CMSGu2013-06

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Child Online Protection

CERT-MU

National Computer Board
Mauritius

December 2013

Issue No. 6

Version 1.1

Table of Contents

1.0 Introduction....4
1.1 Purpose and Scope....4
1.2 Audience....4
1.3 Document Structure....4
2.0 Background....5
3.0 Common Usage of the Internet by Youngsters....6
3.1 Interactivity and User Generated Content....6
3.2 Social Networking Sites....6
3.3 Instant Messaging and Chat....7
3.4 Peer-to-Peer File Exchange Programmes....8
4.0 Child Abuse Material (CAM)....9
5.0 Main Risks to Children Online....11
5.1 Content....11
5.2 Contact....11
5.3 Conduct....11
5.4 Commerce....12
5.5 Excessive use....12
5.6 Societal....12
6.0 Recommendations for addressing the risks....13
7.0 General Rules for Staying Safe Online....15
7.1 Set Your Limits....15
7.2 Meeting Online Friends Offline....16
7.3 Accepting Invitations / Friendships....16
7.4 React....17
7.5 Tell Someone About Your Concerns....17
7.6 Learn To Use Your Machine Safely....18
7.7 Your Online Rights....18
8.0 Guidelines for different age groups of children....19
8.1 The first age group: 5-7 year old....19
8.2 The second age group: 8-12 year old....19
8.2.1 Chatting....20
8.2.2 Netiquette....20
8.2.3 Playing Online Games....21
8.2.4 Bullying....21
8.2.5 Your digital footprint....23
8.2.6 Offensive or illegal content....23
8.3 The last age group: 13 year old and above....24
8.3.1 Harmful and illegal content....24
9.0 Conclusion....26
10.0 References....27
Appendix A....28
List of Acronyms....28

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide guidance on how the evolution of the Internet has impacted children and young people. It is also meant for protecting them from the dangers arising from new technologies and being always connected to the Internet.

1.2 Audience

The targeted audience for this document includes parents, teachers and children who make use of the Internet and also law enforcement agencies who are involved in enforcing new policies and regulations at national level.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an overview of the document's content, the targeted audience and the document's structure.

Section 2 presents a background the on how the Internet has evolved in the past years.

Section 3 describes the common usage of the Internet by youngsters.

Section 4 provides an outline on Child Abuse Material.

Section 5 portrays the main risks children are exposed to while being online.

Section 6 provides some recommendations to address the underlying risks.

Section 7 gives some general rules on how to stay safe online.

Section 8 illustrates some guidelines for different age groups of children.

Section 9 concludes the document.

Section 10 consists of a list of references that have been used in this document.

Appendix A provides a list of acronyms that have been used in the document.

2.0 Background

The Internet is now in full force since quite a few decades. Nevertheless, its nature has changed dramatically since its origin. In the beginning it was merely a tool for exchanging information and data between governmental agencies and academic institutions. In the 1980s, the Internet was made accessible to the general public. With the advent of the World Wide Web in the 1990s, the Internet started to grow at an astounding rate. The web has become more interactive and a much larger number of people have a presence on the Internet, with children and young people very often being at the forefront of adopting and adapting to new technologies.

New developments in technology helped in establishing a new type of Internet; instead of simply connecting individuals to firms, organisations and governments, the Internet also began to enable individuals to connect with each other and allow them to become their own online publishers. This new Internet, often referred to as Web 2.0, has the following characteristics:

- High levels of connectivity
- High bandwidth
- High levels of storage capacity
- Personalised and interactive contact (user generated content)

New tools have been developed, providing users with various means to socialise and connect with each other. These tools include: SMS, e-mail, instant messaging (chat), online dating, multiplayer gaming, photo and video hosting services, and peer-to-peer file exchange programmes (P2P). Taken together, these technologies and others have given rise to the extraordinary growth in social networking sites which in a very short period of time have become very much popular amongst children and young people.

The present digital world has transformed everyone's life. Being always online has become the rule of thumb, with people spending more and more time consuming digital media than any other medium. Although these technologies mean added advantage and entertainment for many, regulators and users are often one step behind the fast-paced innovations in this field.

3.0 Common Usage of the Internet by Youngsters

3.1 Interactivity and User Generated Content

Children and young people, as well as adults, increasingly make use of these new technologies in their everyday lives, and as a result, the nature of the risks they take is linked to their behaviors. It is now practically impossible to differentiate between so called "Internet issues", and "real world" problems.

3.2 Social Networking Sites

Social networking sites allow users to create an online profile in which they can display a lot of personal information, such as age, gender, location, relationship status and interests. In particular the new interfaces developed by the social networking sites make it simple to personalise individual user web pages, for example by adding some of the users' favourite music, photographs and videos.

Children and young people are very much engaged in this innovative process. User profiles on a social networking site have become the virtual part of the users and an important way for the users to express themselves with their friends and the wider world. Most importantly, social networking sites allow users to add friends with whom they can exchange messages, images and videos. The audience that can view an individual's profile normally depends on the user's site's privacy settings.

Frequently, particularly in the early days of social networking, children and young people appeared to be unaware that, unless they took specific steps to limit access, for example by setting their profile to "private" or "friends only", their full profiles would be open for anyone to view. This made them vulnerable to online predators, who might have hidden their age in order to build a relationship with the child or young person. There have been cases reported to CERT-MU, where some children and young people have posted sexualized or obscene images of themselves, or have exchanged them via mobile phones, a phenomenon known as "sexting" often without realising that the image itself might be both harmful to them and illegal, but, also, it might be viewable by large numbers of people who visit their site or profile.

Social networking sites have highlighted the problem of how to manage user generated content, the characteristic feature of Web 2.0. Some sites have developed proactive violation

policies, where they search out inappropriate or illegal videos and images, whereas others only look at an individual picture or video if it is drawn to their attention by a report from someone who finds it to be objectionable and wants it removed.

A few examples of social networking sites are: MySpace, Facebook, Hi5, Orkut, Friendster and LinkedIn.

Online expressions, personal profiles or other types of postings have four fundamental characteristics that can lead to additional risks for children and young people:

1. **Permanence:**
   Networked communications such as chat messages, videos and photos can be saved and stay on the net permanently.

2. **Searchability:**
   By knowing someone's identity online, it becomes easy to help find others with the help of search and discovery tools.

3. **Replicability:**
   Networked communications can be copied from one place to another in such a way that there is no possibility to distinguish the "original" from the "copy."

4. **Invisible Audiences:**
   With the advent of anonymisers, it has become practically impossible to determine who might run across profiles or other online communications. This is further complicated by the other three characteristics mentioned above, since profiles may be viewed or accessed at a different time and place from when and where they were originally created.

3.3 Instant Messaging and Chat

Instant messaging (IM) tools allow people to connect with others online directly and have conversations through written messages and increasingly through video conferencing. People can add the names of individuals they know to their contact list and can see if they are online.

These conversations, or “chats”, can be held with one person or with a group of people. With most tools, the content of the conversations can be saved if wanted or required.

Well known IM and chat programmes include Skype, Facebook chat, MSN Messenger, Yahoo! Messenger and Google Talk.

3.4 Peer-to-Peer File Exchange Programmes

Peer-to-peer (P2P) file exchange programmes allow individuals to directly upload and download files from and to their own storage discs. Anyone using the same programme can search for files and download them from others that have these files available. These programmes make the sharing of knowledge and information easy, but have also led to copyright infringement and the proliferation of malicious software (malware) such as viruses and Trojans. These networks are also used to distribute Child Abuse Material (CAM).

Well-known P2P programmes include Bittorrent, E-mule, E-donkey and Kazaa.

4.0 Child Abuse Material (CAM)

In many jurisdictions, still images or videos of children being sexually exploited and abused are called either "child pornography" or "indecent photographs of children". Today many practitioners prefer to use the term "Child Abuse Material" or CAM because it is felt that this term more accurately conveys the real nature of the content. The Internet has completely transformed the scale and nature of the production and distribution of CAM.

The sexual revolution of the mid 1960s, marked by the openness to sexual expression and variation, encouraged a growing demand for pornography. Some of the pornography that was bought, sold or traded included images of children being sexually abused. Anti-CAM laws passed in 1977 in the United States soon spread to Europe and the production of CAM soon vanished and was driven underground. By 1986, almost all the traditional channels for obtaining this kind of material had disappeared, increasing the thorough containment of the CAM trade.

At that time, the difficulties of finding CAM meant that people who wanted to indulge in CAM had to take huge risks and a lot of expense in order to get access to such material. All of this changed with the advent of the Internet.

The following 3 A's for cyber sexuality can easily be transferred to the way the Internet revolutionised the possession and distribution of CAM:

- Accessibility - the Internet makes CAM available 24/7 all the year round
- Affordability - most CAM is free and available for exchange or download
- Anonymity - people genuinely believe that their communications on the Internet are private and hidden

This encouraged predators to hunt for and deal in CAM as they felt there were no consequences. The fact that it was free and available also encouraged the belief that it was harmless. Today CAM is a global industry. It seems that no country is immune. It is very difficult to determine the exact size or shape of what is essentially an undercover and often illegal venture. A lot of estimates have been made at different points about the number of web sites involving the number of children being abused to create the images and of the total monetary value of the market in the images. The number of illegal images now in circulation

on the Internet runs into many millions, while the number of individual children depicted in those images runs into the tens of thousands. Appallingly, these are only the ones that have so far been discovered.

Originally one of the main ways of distributing CAM over the Internet was from within Usenet Newsgroups. That remains an important source but today several other Internet technologies are also being used. Out of these, the World Wide Web is considered the most important, because it is the most accessible and easiest to use. However, as some countries have made it very difficult to use the web to distribute CAM, other Internet technologies are also being used more and more frequently. In such cases, P2P or file sharing software is seen as the most common technology regarding the distribution of CAM. According to Interpol, P2P is technically quite easy to regulate, however the huge number of people involved makes it virtually very difficult.

Every time the image of a child being abused appears on the Internet or is downloaded, in a way, that child is being re-abused. Victims must live with the lingering existence and widespread view of these images for the rest of their lives. The best proof of this is the reaction of the victims and their families when they learn that the images have been circulated or uploaded to the Internet.

For that reason, it is recommended that as soon as a child abuse image or website is discovered it is important to move as quickly as possible to remove the image or have the website taken down or rendered inaccessible.

Another reason for moving quickly to remove or render inaccessible any illegal images found on the Internet is because the longer they stay up the greater the possibility that a new person will find the image and perhaps download it. It is believed that people who get involved in downloading and collecting CAM are more likely to engage in contact offending or abusing children in the real world.

5.0 Main Risks to Children Online

While adults and children alike are exposed to a range of risks and dangers online, children and young people are often particularly vulnerable. Children are still in a process of developing and learning. That is why it is difficult for them to identify, assess and manage potential risks. The idea that children are vulnerable and should be protected from all forms of exploitation is outlined in the "UN Convention on the Rights of the Child". There are a number of issues in relation to children's and young people's use of the Internet which are of ongoing concern to parents and children alike, as well as to governments. These concerns can be summarised as follows:

5.1 Content

- The Internet's ability to expose children and young people to illegal content, e.g. CAM.
- The Internet's ability to expose children and young people to legal but age inappropriate material e.g. very violent imagery.

5.2 Contact

- The Internet's ability to expose children and young people to sexual predators, be they adults or other legal minors.
- The way in which the Internet may expose children to harmful online communities such as sites which encourage anorexia, self harm or suicide as well as sources of political influence supporting violence, hate and political extremism.

5.3 Conduct

- The way in which the Internet facilitates and can promote risky sexual interactions between children themselves, including encouraging them to take and post pictures of themselves or others (sexting) which, aside from being harmful, may also be illegal.
- Normal sexual development and experimentation online can sometimes result in the unintentional production and distribution of CAM exposing the child and his friends to possible legal sanction(s).
- The way in which some features of the Internet encourage children to publish information about themselves, or post pictures or videos or text which might

compromise their personal safety, promote blackmailing (through *Sextortion*[1]) or even jeopardise their career in the future.

- The Internet's ability to expose children and young people to cyberbullying and to allow or promote an environment in which children and young people are encouraged to bully others.

5.4 Commerce

- The ways in which the Internet has enabled children to access or acquire age inappropriate goods and services, typically goods and services which they could not purchase in person from a shop.
- The Internet's ability to expose children and young people to scams, identity theft, fraud and similar threats which are financial in nature or breach data protection or privacy laws.

5.5 Excessive use

- The way the Internet seems, with some children and young people, to have encouraged forms of obsessive behavior or excessive use which may have harmful effects on children's and young people's health and social behaviour.
- Games and gaming over the Internet often feature in this type of online behavior, which in some countries is referred to as a form of addiction.

5.6 Societal

- The way the Internet has opened up a new digital divide among children and young people, both in terms of those who have ready it at home, school and elsewhere, and those who do not; between those who are confident and proficient users of it and those who are not. This divide threatens to widen existing patterns of advantage and disadvantage or perhaps create new divides.
- The potential of the Internet to increase the existing vulnerabilities of particular children and young people and add to dangers that they may face in the offline world.

[1] Sextortion: is an emerging phenomenon in which predators take advantage of webcams and the emotional vulnerability of teenagers to elicit sexual favours. The predators typically meet their victims on social media sites and draw them into exposing themselves on a webcam. The predators normally record that footage without the victims' knowledge. Some also extort the victims with the threat of posting it to a wider audience. In exchange for keeping the humiliating photos or footage secret, the predators or sextortionists may demand that the victim perform other sexual acts on camera or money.

6.0 Recommendations for addressing the risks

Recommendation	No.	Description
Comprehensive Legal Framework	1	A body of laws should be in place, which makes it clear that each and every crime that can be committed against a child in the real world can also be committed on the Internet or on any other electronic network. In Mauritius, we have the following legislations in place to address the risks of child online safety: • Child Protection Act 1994 Section 14 (1)(a) - Causing, inciting or allowing a child to be sexually abused • Child Protection Act 1994 Section 15 and Computer Misuse and Cybercrime Act 2003 Section 22 – Indecent photographs of children • Information and Communication Technologies Act 2001 Section 46 (f) – Use of an information and communication service, including telecommunications service (i) for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character; or (ii) for the purpose of causing annoyance, inconvenience or needless anxiety to any person. • Child Online Protection Bill (Forthcoming legislation) – Addressing grooming or child luring online, where an adult lures a child online, leading to meeting where he intends to engage in sexual activity with child.
Need For a National Focus on Online Child Protection	2	The Internet can now be accessed via several different kinds of devices. Computers are only one of many ways of going online. Mobile phones, games consoles and PDAs are also increasingly important. The providers of both wireless and fixed-line access need to be involved. Moreover, in many countries the network of public libraries and Internet cafes can be important sources of Internet access particularly for children and young people. In Mauritius, the National ICT Strategic Plan (NICTSP) 2007-2011 has come up with a Child Online Committee to look into the development of a Child Online Safety Action Plan. This initiative put in place various recommendations from different stakeholders, as follows: • Ministry of Information and Communication Technology • Ministry of Women's Rights, Child Development and Family Welfare • Ministry of Education, Culture and Human Resources • IT Police Unit, Mauritius Police Force • Office of the Ombudsperson for Children

		• National Computer Board (NCB) • Information Communication Technologies Authority (ICTA) • Mauritius Chamber of Commerce and Industry (MCCI) • Internet Child Safety Foundation (ICSF)
Need to Develop Local Resources Which Reflect National Laws and Local Cultural Norms	3	Many of the large Internet companies produce web sites which contain a great deal of information about online issues for children and young people. However, very often this material is only available in English or in a very narrow band of languages. It is very important, therefore, that materials are produced locally which reflect local laws as well as local cultural norms. This is essential for any Internet safety campaign or any training materials that are developed.
Helping Children to Stay Safer Through the Use of Technical Tools	4	A number of software programmes are available and can help screen out unwanted material or block unwanted contacts. Some of these child safety and filtering programmes may be essentially free because they are part of a computer's operating system or they are provided as part of a package available from an Internet Service Provider (ISP). The manufacturers of some game consoles also provide similar tools if the device is Internet enabled. These programmes are not foolproof but they can provide a welcome level of support, particularly in families with younger children. These technical tools should be used as part of a broader arsenal. Parental involvement is critical. As children start growing older they want more privacy and also feel a strong desire to start exploring on their own.

7.0 General Rules for Staying Safe Online

Using the Internet can be fun. Children can enjoy it most by keeping themselves safe. As a child,

- You can do a lot of great things on the Internet. You can play games; you can 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.

- 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. While using the Internet you need to be aware of certain basic rules to be able to safeguard yourself and others.

- 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.

7.1 Set Your Limits

- 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.

- 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 recognise. Other interactive services, for example instant messaging, will often also provide privacy tools. Use them.

- 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.

- 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.

- 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.

7.2 Meeting Online Friends Offline

- Sometimes online contacts develop into friendships.

- 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 or another trusted adult to join you to avoid any trouble in case the meeting turns out to be a disappointment.

- 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.

7.3 Accepting Invitations / Friendships

- 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?

- 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 is nothing wrong with

declining invitations you are not sure about. Getting more and more contacts is after all not the point of social networking.

7.4 React

- 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 or someone you trust.

- Ignore bad behaviour and leave unpleasant conversations or sites with inappropriate content. 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.

- 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.

- 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.

- 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 get 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.

7.5 Tell Someone About Your Concerns

- If you have any concerns or problems while online, you need to tell someone you can trust. Your parents or some other adult can help and give you good advice on what to do.

- You can report harmful or inappropriate content or activities on the websites to the abuse e-mail of the host of the site. You can report illegal content to the ICTA, CERT-MU or to the police.
- You can report illegal or possibly illegal activities to the police.

7.6 Learn To Use Your Machine Safely

- Make sure you have installed and learned how to use a firewall and anti-virus software and keep them up to date.
- Learn about your computer's operating system (like Windows, Linux, etc) and especially about how to patch it and keep it up to date.
- If parental controls are installed then talk with your parents and agree on the level that matches your age and needs. Do not try to bypass them.
- If you receive a file you are unsure of or do not know who has sent it, do NOT open it. This is the way Trojans and viruses infect your machine.
- Get a feeling for your machine and how it works so that you can act if you spot something unusual
- Learn to check who you are connected to, learn to use tools like "Netstat".

7.7 Your Online Rights

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

You have the right to protect your identity

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

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

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

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

8.0 Guidelines for different age groups of children

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. Three principal age groupings of young Internet users have been identified by the Child Online Protection (COP) initiative brought to light by the International Telecommunication Union (ITU). 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, there is not a one-size-fits-all. Nothing should ever be assumed or taken for granted.

8.1 The first age group: 5-7 year old

Many young people in this age group will not be able to read or understand such guidelines. Their Internet usage should be closely supervised by a parent or a trusted adult at all times. Filtering software or other technical measures such as parental controls can also be used to support the use of the Internet by a child of this age. It is recommended limit such a young child's potential access to the internet e.g. by building a list of safe web sites which are age appropriate. The aim is to provide this age group with the basics in Internet safety, good use and understanding.

8.2 The second age group: 8-12 year old

This age group is a challenging evolution for the child. Typically he or she is becoming a young person with a greater capacity to devise questions. Their curiosity will push them to seek out and challenge boundaries, looking for their own answers. 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 common naive 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.

There are many things that this particular age group can do online. Very often things turn out very bad and they do not know what to do about it. Below are some useful tips to help them be safe online.

8.2.1 Chatting

Chatting using IM in chat rooms and on social networking sites can be great ways to keep up to date with friends. Meeting new friends online is also fun. Young people can meet people online who like the same movies or sports as them. However, while there is lots of fun in staying in touch with online friends, there are also some risks with meeting people online, especially if they do not know them in real life. To help stay safe while chatting, this age group can make use of the following tips:

1. Be careful who you trust online. A person can pretend to be someone they are not.
2. Choose your friends. While it is good to have a lot of friends, having too many, makes it harder to keep an eye on who sees what you post online. Do not accept friend requests if you really do not know the person and you are 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 do not know. Ask your parents 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 to help you do this if you are not sure.
5. Always keep your password secret. Do not even share it with your friends.
6. If you want to arrange to meet someone you have met online, check with a parent 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 do not like, tell your parents or another adult you trust about it.

8.2.2 Netiquette

Sometimes it is 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 is 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 is 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 do not say things to someone to make them feel bad.
3. Learn about the 'netiquette' of being online.
4. What is 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.
5. If someone says something rude or something that makes you feel uncomfortable, do not respond. Leave the chat room or forum straight away.
6. Tell your parents or another adult you trust if you read upsetting language, or see nasty pictures or something scary.

8.2.3 Playing Online Games

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

8.2.4 Bullying

The same rules apply online as in the 'real world' about how to treat other people. Unfortunately, people do not 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 outside school

premises, any hour of the day, from people you know, and sometimes people you don't know. It can leave you feeling unsafe and alone. Nobody has the right to bully another person. At its most serious, bullying is illegal and can involve police cases. Tips:

If you are being bullied online:

1. Ignore it. Do not respond to the bully. If they do not 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 voicemails as proof.
4. Report it to:
    - Your school (teachers, rector)
    - The Computer Emergency Response Team of Mauritius (CERT-MU)
    - The Information and Communication Technologies Authority (ICTA)
    - The Cybercrime Unit, 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.

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 will want them to do the same for you.
2. Do not 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.

8.2.5 Your digital footprint

It is 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 do not know. They may also be able to look at it for years to come. Everything you post add up to your digital footprint and, once it is 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 before giving anyone on the Internet your name, address, phone number or any other personal details.
2. Do not 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. Do not post anything you don't want others to know or find out about, or that you would not 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.

8.2.6 Offensive or illegal content

When you are 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 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 'Ctrl-Alt-Del' 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 that your search engine is set to block material that is meant for adults.
5. Ask your parents to install internet filter software to block bad sites.
6. Ask your parents to help you find safe and fun sites to use and bookmark for later.

8.3 The last age group: 13 year old and above

This group is the one covering the longest span. This is the group consisting of 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 likes and dislikes. 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 adult 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.

A large number of young people in this age group use social network sites, online games and IM applications. Going online is not just something they do occasionally or for fun. For many it is an integral part of their daily lives. Below are some tips on how to stay safe using these online platforms as well as insight into what can be done to create a safe and positive online space for young people as well as their friends.

8.3.1 Harmful and illegal content

The Internet is no doubt a great tool to satisfy needs such as curiosity, interests, and a desire to learn new things and explore new facets of knowledge. However, the Internet is an open world in which everyone is free to circulate news or almost everything. It contains such an infinite amount of information 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 materials or CAM. 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.

Therefore:

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. Try to determine whether the site is trustworthy:
    - 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 CAMs, do not forget that these sites can be reported. Your parents 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 which is not appropriate to your age group.

9.0 Conclusion

The evolution of the Internet has brought with it the advent of Web 2.0 and social networking websites. Some websites offer webcam chat sessions, which are appealing to children, but often expose them to high levels of sexual activity and sexualised conversation. To counteract this, it is essential to discuss openly the dangers which exist for children and young people online and teach them how to deal with these. When it comes to the safety of children online, parental involvement and supervision is one of the fundamental measures. On top of this, relevant laws and technical tools are required to protect children online.

10.0 References

- Guidelines for Industry on Child Online Protection (International Telecommunication Union), **www.itu.int/cop**
- Guidelines for Policy Makers on Child Online Protection (International Telecommunication Union), **www.itu.int/cop**
- Guidelines for Children on Child Online Protection (International Telecommunication Union), **www.itu.int/cop**
- Microsoft, **www.microsoft.com**
- CEOP, **http://ceop.police.uk**
- CBC News, **http://www.cbc.ca**

Appendix A

List of Acronyms

CAM	Child Abuse Material
COP	Child Online Protection
IM	Instant Messaging
ISP	Internet Service Provider
ITU	International Telecommunications Unit
P2P	Peer-to-Peer