



L E S O T H O
C O M M U N I C A T I O N S
A U T H O R I T Y

CHILD ONLINE PROTECTION GUIDELINES

2024

Lesotho Transposition

Table of Contents

1. DEFINITIONS	3
2. INTRODUCTION	3
3. CHILD ONLINE RIGHTS	4
4. CHILD ONLINE OBLIGATIONS	5
5. OBLIGATIONS OF MOBILE AND INTERNET SERVICE PROVIDERS	6
6. OBLIGATIONS OF CONTENT SERVICE PROVIDERS	6
7. WHAT CHILDREN NEED TO KNOW TO STAY SAFE ONLINE	7
8. DUTIES OF PARENTS/ADULTS IN CHILD ONLINE PROTECTION	8
9. TIPS FOR PARENTS/ADULTS IN CHILD ONLINE PROTECTION	9
10. SAFER ONLINE ENVIRONMENT AND APPROPRIATE AGE	11
11. NETIQUETTE	13
12. PLAYING ONLINE GAMES	13
13. BULLYING	14
14. DIGITAL FOOTPRINT	15
15. HARMFUL, OFFENSIVE, OR ILLEGAL CONTENT	16
16. GROOMING	17
17. LIST OF REFERENCES	18

1. DEFINITIONS

In these Guidelines, unless the context otherwise requires –

“**child**” means a person under the age of eighteen years;

“**cyberbullying**” means the act of child or adult using internet (emails, text messages, instant messaging direct messaging, social media platforms etc.) to harass threaten or humiliate another child online;

“**data**” means unidentified data, anonymised personal data or a fact about an unidentified individual and any digital information in the form of sound, visual or audio-visual recording;

“**digital environment**” information and communications technologies, including ‘digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology;

“**grooming**” means a deliberate process in secrecy usually conducted by an adult to gradually initiate and maintain friendship with a child online and builds an emotional connection with future intention of sexual relationships /abuse/exploitation/trafficking;

“**guardian**” means any person who is for the time being in charge of and has control over the child;

“**internet service provider**” means an organization that provides services for accessing and using the internet;

“**netiquette**” means the rules of conduct for respectful and appropriate communication on the internet. The rules advise people on how to communicate and treat others when interacting online;

“**personal information**” means any information relating to an identified natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. INTRODUCTION

In the fast-changing digital world parents, guardians, communities, service providers and government face new challenges in keeping children safe online. These guidelines are therefore made sequel to the clarion call made by the International Telecommunications Union (ITU). The guidelines are a transposition of the ITU Guidelines on Child Online Protection 2020. They aim to promote awareness and education for children, parents and communities about children’s safety and their responsible use of ICT services and tools. In addition, they seek to outline the

responsibilities of service providers on the steps and measures they may take to enhance protection of children online.

These Guidelines target to equip children, parents and guardians in Lesotho with knowledge and practical advice to appreciate safe internet use to protect the children against a range online abuses or harmful activities such as trafficking, cyberbullying, online sexual exploitation and hacking or harvesting of personal information as well as invasion of their privacy. With the right education and concerted efforts with parents, guardians, teachers, internet service providers and all other relevant stakeholders, children can learn to avoid these risks and to take advantage of the internet's many opportunities.

3. CHILD ONLINE RIGHTS

The United Nations Committee on the Rights of the Child explains in General Comment No. 25 on children's rights in relation to the digital environment that state parties should take legislative and administrative measures to protect children from violence in the digital environment. This includes the regular review, updating and enforcement of robust legislative, regulatory, and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. The rights include:

a) Right to Privacy and data protection.

Children have a right to private and family life in the digital environment. Children's personal data must be protected and processed lawfully for specific purposes and with clear consent of the children and/or their parents or guardians.

b) Right of access to information with age suitability and right to education.

A child shall have access to information and material from a diversity of sources. The information must be in the best interest of the child for promotion of his or her education, social, spiritual and moral well-being and physical and mental health. The information and material must be age appropriate and not injurious to a child.

c) Right to be safeguarded from online abuse.

Children have the right to be protected from all forms of violence, exploitation and abuse in the digital environment to ensure healthy development and well-being.

d) Right to freedom of expression and right to be heard.

Children have a right to freedom of expression in the digital environment, and a right to have their views heard in all matters affecting them.

e) Right to freedom of association online.

Every child shall have the right to freely and peacefully associate with his or her peers or any person online in conformity with the law. This include engaging in online communication, gaming, networking and entertainment. This right also entails freedom to refuse any requests made online.

4. CHILD ONLINE OBLIGATIONS

In as much as children have rights in the digital environment, they also have the obligation to use internet safely and responsibly by observing to the following:

a) To protect their privacy

A child must keep passwords private and avoid giving out personal information like telephone numbers, addresses of their school, home and parents' work and personal email address.

b) To be respectful of others online -

A child must avoid sending or sharing harassing, provoking or humiliating messages or content about other people. This includes responsibility not to share personal information of others online such as photos, phone numbers, email and home address.

c) To protect their dignity and reputation

A child must think of the consequences of sending or posting any personal or private information (photos or videos) which may have potential to damage his or her dignity and reputation. Content once posted can be difficult to remove.

d) To observe and manage the time spent on the internet

A child must maintain a balanced digital diet, such that a time online is time well spent and contains a mix of activities that include learning, creating, and connecting in positive ways.

e) To report

A child has an obligation to report abuse, inappropriate or harmful content found on personalised internet use or harm done to other children and friends online.

f) To observe SMART RULES online

A child must always be vigilant and observe SMART Rules as defined in section 7 below.

5. OBLIGATIONS OF MOBILE AND INTERNET SERVICE PROVIDERS

It is the responsibility of mobile network operators and other internet service providers to include child online safety in the national broadband and digital plans and improve affordable and safe access to digital devices and connectivity for children, especially for disadvantaged and marginalized children. The following are equally important to make online platforms safe and accessible for children:

- a) Provide age appropriate and safe online learning resources for free or at a reduced cost to educators and students, including resources accessible to children with disabilities.
- b) Share child-friendly information and child online safety advice to support children digital resilience skills.
- c) Use their platforms to promote and facilitate cost-free child safety referral services and Child Helpline 116.
- d) Place child safety at the centre of products development and ensure that safety tools and features are incorporated into all devices, such as parental controls, age-verification tools.
- e) Develop and use terms of service and conditions or acceptable use guidelines to specifically prohibit certain behaviour such using mobile services to store, share or distribute child sexual abuse materials. Make sure these terms clearly state that child sexual abuse material will not be tolerated.
- f) Make online safety resources age-appropriate and easily accessible for parents, guardians and children detect and stop harmful activity against children online, use scanning and filtering technology to ensure child user safety and users are not exposed to inappropriate content. This includes content hosted on the service provider's servers from a third-party content provider.
- g) Educating children, parents, guardians and teachers about children's safety and their responsible use of ICTs.
- h) Adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children and ensure that third party content service providers whom they have contractual relationship with uphold and adhere to similar standards.

6. OBLIGATIONS OF CONTENT SERVICE PROVIDERS

Content service providers have the following obligations in respect of creating a safer online environment for children:

- a) To have mechanisms to get parental consent before collecting or using a child's personal information, such as a name, address, phone number, etc.
- b) Integrating child rights considerations into all appropriate corporate policies and management processes.
- c) Develop and put in place processes on how cases of child online abuses are reported and handled and commit to collaborate with the law enforcement agencies in investigations of such cases.
- d) Helping to create a safer and age-appropriate online environment by restricting access of children to harmful or inappropriate content through adopting measures such as age-verification, age classification of content etc.
- e) Educating children, parents, guardians and teachers about children's safety and their responsible use of ICTs, how to report online abuse and available parental controls tools.

7. WHAT CHILDREN NEED TO KNOW TO STAY SAFE ONLINE

While using the internet children need to be aware of certain basic rules to be able to safeguard them and others. Children must be smart, responsible, and safe online, as well as in real life. Children must know the **SMART RULES** which are defined as follows:

a) SAFE

Keep safe by being careful not to give out personal information, such as full name, email address, phone number, home address or school name to people online.

This is particularly crucial when using social media where revelation may surface. Such revelations can leave a trace of one's identity and dwelling place to strangers among others. Change all settings to private to allow sharing to be solely with people personally known offline.

b) MEETING

Meeting offline with an online friend or contact can be risky because the said friend could turn out to be different person one would not wish to have met. If the friendship turns out to progress online, it should solely be under the supervision of a parent/guardian/teacher or trusted adult.

c) ACCEPTING

Extreme caution needs to be exercised when accepting any message requests online. Accepting emails or opening pictures, or videos from strangers online can lead to various hazards including viruses and nasty/inappropriate messages. The same extends to strangers who request friendship on social media platforms.

Accepting such friendship could be dangerous as the strangers would access one's private information from the profiles.

d) RELIABLE

Information online may not be true, or someone may be lying about who they truly are. Children must be critical of what appears to be a fact may not be true at all. Unfortunately, if it appears too good to be true, it probably is. It is important to always double-check the information from other reliable sources.

e) TELL

Tell a parent/teacher/guardian/police/trusted adult and block the online friend that bullies or know someone being bullied online. Tell a parent/guardian/teacher/police/ trusted adult if the following occurs:

- i. Being lured or tricked into virtual sexual activities, sharing nude photographs of yourself or engaging in sexting with an online friend.
- ii. Visited a website containing upsetting or distressing content or having online friends sharing harmful content or being pressured or tricked into unknowingly accessing or sharing links to such sites.
- iii. Experience aggressive behaviour or provoking content towards others or have friends sharing harmful content.

For any online acts that may require to be reported, the Child helpline toll-free number is **116**; and illegal or possibly illegal activities can be reported to the nearest police station (or call 112) - Police Hotline.

8. DUTIES OF PARENTS/ADULTS IN CHILD ONLINE PROTECTION

Parents need to support their children so that they can benefit from technology safely. In all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration. To ensure that children use internet sites safely and responsibly, parents, and guardians should among others do the following:

- a) To train children to be vigilant, astute, and principled in browsing the internet.
- b) To check content, web browsers and single/default search engine with suitable age for children.
- c) Familiarise themselves with the risks and opportunities that their children may encounter online.
- d) Stay actively engaged in what their children are doing online, the type of content they are watching, sharing, or creating, the services, platforms, and games they are using, and the people that they are connecting with.

- e) Familiarise themselves with good websites and games for learning and entertainment that they can use with their children.
- f) Have a regular, honest, and open dialogue with children and young people that is age-appropriate and changes over time.
- g) Ensure that the child knows when and where to get help if they experience anything upsetting online.
- h) Ensure that the children have a balanced digital diet, such that their time online is time well spent and contains a mix of activities that include learning, creating, and connecting in positive ways.
- i) Make use of numerous tools that can assist parents with the 'management' of connected technology both in and out of the home.
- j) Remind your children to avoid giving out personal information like telephone numbers, addresses of their school, home and parents' work and personal email address on their home page. Teach your children not to share their access passwords with friends or siblings.
- k) Avoid threatening to remove or confiscate devices as they can be social lifelines for some children. If a child fears that a device will be removed, he/she is likely to be increasingly reluctant to share problems or concerns.
- l) Teach children how to block someone/contact who they no longer wish to talk to.
- m) Create family rules which will all be agreed to on online use.

9. TIPS FOR PARENTS/ADULTS IN CHILD ONLINE PROTECTION

Below are the tips and approaches which parents and guardians may adopt to promote a positive and responsible use of the internet services and devices:

- a) Ask your child questions
- b) Discuss the risks of technology use
- c) Be on the lookout for underlying issues
- d) Make "yes" and "no" rules
- e) Create tech-freezones
- f) Establish expectation around content
- g) Explore technology together
- h) Know when to take a step back
- i) Act as a team
- j) Make it playful

9.1 Ask your child questions

Pose questions about the children's devices the same way you would in any other activity they are engaged in. Find out what they like about them, what they do not like about them, how often they use them and what is working.

9.2 Discuss the risks of technology use

Talk to your children honestly about your concerns such as devices hindering other activities, worries about content they may see or things they may do online.

9.3 Be on the lookout for underlying issues

It is important not to blame everything on technology. Sometimes there are other things going on that are manifesting in the way children use their devices. Children may spend more time online due to proving themselves worthy as they may find social media as escape from reality through constant feed updating to seek approval from their peers who look down upon them at school or other places where they congregate.

9.4 Make "yes" and "no" rules

"Yes" rules include children's obligations online such as the way they ought to conduct themselves online. The same includes how to be good digital citizens and what healthy technology for the family entails. "No" rules on the other hand entails forbidden things which include bullying.

9.5 Create tech-freezones

Boundaries which include the day/s or location/s that are tech-free should be set by parents. There should be a doc station where the devices are kept during the tech-free day or when at the tech-free station. The parents should set the time when devices are removed from the bedrooms to allow proper sleep.

9.6 Establish expectation around content

Online content should be age and developmentally appropriate content and same should be monitored through filtering as provided under 7.

9.7 Explore technology together

Parents should consider co-viewing and co-use with children of all ages. For older children reporting the sites/ applications that they access should be mandatory.

9.8 Know when to take a step back

Whereas it is important to keep tabs on the children it is equally important to take a step back as the children get more experience with their devices to give more age and stage appropriate independence. However, giving children space should not absolve the parents from knowing what the children do online.

9.9 Act as a team

Parents need to be aware of how (and how often) the use of their own devices entice children to follow suit. It is important to join children in establishing healthy habits and boundaries to step outside the 'me' versus and 'you' dynamic.

9.10 Make it playful

There are so many ways to use technology to facilitate play and fun opportunities with children. That could include using an application or playing a game together. The same could also range from cooking, sports, music etc.

10. SAFER ONLINE ENVIRONMENT AND APPROPRIATE AGE

Internet safety messages need to be timely, age-specific, culturally sensitive and match the values and laws of the society in which the child lives. The COP Initiative has identified three principal age groupings of young internet users. These groupings broadly correspond with the key stages of development on a child's journey to adulthood. It is important to emphasise that every child is different and requires and deserves individual attention. One size does not fit all. Nothing should ever be assumed or taken for granted.

a) The first age group: up to 7-year-old

This group experiences their first contact with technology. Their usage should be closely always supervised by a parent, guardian or adult. Filtering software or other technical measures may also have a particularly useful role to play in supporting the use of the internet by a child of this age. It would be wise to consider limiting such a young child's potential access e.g. by constructing a list of safe websites which are age-appropriate such as a walled garden. The aim is to provide this age group with the basics of internet safety, etiquette and understanding. This age group will probably not be able to decode more sophisticated messages and may need adult assistance to stay safe online.

b) The second age group: 8-12-year-old

This age span is a challenging transition for the child. Typically, he or she is becoming a young person with a greater capacity to form questions. Their curiosity will start to push them to seek out and challenge boundaries, looking for answers. It is an age group where awareness of what is available online exists. The impulse to seek and find out what's there is great. Throughout childhood, a child is expected to test the barriers and evolve through this kind of learning. Filtering software or other technical measures may have a particularly useful role to play in supporting the use of the internet by a young person of this age. An important aspect of this age group is the sometimes-uncritical approach to content and contact, which can put the age group in a

particularly vulnerable situation for predators and commercial entities wishing to engage with them.

c) The last age group: 13-year-old and above

This group is the one covering the longest span. The group consists of young people who are, namely, teenagers. This group is growing rapidly, transitioning from being young people to becoming young adults. They are both developing and exploring their own identities, and their own tastes. They will very often be able to use technology with a high level of proficiency, without any adult supervision or interaction. Filtering software will start to become less useful and less relevant, but it certainly could continue to play an important supporting role, particularly for some young people who may have temporary or longer-term vulnerabilities.

To help stay safe while chatting, the following tips should be applied:

- a) A child should be careful on who to trust online. A person can pretend to be someone they are not.
- b) Exercise great care when choosing friends online. While it is good to have a lot of friends, having too many makes it harder to keep an eye on who sees the stuff you post online. A child should not accept friend requests from unknown person.
- c) Keep personal details private. Use a nickname instead of real name on a site or game where there may be lots of strangers or unknown people. Seek advice from parents or guardian before giving anyone on the internet your name, address, phone number or any other personal details.
- d) It is important to set a profile to private. Parents or guardians should help the children with such settings.
- e) Password should always be kept secret and should not be shared with anyone, including friends.
- f) Where a child wants to arrange to meet someone they have met online, such meeting should happen in the presence of a parent or guardian. Such meeting should always be in a brightly lit public place where lots of other people will be around, preferably during the day.

- g) If someone writes something rude, scary or something not likable, it is important to inform the parents, guardian, or any trusted adult.

11. NETIQUETTE

It is always important to bear in mind that people chatting with on Instant Messaging, playing a game with, or posting to their profile are real persons and care should be taken to avoid saying or doing things that may hurt their feelings or make them feel unsafe or embarrassed. It is important to be kind and polite to others online. One should stop and think about how his/her behaviour will affect other people.

Note the following:

- a) Treat other people the way you would like to be treated.
- b) Avoid using bad language and do not say things to someone to make them feel bad.
- c) Learn about the 'netiquette' of being online. What is considered okay to do and say and what is not. For example, if you type a message to someone in UPPER CASE, they may think you are shouting at them.
- d) If someone says something rude or something that makes you feel uncomfortable, don't respond. Leave the chat room or forum straight away.
- e) Tell your parents, guardian or another adult you trust if you read upsetting language or see nasty pictures or something scary.

12. PLAYING ONLINE GAMES

Playing games online can be great fun to children, but one needs to be careful about how much time is spent playing and with who. It is important to protect private or personal information when chatting with other gamers. Parent or guardian advise should be sought where one is unsure on whether a game is suitable.

A child should note the following regarding online games:

- a) If another player is behaving badly or making you uncomfortable, block them from your players list. You may also be able to report them to the game site operator.
- b) Limit your gameplay time so you can still do other things like homework, jobs around the house and hanging out with your friends.
- c) Keep personal details private.

- d) Remember to make time offline for your friends, your favourite sports and other activities.
- e) Remember it is easily addictive to always stay online, which can make you vulnerable to internet dangers, you should, therefore, exercise self-discipline.

13. BULLYING

What is bullying? Bullying is the act of intentionally causing harm to another person through verbal harassment, physical assault, or other subtle methods of coercion such as manipulation. Bullying often describes a form of harassment perpetrated by an abuser who possesses more physical and/or social power and dominance than the victim. The victim of bullying is sometimes referred to as a target. The harassment can be verbal, physical and/or emotional. A child may be a target of bullying. Online bullying can have just as painful consequences as that of traditional forms of bullying.

A child should do the following if bullied online:

- a) Ignore it. Don't respond to the bully. If they don't get a response, they may get bored and go away.
- b) Block the person. This will stop you from seeing messages or texts from a particular person.
- c) Tell someone. Tell your parent/guardian/teacher, or another adult you trust. Keep the evidence. This can be useful in tracking the bully down. Save texts, emails, online conversations, or voice mails as proof.
- d) Report it to:
 - i. Your teacher/school principal - they should have policies in place about bullying.
 - ii. Your Internet Service Provider and/or phone provider or the website administrator - there are actions they can take to help.
 - iii. The police - if there is a threat to your safety the police will help.

If a friend is being bullied online:

It can be hard to know if your friends are being bullied. They might keep it to themselves. If they are being bullied, you might notice that they may not chat with you online as much, or they suddenly receive lots of SMS messages or are unhappy after they have

been on the computer or checked their phone messages. They may stop hanging around with friends or have lost interest in school or social activities.

Research shows that young people often use suggestive comments that show distress in their online posts, particularly on social sites e.g. WhatsApp status. In extreme cases, some young people have resorted to suicide after posting comments that could have raised alarm.

A child can help to stop bullying by doing the following:

- a) Stand up and speak out! If you see or know about bullying happening to a friend, support them and report it. You would want them to do the same for you.
- b) Don't forward messages or pictures that may hurt or be upsetting to someone. Even though you may not have started it, you will be seen to be part of the bullying cycle.
- c) Remember to treat others as you would like to be treated when communicating online.
- d) Raise the alarm when you see any statements on your friends' social media sites that may suggest that they are in distress.

14. DIGITAL FOOTPRINT

It is great to share things online with friends. Part of the fun of sharing videos, images, and other content is that lots of people can view and respond. Remember that what one shares with friends may also be viewed by others whom one does not even know. Shared information may be kept and be able to look at it for years to come. Everything one posts adds up to his/her digital footprint and, once it is online, it could be there forever. It is therefore important to think before posting or sharing.

A child should note the following regarding his or her digital footprint:

- a) Keep your details private. Use an appropriate nickname instead of your real name. Ask your parents/guardian /teacher before giving anyone on the internet your name, address, phone number or any other personal details.
- b) Don't share your username or password with anyone.
- c) Think before you hit send or post. Once posted, it can be difficult to remove content.

- d) Don't post anything you don't want others to know or find out about or that you wouldn't say to them face to face.
- e) Remember that private images and videos you send to friends or post on a social networking site may be passed on to others and uploaded to public sites.
- f) Be respectful of other people's content that you post or share. For example, a photo that your friend took is their property, not yours. You should post it online only if you have their permission and make a note about where you got it from.

15. HARMFUL, OFFENSIVE, OR ILLEGAL CONTENT

When surfing the internet, one may come across websites, photos, texts or other material that makes one feel uncomfortable or upset. There are sites that, for example, promote racial hatred or incite violence, sites which could lead a child to come across pornographic or child abuse material. There are some easy ways to handle these situations.

A child should do the following to handle harmful, offensive or illegal content:

- a) Tell your parents, guardian, or another trusted adult if you come across material that upsets you.
- b) Know how to 'escape' from a website if an internet search takes you to an unpleasant or nasty website. Hit control-alt-delete if the site will not allow you to exit.
- c) If a website looks suspicious or has a warning page for people under 18 years old, leave immediately. Some sites are not meant for children.
- d) Check with your parents or guardian or teacher that your search engine is set to block material that is meant for adults.
- e) Ask your parents or guardian or teacher to install internet filter software to block bad websites.
- f) Ask your parents or guardian or teacher to help you find safe and fun sites to surf and bookmark for later use.

- g) If, while surfing online, you come across sites containing violent, racist, illegal or child abuse materials do not forget that these sites can be reported to the police or Childline hotline **116**.

16. GROOMING

Sexual predators use the internet to contact children and young people for sexual purposes, often using a technique known as “grooming”. The internet and mobile phones can potentially be used by abusive adults to contact boys and girls. This happens particularly through SMS and MMS messaging, chat rooms, Instant Messaging programmes, newsgroups, forums, online games, and, more generally, through all the social networking spaces, where it is possible to obtain information on users’ ages, sex and more, through the profiles they have compiled.

This involves gaining the child’s or young person’s confidence by appealing to his or her interests. These predators are highly manipulative people. They often introduce sexual topics, photos and explicit language to raise sexual awareness and get their intended victims to drop their guard. Gifts, money and other benefits are sometimes used to persuade and lure the child to a place where the predator can sexually exploit him or her. These encounters may even be photographed or videotaped, or if a meeting does not take place in the real world the predator might persuade the child to make sexual images of themselves or their friends or take part in sexual activity using a webcam to broadcast it. Victims of grooming may also be hesitant to tell adults about their encounters for fear of embarrassment or of losing access to the internet. In some cases, they are threatened by predators and told to keep the relationship or what happened a secret.

A child should be aware of the following to avoid being a victim of grooming:

- a) It is essential that you be aware of this risk, and of the fact that not everyone online is who he/she claims to be. Online seducers can often pretend to be your age to create an atmosphere of familiarity and trust that could lead to an off-line meeting and possible abuse.
- b) Protecting your data is important; in the real world, you would never give out such details and you’d never tell people you don’t know about your private matters. Even if a nice virtual friendship has been formed, that might seem like it could lead to something more, it is important to remember that you don’t always know who is really at the other end of the computer. The online friend may have given false information or images of themselves.

- c) When entering a chat room, forum, or more generally, a social network, a child must compile a personal profile, inserting information that can be detailed to varying degrees. In such cases, it is essential to be cautious about inserting identifiable or traceable data (name and surname, address, the name of your school, mobile phone numbers, e-mail address, etc.). Such details can become accessible to anyone, and it is, therefore, advisable to create an identity for yourself, using nicknames or aliases and fictional images or avatars, and not provide any detailed personal information.
- d) When you are curious about your sexuality or your more intimate feelings, remember that the internet can sometimes be a source of really good advice and information but very often it is better to try to find a way to discuss these things with parents/guardians/teachers/ trusted adults in real life.
- e) If attempts at allurement or awkward situations should occur, it is important to find someone to speak to, a parent/guardian/teacher or friend. Alternatively, you can turn directly to Police hotline **112** Nthuseng or Child helpline **116**.
- f) It is also advisable to save e-mails and chat room text, SMS or MMS messages (using “messages inbox”, for example), as they can be provided as evidence to the Police.

17. LIST OF REFERENCES

1. Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Council of Europe, September 2018.
2. African Charter on Rights and Welfare of the Child, 1999.
3. Constitution of Lesotho, 1993.
4. Children Protection and Welfare Act, 2011
5. Guidelines on Industry for Child Online Protection, 2015 – ITU and UNICEF
6. United Nations Children’s Fund (2022) ‘Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse’.