POSTAL AND TELECOMMUNICATION
REGULATORY AUTHORITY OF ZIMBABWE

'creating a level playing field'

# CHILD ONLINE PROTECTION GUIDELINES FOR CHILDREN

Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ)
Box MP 843 Mount Pleasant
Harare

www.potraz.gov.zw

**December 2015**

# Table of Contents

# 1 INTRODUCTION

Over the last few years, Zimbabwe has witnessed phenomenal growth in the field of telecommunications. This development has resulted in massive rollout of broadband access networks in the country. As broadband services and applications expand into every aspect of life, greater numbers of people are beginning to use broadband Internet connections for a variety of activities. This growth in Internet use brings with it numerous cybersecurity issues, especially when it comes to the protection of our youngest and most vulnerable digital citizens - our children.

We are in the information age and today's children are growing up in an environment in which an unprecedented level of services and information is accessible through a computer or a mobile device with Internet access. With the cost of these devices and the costs of accessing the internet diminishing rapidly, more and more children are being presented with unparalleled opportunities to explore new frontiers and meet people from faraway places. Children and young people are truly becoming digital citizens in an online world that has no borders or frontiers.

Whilst the internet assists children in enhancing their learning experience, children and young people need to be aware of some of the potentially negative aspects of the technologies. Harmful activities can include bullying and harassment, identity theft and online abuse (such as children seeing harmful and illegal content, or being exposed to grooming for sexual purposes, or the production, distribution and collection of child abuse material). These are all threats to children and young people's wellbeing and a challenge that must be addressed by all stakeholders, including children themselves.

According to the International Telecommunication Union (ITU), over 60 per cent of children and young people with internet access talk in chat rooms on a daily basis. Three out of four children online are willing to share personal information about themselves and their family in exchange for goods and services and as many as one in five children could be targeted by a predator each year. It is in light of these frightening statistics that the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) compiled this set of Guidelines.

These guidelines came out of the realization that the first and best form of defence in protecting children is making them aware of what can happen online and make them understand that there is always a solution to a problem that they may encounter online. Empowering children and young people through education and raising awareness is therefore of paramount importance.

The Internet knows no country boundaries, and international cooperation is fundamental in winning the battles ahead. In line with the desire to embrace international best practice, these Guidelines were adopted, and adapted to the Zimbabwean environment, from those developed by the ITU in collaboration with a team of contributing authors from leading institutions active in the ICT sector and in child online safety. They were prepared within the context of the Child Online Protection (COP) Initiative in order to establish the foundations for a safe and secure cyberworld for present and future generations. The COP initiative is a special UN led multi-stakeholder effort to promote awareness on the importance of child safety in the online world and to develop practical tools to assist governments, industry and educators in this domain.

# 2 INTERNET SAFETY GUIDELINES

## 2.1 Principal Age Groupings

Internet safety messages need to be timely, age specific, culturally sensitive and match the values and laws of the society in which the child or young person 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. Hence the guidelines can be seen as a ladder which takes you through progressive phases. However, we cannot emphasise too strongly 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.

### 2.1.1 The first age group 5-7 year old

This group experiences their first contacts with technology. Their usage should be closely supervised at all times 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 web sites which are age appropriate such as a walled garden. The aim is to provide this age group with the basics in 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.

### 2.1.2 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 their own 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.

### 2.1.3 The last age group: 13 year old and above

This group is the one covering the longest span, is the group consisting of young people who are, namely, teenagers. This group is growing up rapidly, transitioning from being young people to becoming young adults. They are both developing and exploring their own identities, 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.

Linked to their own hormonal development and a growing sense of physical maturity, teenagers can go through phases when they feel a very strong need to find their own way, to escape close parental or guardian supervision and seek out their peers. A natural curiosity about sexual matters can lead some people in this age group into potentially worrying situations and this makes it all the more important for them to understand how to stay safe online.

The COP guidelines recognize the difficulty in creating messages that will cover the needs of all ages within the defined groups. Zimbabwean laws and customs are therefore profoundly important in matters of this kind.

## 2.2 What you need to know to stay safe online

### 2.2.1 SMART Rules

Using the Internet is fun. Enjoy it most by keeping yourself safe.

1) You can do a lot of great things on the Internet. You can play games, chat with your friends, meet new friends and find a lot of useful information. You have the right to enjoy and explore all that the digital world has to offer.

2) But you also have to be aware that you can find some unpleasant things on the Internet, such as images and stories that may confuse or even frighten you. Your friends and trusted adults are not the only people within this digital world. Unfortunately the Internet is also used by people who are not so nice or who might even want to harm, harass or bully you or other people. While using the Internet you need to be aware of certain basic rules to be able to safeguard yourself and others.

3) You have the right to use the Internet safely and to set your own limits. Be smart, responsible and safe online, as well as in real life.

### 2.2.2 Set Your Limits

1) Take care of your privacy. Whether using a social networking site or any other online service take care of your privacy and that of your family and friends. You might have the feeling of being anonymous online but collecting information from various sources can reveal too much private information about yourself or others you are close to, including your family.

2) If you join a social networking site use the privacy settings to protect your online profile so that only your friends can see it. Wherever possible instead of your real name you should use a nickname that your real friends will be able to recognize. Other interactive services, for example instant messaging, will often also provide privacy tools. Use them.

3) Think twice before you publish or share anything online. Are you prepared to share it with everyone online; your close friends, as well as strangers? Once you

post information, photographs or any other material on the Internet, you may never be able to remove it or prevent other people from using it. You can never know for sure where it might end up.

4) Be critical what appears to be a fact may really not be true at all. Unfortunately, if it appears too good to be true, it probably is. Always double check the information from other reliable sources.

5) You have rights and you, as well as other people, should respect them. You should never accept harassment or bullying by other people. The laws and expectations of decent and acceptable behaviour are valid online as well as in real life.

### 2.2.3 Meeting online friends offline

1) Sometimes online contacts develop into friendships.

2) Think twice before meeting an online friend in real life. If you still would like to meet an online friend offline, you should always take someone reliable with you. You should ask your parent, guardian or another trusted adult to join you to avoid any trouble in case the meeting turns out to be a disappointment.

3) Bear in mind that your online friend might turn out to be a different kind of person than you thought he or she would be.

### 2.2.4 Accepting Invitations / Friendships

1) Most of the people you communicate with online are probably already your friends in real life. You can also be connected to the friends of your friends. Very often that can be fun but at the same time if you do not actually know someone yourself, are you really prepared to count them as a “friend” and share with them exactly the same information that you share with your oldest and best friends?

2) Through online connections you can connect with people previously unknown to you. You may get requests by strangers who want to be included in your contact list and see your profile, but it is not wise to accept them. There’s nothing wrong with declining invitations you are not sure about. Getting more and more contacts is after all not the point of social networking.

### 2.2.5 Reacting to inappropriate content or requests

1) Protect yourself from upsetting or distressing content. Do not knowingly access or share links to such sites. If you see something that bothers you, talk about this with your parents, guardian or someone you trust.

2) Ignore bad behaviour and leave unpleasant conversations or sites with inappropriate content. As in real life there are people who for some reason, may behave aggressively, insultingly or provocatively towards others, or who want to share harmful content. Usually it is better just to ignore them and then block

them.

3) Block anyone approaching you using rude, intruding or threatening emails or comments. Even if the message may be upsetting and makes you feel uncomfortable you should save it so you can show it to an adult for advice if needed. You are not the one to be ashamed of the content of the messages.

4) Always be alert if someone, especially a stranger, wants to talk to you about sex. Remember that you can never be sure of the true identity or the intentions of that person. Approaching a child or a young person in a sexual way is always a serious cause for concern and you should tell a trusted adult, so you or the trusted adult can report it.

5) If you have been lured or tricked by someone into engaging in sexual activities or transmitting sexual images of yourself, you should always tell a trusted adult in order to receive advice and help. No adult has a right to request things of that particular nature from a child or a young person - the responsibility always lies with the adult.

### 2.2.6 Handling your concerns

1) If you have any concerns or problems while online, you need to tell someone you can trust. Your parents, guardian or some other adult can help and give you good advice on what to do. There are no problems that are too big to be solved! You might also want to call Childline Zimbabwe on their **free helpline 116** for advice or report any form of harassment.

2) You can report harmful or inappropriate content or activities on websites to the abuse e-mail of the host of the site.

3) You can report illegal content to an Internet Hotline, Police Victim Friendly Units or to Childline Zimbabwe on their website http://www.childline.org.zw or their free helpline 116.

4) You can report illegal or possibly illegal activities to the nearest police station.

5) In addition to taking good care of yourself, you should also take care of your computer or mobile device. Like the SMART rules, there are some easy tips to remember in order to keep your computer and mobile device safe.

### 2.2.7 Making safe use of your computer

1) Make sure you have installed and learned how to use a firewall and anti-virus software. Remember to keep them up to date!

2) Learn about your computer's operating system (like Windows, Linux, etc) and especially about how to patch it and keep it up to date.

3) If parental controls are installed then talk with your parents or guardian and agree

on the level that matches your age and needs. Don’t try to crack them.

4) If you receive a file you are unsure of or don’t know who has sent it, do NOT open it. This is the way Trojans and viruses infect your machine.

5) Get a feeling for your machine and how it works so that you can act if you spot something unusual.

6) Learn to check who you are connected to. Learn to use tools like “Netstat” which is a command-line tool that displays network connections (both incoming and outgoing).

7) Finally, a great way to make sure that your parents or guardian agree with your online life is to set up a written agreement with them. The purpose is to reassure them that you are aware of the risks associated with being online, knowing how to behave and what to do, as well involving your parents or guardian making them understand what you actually do when you are online. The agreement needs to be based on a mutual agreement between you and your parents or guardian. There is an example of such a contract at the end of these guidelines (Appendix 1). You will be able to find different versions of a Family Internet Safety Contract online.

### 2.2.8 Your online rights

1) You have the right to make use of technologies to develop your personality and help increase your capabilities;

2) You have the right to protect your identity;

3) You have the right to participate, have fun and access information appropriate to your age and personality;

4) You have the right to express yourself freely, and be treated with respect while always respecting others;

5) You have the right to be critical and discuss anything you read or come across when online;

6) You have the right to say NO if someone makes you feel uncomfortable with his/her requests when online.

7) You have the right to report harmful content found in your internet use.

### 2.2.9 Your online responsibilities

1) You have the responsibility to report harmful content found in your internet use;
2) You have the responsibility to report harm done to other children and friends online;
3) You have the responsibility to manage the time you spend on the internet.

## 2.3 Guidelines for the age group 5-7 year old

Many young people in this age group will not be able to read or understand Guidelines of this kind. Their usage should be closely supervised at all times by a parent or guardian. 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 to the internet e.g. by constructing a list of safe web sites which are age appropriate. The aim is to provide this age group with the basics in 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.

## 2.4 Guidelines for the age group 8-12 year old

There are lots of different things you can do online. While most of the time it's all great fun, sometimes things don't go as well as you hoped and you may not immediately know why or what to do about it. This section has some really helpful tips to help you to be safe online.

Chatting to friends using IM, in chat rooms and on social networking sites can be great ways to keep up to date. Meeting new friends online is also fun. You can meet people online who like the same movies or sports as you. But while there are lots of good points about keeping in touch with online friends, there are also some risks with meeting people online - especially if you don't know them in real life. To help stay safe while you chat, remember these simple tips:

1) Be careful who you trust on- line. A person can pretend to be someone they are not.

2) Choose your friends. While it's 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. Don't accept friend requests if you really don't know the person and you're not sure about them.

3) Keep your personal details private. Use a nickname instead of your real name if you are in a site or game where there may be lots of people you don't know. Ask your parents or guardian before giving anyone on the Internet your name, address, phone number or any other personal details.

4) Set your profile to private. Ask your parents or guardian to help you do this if you're not sure. It's really important.

5) Always keep your password secret. Don’t even share it with your friends.

6) If you want to arrange to meet someone you’ve met online, check with a parent or guardian first and ask them to go with you. Always meet in a brightly lit public place where lots of other people will be around, preferably during the day.

7) If someone writes something rude, scary or something you don’t like, tell your parents, guardian or another adult you trust.

### 2.4.1 Netiquette

Sometimes it’s easy to forget that the other person you are chatting to on IM, playing a game with, or posting to their profile is a real person. It’s easier to say and do things online that you might not do in ‘real life’. This may hurt that person’s feelings or make them feel unsafe or embarrassed. It’s important to be kind and polite to others online - stop and think about how your behaviour will affect them.

**Tips**

1) Treat other people the way you would like to be treated.

2) Avoid using bad language and don’t say things to someone to make them feel bad.

3) Learn about the ‘netiquette’ of being online. What’s considered okay to do and say and what isn’t? For example, if you type a message to someone in UPPER CASE they may think you are shouting at them.

4) If someone says something rude or something that makes you feel uncomfortable, don’t respond. Leave the chat room or forum straight away.

5) Tell your parents, guardian or another adult you trust if you read upsetting language, or see nasty pictures or something scary.

### 2.4.2 Playing online games

Playing games online and using consoles or games on a computer can be great fun, but you need to be careful about how much you play and who you play with. It is important that if you chat with other gamers you protect your privacy and don’t share personal or private information. If you are unsure whether a game is suitable, ask your parents, guardian or a trusted adult to check its classification and reviews for you.

**Tips**

1) 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.
2) Limit your game play time so you can still do other things like homework, jobs around the house and hanging out with your friends.
3) Keep personal details private.
4) Remember to make time offline for your friends, your favourite sports and other activities.
5) Remember it is easily addictive to always stay online, which can make you vulnerable to internet dangers, you should therefore, exercise self-discipline.

### 2.4.3 Bullying

The same rules apply online as in the ‘real world’ about how to treat other people. Unfortunately, people don’t always treat each other well online, and you, or a friend, may find that you are the target of bullying. You might be teased or have rumours spread about you online, receive nasty messages or even threats. It can happen in school, or out of it, any hour of the day, from people you know, and sometimes people you don’t know. It can leave you feeling unsafe and alone. No one has the right to bully another person. At its most serious, bullying is illegal and can be investigated by the police.

**Tips**

**If you are being bullied online:**

1) Ignore it. Don’t respond to the bully. If they don’t get a response they may get bored and go away.

2) Block the person. This will stop you seeing messages or texts from a particular person.

3) Tell someone. Tell your mum or dad, 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.

4) Report it to:
    - Your school - they should have policies in place about bullying.
    - Your ISP and/or phone provider or the website administrator - there are actions they can take to help.
    - 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.

#### Help stop bullying:

1) 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.
2) 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.
3) Remember to treat others as you would like to be treated when communicating online.
4) Raise the alarm when you see any statements on your friends' social media sites that may suggest that they are in distress.

### 2.4.4 Your digital footprint

It's great to share things online with your friends. Part of the fun of sharing videos, images and other content, is that lots of people can view and respond. Remember that what you share with your friends may also be viewed by others whom you don't know. They may also be able to look at it for years to come. Everything you post adds up to your digital footprint and, once it's online, it could be there forever. So think before you post.

#### Tips

1) Keep your personal details private. Use an appropriate nickname instead of your real name. Ask your parents or guardian before giving anyone on the Internet your name, address, phone number or any other personal details.

2) Don't share your username or password with anyone.

3) Think before you hit send or post. Once posted, it can be difficult to remove content.

4) 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.

5) 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.

6) 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.

### 2.4.5 Offensive or illegal content

When you’re surfing the web you may come across websites, photos, text or other material that makes you feel uncomfortable or upset. There are some easy ways to handle these situations.

**Tips**

1) Tell your parents, guardian or another trusted adult if you come across material that upsets you.

2) 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.

3) If a website looks suspicious or has a warning page for people under 18 years, leave immediately. Some sites are not meant for kids.

4) Check with your parents or guardian that your search engine is set to block material that is meant for adults.

5) Ask your parents or guardian to install internet filter software to block bad sites.

6) Ask your parents or guardian to help you find safe and fun sites to use and bookmark for later.

## 2.5 Guidelines for the age group 13 year old and above

At the onset, it is important to note that all guidelines discussed above, under the age group 8 to 12 years old are also equally relevant to those in the age group 13 years old and above. Readers above 12 years of age are therefore encouraged to read the guidelines and tips given above for those below 13 years.

A huge number of young people in this age group use social network sites, online games and Instant Messenger applications. Going online is not just something they do occasionally or for fun. For many it is an integral part of their daily lives. It is how they stay in touch with and communicate with their friends, how they organize large parts of their social lives and school work. Here you will find information on how to be safe using these online platforms as well as insight into what you can do to help create a safe and positive online space for you and your friends.

### 2.5.1 Harmful and illegal content

Curiosity, interests, and a desire to learn new things and explore new facets of knowledge: the Internet is a great tool to satisfy such needs. But the Internet is an open world in which everyone is free to circulate news or almost anything else. It contains an infinite amount of information, so vast in scope that it is easy to get lost or run into untruths and material not appropriate to your needs or age. We are referring to sites that, for example, promote racial hatred or incite violence, sites which could lead you to come across pornographic or child abuse material. This can occur in a purely accidental way, as in the case of searches on completely different subjects, through e-mailing, P2P programmes, forums, chat rooms and, more generally, through the many channels involved in social networking.

**<u>Tips</u>**

1) Before starting a search you should have a clear idea of what you are looking for;

2) In order to narrow things down you can use advanced search functions or directories, that is, the thematic categories that most search engines provide (i.e., for sports, health, cinema, etc.);

3) Put your critical sense to work and try to determine whether the site is trustworthy by watching out for the following:

   - When you access the site do other pages begin to automatically open?
   - Are you able to find out who owns the site?
   - Is it easy to contact the owner?
   - Can you tell who wrote the page or particular article you are viewing? (You can always do another search to find out more about the author and/or owner). Make sure you have written the website address correctly; there are some sites that use a name similar to another to take advantage of possible incorrect typing.
   - Is the site's text spelt correctly or are there grammatical errors?
   - Are there dates included that can indicate whether the site has been updated?
   - Are there any legal notes (regarding, for example, privacy)? ;

4) If, while surfing online, you come across sites containing violent, racist, illegal or child abuse materials don't forget that these sites can be reported to the police or Childline hot line 116. Try to find out to whom you can send

these reports in your country; your parents, guardian or another adult you trust can also help you in filing a report. You should also talk to someone about what happened and any feelings you may still have about the occurrence/experience;

5) Contents (images, videos, etc.) that are found on the web relating to sex, can often be of a pornographic nature and convey sexual material in a typically adult manner with sentiments which are not appropriate to your age group.

### 2.5.2 Grooming

The Internet and mobile phones can potentially be used by abusive adults to make contact with 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.

Sexual predators use the Internet to contact children and young people for sexual purposes, often using a technique known as "grooming". 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 even tickets for transportation 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 video-taped, 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 web cam to broadcast it. Many children and young people who get drawn into these kinds of predatory relationships will lack a certain level of emotional maturity or have low self-esteem. That can make them susceptible to this kind of manipulation and intimidation. They 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.

**Tips**

1) 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 in order to create an atmosphere of familiarity and trust that could lead to an off-line meeting and possible abuse;

2) Protecting your personal 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;

3) In order to enter a chat room, forum, or more generally, a social network, you often have to 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;

4) 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 people who you already know and trust in real life.

5) If attempts at allurement or awkward situations should occur, it is important to find someone to speak to, an adult or friend; Internet service providers will also often allow users to report incidents by clicking on “report” or “notify”, in order to report the abuse. Alternatively, you can turn directly to Police Victim Friendly Units;

6) 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.

### 2.5.3 Cyber Bullying

Through services such as e-mail, forums, chat rooms, blogs, Instant Messaging programmes, SMS and MMS, and video cameras, it is possible to keep in touch with old friends or make new ones in real time and in all parts of the world and to exchange ideas, play games, carry out research, etc. Although most of these services and the ways they are used are positive, in some cases these same tools can be used to offend, deride, defame and annoy Internet users; and furthermore, violent or offensive off-line behaviour becomes magnified when filmed with mobile phones and exchanged or posted on the Net.

What is bullying? Bullying is the act of intentionally causing harm to another person through verbal harassment, physical assault or other more subtle methods of coercion such as manipulation. In everyday language 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.

Very often bullying takes place in schools or local neighbourhoods. Unfortunately, there are increasing numbers of bullies and real forms of bullying online, ranging from offensive websites to harassing text messages, and sending unwanted photos via mobile phones and so on. This particular form of bullying which can possibly offend and hurt someone without necessarily involving any physical contact can have just as painful consequences as that of traditional forms of bullying.

For this reason it is important that you know that this phenomenon exists and that you are aware of the different forms it can take and what can be done to avoid becoming a victim:

**Tips**

1) Do not circulate your personal data thoughtlessly, as this could make you easily identifiable and more prone to acts of bullying and intimidation by others your own age;

2) Once information is posted online it is out of your control and available to anyone and open to any sort of use. You need to be completely clear on this concept; what may seem like an innocent joke could wind up having very irritating and hurtful consequences for others;

3) It is important to refrain from reacting to provocations received via SMS, MMS, instant messages, in offensive or defamatory e-mails, in chat rooms or during online encounters with other users. Instead you need to employ certain strategies that can exclude or limit the actions of those attempting to provoke you such as:

   - Many games allow for the exclusion of undesirable (or unwanted users);

   - When chat rooms are monitored, it is possible to save the offending text from the chat and report it to the monitor;

   - Abuses can be reported to service providers or, in the case of abuse via mobile phones, the report can be sent to the mobile phone company;

   - In the more serious cases, such as cases involving physical threats, it is advisable that the police also be informed;

   - It is possible to trace the e-mail account from which the offensive message was sent, but practically impossible to prove who actually used it to send the message. The online bully could also hack into someone else's account and use it for his/her offensive behaviour and therefore letting the blame fall on the unfortunate person whose e-mail account was wrongfully used;

   - Most e-mail programmes offer filters to block unwanted incoming e-mails.

4) Many instant messaging programmes offer the possibility of creating a list of names that users can choose to block. In this way, you can prevent

unwanted people from making contact with you. An Instant Messaging (IM) system lets you know when one of your known and approved contacts is online and, at that point, you can begin a chat session with the person you feel like talking with;

5) There are quite a number of different IM systems, such as ICQ, AOL Messenger, Yahoo Messenger! Bullies know which are the most popular among youngsters and make use of them for their own purposes such as flaming, or provoking an online fight. Conversations or fights that break out online can, at times, have after-effects that drag on at school or other places offline.

6) In all cases remember that it is important to tell someone about what is happening if you ever feel at all uncomfortable or threatened. Tell your parents, guardian, teacher or someone within the school staff you feel you can trust. Even telling your friends could be helpful.

7) You can also report to the service provider or mobile operator, and even to the police if it is serious. Remember to save the evidence of the bullying, as this will be really important when you tell someone.

### 2.5.4 Defending your privacy

Nowadays, setting up a blog or a personal website, is relatively simple. In order to join a chat room, forum or more generally, a social network, you must first put together a personal profile that includes more or less detailed types of information. Different sites have different rules. Before you enter any information about yourself into a site’s database or membership records, check how the information might be used, whether or not some or all of it will be published, and if so where. If you feel uncomfortable with the amount of information being asked of you, if you do not really know or trust the site, don’t provide it. Look for another or similar service which asks for less information or promises to treat your information more carefully. Wherever possible it is advisable to create an identity (or alias) by using an invented nickname and not add anything else. Above all it is important for you to have a clear understanding of what may be and what is best not to share with others. What goes online can quickly go beyond your control and be at anyone’s disposal for any possible use:

**Tips**

1) Whenever you need to divulge your personal data make sure that whoever is requesting information about you is authentic and serious and also remember that before giving data regarding your friends you need to first inform them and have their permission because they may not be happy about having their e-mail addresses or other information about them passed on to others;

2) You may not be obliged to provide all of the information requested of you and you should insert only the types of data that are strictly required. In any event, it is always best to find out as much as possible about the

person, service or company you are dealing with before providing your data. In particular check to see if the site asking for the data proposes to send you any advertising material, or if they propose to pass on your details to any other companies. If you don’t want them to do either or both of those things, tick the relevant boxes. If they don’t offer you an option you really should think about not using the service at all.

3) Send personal photos and videos only to those you actually know, your image constitutes personal data and you need to make sure it is not circulated thoughtlessly. The same goes for images of others. Keep in mind that it is practically impossible to determine where an online image can end up; before filming or photographing someone you should always ask for their permission;

4) When you need to register for a particular service, try to employ a few simple devices: for example, use a password that would be hard to figure out so that no one else can guess it and get into your account ; use a complex e-mail address, possibly with both numbers and letters (e.g. mrxt3wec97@... . com) so it becomes more difficult to guess by spammers or unknown people who might want to send you unwanted mail; make sure your anti-spam service (for incoming e-mails) and anti-virus controls (for e-mail attachments) are activated and continuously updated; use two e-mail addresses, one which is strictly personal and for correspondence with only your real life contacts (friends, relatives, and such), and another to be inserted in all those online registration forms that ask for personal data (user profiles, competition announcements, online games, etc.) that you already know could be accessed by strangers.

5) Do not open email attachments from sources you do not know or programmes you do not know the possible effects of, they could be a Key Logger (capable of recording all the keys being punched on the keyboard, enabling them to find out passwords, numeric codes, credit card numbers etc.), E-Grabber (capable of gaining access to all the e-mail addresses stored on the victim’s PC), or Info Grabber (capable of extracting information such as the various Registration Keys of a PC’s most important programmes). Without your knowledge these programmes can send over the Internet all the information these programmes pick up to unknown persons.

6) Only engage in activities that you feel you are absolutely sure about. If you “smell something fishy”, something that’s not quite right, that doesn’t totally convince you, or you think is being unjustly charged for, then your best move is to leave it alone. You have the right to criticise and question what you come across while online. Remember things are not always as they appear.

### 2.5.5 Respecting copyright

What is great about the Web is the infinite possibilities of finding and accessing all kinds of materials through search engines and they can be downloaded either free of charge or paid for through your PC or mobile phone, and then used offline.

Not everything found online can be used as you might wish; a lot of content is protected by copyright law or entitlement rights.

Peer to Peer (P2P) software enables one to share and exchange one’s files directly with other Internet users, without any extra connection costs. Music, films, videos, and games are among the materials that are most sought after and downloaded by youngsters, but they are often covered by copyright provisions and protected by law. Unauthorized downloading and distribution of copyright-protected content is a crime in most countries and punishable by law. It is also possible for your involvement in illegal downloading of copyrighted material to be traced. This has led, for example, to a child’s parents or guardian being sent an enormous bill to cover the cost of the material downloaded and if the family refuses to pay the bill other forms of legal action can be taken. Some countries are considering banning people from using the Internet if they are caught persistently using it to obtain unauthorised access to copyrighted material. In addition, when using other people’s work, like articles or dissertations, remember to quote the sources appropriately. If you fail to do so it will be classified as plagiarism and that can cause you a great deal of trouble.

**Tips**

1) You are free to use, modify and distribute freeware programmes that are not copyright-protected;

2) Some software are, on the other hand, shareware, and therefore free for a specific trial period;

3) Your privacy and your PC could be harmed by viruses or other “malware”. It is therefore always best to install and continuously update protection systems such as antivirus, anti-dialer software and a firewall. Always make sure to read the guide relating to the programme you are using to avoid making the errors that are listed below;

4) Copyright protected material is generally indicated by standard wording, such as “all rights reserved” or other similar phrasings; in cases where this is not evident, it is nonetheless best not to take any risks;

5) The Peer to Peer (P2P) programmes you use to share and download files also carry certain risks. One must have a very thorough understanding of them to be able to use them without running any security risks:

   - You may not always end up downloading what you intended to download. Different types of content may be concealed behind the title of a song or video. In the worst cases, for example, it might contain child abuse images. Examine your particular programme guide to find out how you can detect fake files and only go to sources you know are trustworthy. Ask your friends to tell you which sources to use and which to avoid;

   - Before opening a downloaded file make sure to scan it for viruses;

another quite frequent risk is in fact that a downloaded file might contain viruses and spyware that can put PCs, personal data and privacy at risk;

- Do not share your entire hard disk: check your configurations to ensure that you have shared only those folders you wanted to share and remember that sharing files protected by copyright is a crime.

### 2.5.6 Online commerce

You can purchase products online or by using a credit card (e.g. Visa, Mastercard) or a mobile phone (e.g. One Wallet, Ecocash, Netcash and Telecash). Purchases can be made by credit card or, in the case of mobile phones, by debiting the credit on the mobile phone subscription. There are also online spaces devoted to exchanges and purchases of all sorts of products, at very competitive prices.

One of the fundamental difference between online and traditional commerce lies with the difficulty in identifying who is at the other end of the exchange and the risk of fraud that may lie just around the corner. One of the most widespread risks is that of “phishing”. This happens when people respond to fake email spam, which usually appear to come from a reputable source e.g. a bank or credit card company. They will ask you to enter a lot of personal information e.g. bank account details, passwords, date of birth and so on, which they will then misuse. Avoid sharing your passwords and be in the habit of constantly changing your passwords.

An additional complication with online commerce concerns the sale of products or services which are age restricted in some way. For example, in many countries it is illegal for vendors to sell or provide alcohol or tobacco to legal minors. Gambling is also generally limited to people over a certain age. Yet in the online environment it can be very hard for the vendor to determine the age of the person proposing to make the purchase or acquire the service. All that many companies do is ask the person to check a box to confirm they meet the minimum age requirement.

Some companies in a number of countries are beginning to deploy age verification systems linked to their purchasing procedures, but this is still a very new and limited technology, however it is a growing practice. Buying age restricted products online and telling lies about your age in order to do so, means you could be committing a criminal offence and so could the vendor. You could forfeit the goods and you could end up with a criminal record, so don’t do it.

There are, in any case, a series of tactics that can help you reduce the risks and enable you to make use of the convenient opportunities offered by online commerce:

**Tips**

1) Take great care in choosing the sites that you want to make purchases from and ensure their credibility. Gather as much information as you can about the site in question, such as name, address, telephone number and head office of the company, description of the contract’s general conditions and, in particular, how to with- draw from the purchase; also find out about the protection and management of personal data and

payment security; and compare prices, looking for the same item on other sites;

2) Prepaid credit cards, or ones that can be topped up, come with spending limits and can help avoid unpleasant surprises.

3) Before you buy anything online, make sure the site uses a secure system for transactions so as to prevent, for example, “sniffing”, which is a means of capturing data during transmission. Even though many sites incorporate systems that counter the interception of data in transit, your details could still be stolen if someone hacks into the server of the company where your credit card details have been stored. Clearly, by choosing other modes of payment you can avoid the possibility of someone stealing your credit card number;

4) If you receive an unsolicited e-mail offering you an incredible deal, it is highly likely that it is fraudulent;

5) If something looks too good to be true, it most probably is, and it would be best to forget about it;

6) In the case of purchases made by mobile phones for which a credit card is not required, verify what the costs of the services actually are, the service’s conditions of agreement and how one can back out.

## 2.6 Conclusion

By keeping these basic rules in mind, you will be able to steer clear of the majority of the pitfalls you can encounter online. Should you encounter unpleasant or disturbing experiences, make sure you talk to someone you trust. Remember, you have the right to be protected as well as the responsibility to act appropriately, offline as well as online.