaming service or console name and 'parental controls' to see your options.
- Download or purchase family safety controls or filters. To find a filter that is right for you, search online using terms like 'internet filters' or 'family filters' and check out its reviews.
- Set up child-friendly search engines or select safe search settings on digital devices to help prevent your child from stumbling across inappropriate sites and content.

8. Safe browsing tips

- Encourage younger children to always ask an adult before clicking on an 'Accept', 'Allow' or 'OK' button on a website as sites may display other messages or disclaimers that require a response.

- Set up bookmarks in your child's browser for sites you would like them to use.
- Learn how to adapt filtering tool settings to reflect each user's age and skills if multiple members of your family share a device or program.
- Be aware that many search engines also contain advertising and know there is always a risk that inappropriate material could still slip through.



WHAT ARE THE RISKS CHILDREN FACE ONLINE?

Children face several risks on the internet. These risks can be grouped into four broad categories.

1.Content Risk: Consists of harmful information and material that children encounter online. For example, pornography, violence, fake news (mis-information).

2.Contact Risk: Meeting online friends offline can lead to negative consequences. Online grooming can also occur. This is a situation where a person befriends a young person to gain their confidence and then sexually abuses them. There are other physical and psychological risks that could lie in a young person building friendships with strangers online.

3.Conduct Risk: It includes game addiction, mobile phone overuse, impaired sight, loss of confidence and reputational harm due to unguided comments.

4.Commercialization Risk: This is the risk children face from being exposed to making willing and unwilling commercial decisions online - including giving out personal data, gambling and shopping addiction.

CHILD ONLINE SAFETY TALKING POINTS BETWEEN PARENT/CARER AND A CHILD

These questions may be asked as part of a conversation (it is advisable not to adopt a confrontational approach) or in a game form, to avoid the child being evasive or untruthful.

1. On average, how many hours do you spend online daily?

Take note that the time a child spends online may include time spent on academic or other learning activities.

2. What activity will you say you spend the most time on, when online?

Whatever activity they mention, check to see that they are not engaging excessively. It is important that a healthy balance is created between online activities and offline activities. Online addiction is unhealthy for any child. Moderation is key.

3. Who do you turn to for advice on issues arising online?

Do not take it personally if your child says s/he speaks to someone else. Research has shown that most children will rather speak to their peers or other online friends. This is because they either feel uncomfortable having such conversations with their parents or they believe they know more than their parents on online issues. It is the duty of the parents to bridge this gap by proving the child wrong.



**4. Have you been asked for a nude picture of yourself online?
If yes, did you send the picture when asked?**

Sending nudes or sexting is common amongst young children, particularly teenagers. Those children who end up sending their pics do so because they trust the person on the other end of the screen.

Children need to be made to understand that images when shared may never leave the internet and can be reshared a million times and more. It may follow the child to adulthood and such issues have been known to lead to deaths.

5. Do you have friends/followers online who are strangers?

If yes, do not cut off the child's internet/smartphone usage because of this alone. Having strangers as friends could serve as an opportunity for children to discover and express themselves. However, it provides the platform for online grooming of children which portends great danger for children.

Social Network Sites (SNS) have also increased the opportunities for such interactions. The more children are exposed to SNS, the greater the potential for online-offline contacts and negative emotional exposure.

Parents must handle this line of conversation carefully in order not to push the child right into the arms of evil strangers.

6. Have you ever been bullied online?

Find out how they felt and together discuss solutions. Do not make them feel punished twice by blaming them for being bullied. Research shows that 20.8% of children within the 12-16 years bracket have either bullied or been bullied online. Bullying is a common phenomenon online.





FOUR TIPS TO HELP PROTECT YOUR CHILDREN ONLINE

1. Build trust by keeping communication open and supportive:

- Your child knows they can come to you if something goes wrong or does not feel right online.
- Watch TV, play games and enjoy digital platforms with your children.
- Discuss online opportunities, entertainment, learning and risks.

2. Be the parent, offline and online, by setting limits, controls and standards:

- Set time limits for all activities, including online activities. Balance screen time with other activities.
- Set location for device use. Where possible, use desktops not mobile devices. Keep devices away from private locations like bedrooms.
- Set up parental controls and filters for harmful content.
- Have clear agreements on online activities.
- Be alert to signs of distress or problems.

3. Make sure your child understand the 'SMART RULES':

S: Safe- Do not give out personal information when chatting or uploading online. Personal information includes your address, phone number, passwords, e

M: Meeting- Meeting someone you have only been chatting with online can be unsafe.

A: Accepting- Accepting emails, IM messages, or opening files, pictures or text messages from people you don't know or trust can lead to problems; they may contain viruses or horrible messages.

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

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



4. Lead by example:

- Use devices responsibly.
- Show respect in your online platform language and content.
- Help your child to develop digital intelligence and social and emotional skills such as respect, empathy, critical thinking and resilience.
- Help your child practice and become a responsible online citizen.



NCC Toll Free Line: 622

Cece Yara Foundation: 08008008001 (for children, toll free)
07007007001 (for adults, non toll free)

This book is not for sale