Digital Wellness Programme

A proposed toolkit to support the promotion of Information Ethics in schools and communities across Africa

ACTIVITY BOOK FOR SECONDARY SCHOOL LEARNERS

Digital Wellness Programme

A proposed toolkit to support the promotion of Information Ethics in schools and communities across Africa

ACTIVITY BOOK FOR SECONDARY SCHOOL LEARNERS

The *Digital Wellness Toolkit* is dedicated as a tribute to the work in the field of Information Ethics by our Brother, colleague and friend

Chief Michael Anyiam-Osigwe

14 April 1959 - 29 November 2014

telecommunications & postal services

Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

This project is co-sponsored by the South African Government via the Department of Telecommunications and Postal Services

Digital Wellness Programme - ACTIVITY BOOK FOR SECONDARY SCHOOL LEARNERS

October 2015

ISBN: 978-1-928261-69-8

Editors
Beverley Malan
Coetzee Bester

Published By
African Centre of Excellence for Information Ethics
Department of Information Science
University of Pretoria, South Africa

Printed By
Groep 7 Drukkers&Uitgewers BK (1993/24129/23)
Posbus 14717, Sinoville, 0129
Tambotieweg 776, Kameeldrif-oos, Pretoria
www.groep7.co.za

TABLE OF CONTENT

INTRODUCTION AND ORIENTATION

Do you own or have access to a computer or mobile phone? Do you use it to chat to other people, to sell unwanted stuff or to find information on something or other? If you do you could regard yourself as a digital citizen. Most of us today have a parallel existence – in the real / physical as well as in the virtual / digital world of the Internet. We have both an everyday and an online identity, the latter reflected on social media sites, gaming portals, discussions forums, learning communities, blogs and websites. In fact, it has become both a need and a habit to connect with other people on the Internet every day. It is important, however, to ensure that our online habits promote rather than undermine our health, values and relationships. In other words, we not only have to maintain a balance between our online and offline lives but we should also take the necessary steps to protect ourselves against dangers and threats lurking in the online world.

This booklet contains a number of readings and activities dealing with digital matters. The readings and activities are aimed at helping you to be more aware of the dangers but also to provide you with tips on ways of protecting yourself against them. Having worked your way through the Activities Book you should:

- *Be aware of* the benefits and dangers of using the Internet
- *Know how to* protect yourself and your electronic devices against these dangers and threats
- *Have* a basic knowledge of the laws governing Internet engagements AND of the legal consequence of transgressing these laws
- *Understand* the difference between responsible and irresponsible, ethical and unethical Internet behaviour.

- *Prof Theo Bothma*
- *Department of Information Science*
- *University of Pretoria*

- *October 2015*

ACTIVITIES AND READINGS

Activity 1(a): Digital know-how

(For learners in Grades 7 to 9)

As children of the digital age you already know how to use the Internet for schoolwork, recreation and the sharing of information. Let's now find out how much you know about digital wellness.

Answer the questions below by circling the response that you think is the correct one.

You have approximately 10 minutes to do complete the quizz.

1. While using a public discussion forum, whose name should you ideally use?
   a. Your own, real name
   b. A nickname
   c. A friend's name

2. When should you accept friendship requests on social networking sites?
   a. Always
   b. Never
   c. Only when you know the person

3. A group of users in a forum where you discuss television shows is asking you to share your photograph. Should you
   a. Upload your latest and best photograph?
   b. Share someone else's photograph?
   c. Politely decline to share photographs?

4. A web-friend has invited you to meet in person. Should you
   a. Accept the invitation?
   b. Ask advice from a parent or trusted adult?
   c. Take another friend along to the meeting?

5. You have to write a report for a school project? Should you compile the report by
   a. Copy-pasting all the information available on different web-sites without any changes?
   b. Rewriting all the information available on different web-sites in your own words?
   c. Merging the essence of information available on different web-sites in such a way that it shows your understanding of what you have read?

Activity 1(b): Digital know-how

(For learners in Grades 10 to 12)

Answer the questions below by writing what you think is the correct answer in the space below each question.

You have approximately 20 minutes to do so.

1. Do you have a safe, secure password? What does it consist of?

_____

_____

_____

_____

_____

2. What is a computer virus?

_____

_____

_____

_____

_____

3. How do you make sure viruses don't attack your electronic devices?

_____

_____

_____

_____

_____

4. What are pop-ups, and what should you do when a pop-up appears?

_____

_____

_____

_____

_____

5. What is pirating when related to digital matters?

_____

_____

_____

_____

_____

6. How should internet users respond to chain e-mails?

_____

_____

_____

_____

_____

7. Can one permanently remove posts from a Facebook Wall? Why/why not?

_____

_____

_____

_____

_____

8. What should you do if your Facebook account is hacked?

_____

_____

_____

_____

_____

9. How can you change your privacy settings on Facebook?

_____

_____

_____

_____

_____

10. What is identity theft and why would other Internet users try to steal your identity?

_____

_____

_____

_____

_____

Activity 2: Digital wellness

(For learners in Grades 7 to 12)

In this activity you are asked to reflect on the term, “digital wellness”.

First study the table which follows the instructions for this activity. The aspects of your life that could be negatively affected by the way in which you or others conduct yourselves on the Internet are listed in the left hand column. The right hand column lists a number of specific Internet behaviours that could negatively affect specific aspects in the left hand column.

Your job is to match the specific behaviour listed in the right hand column with the appropriate aspect in the left hand column. Having done so, you have to explain, in the spaces below the table how the two terms you matched relate to each other.

Table 1: Terminology Mix and match

Vulnerable aspects	Internet behaviours
Health	Phishing
Wealth	Pop-up advertisements
Happiness	Gaming addiction
Safety	Cyber predators
Security	Cyber Bullying

_____

_____

_____

_____

_____

_____

_____

Activity 3: Cyber-speak

(For learners in Grades 7 to 12)

In order to survive in the digital world and benefit from the opportunities that cyber travel offers, digital citizens / Internet users have to master the language of the cyber world. In this activity your group has to design a flash card or poster for each of the terms or concepts that your teacher allocates to the group. This flash card (or poster) will eventually be displayed on the wall of your classroom or computer laboratory to help other learners understand cyber/digital language. You must therefore make sure that the meaning of the term / concept is absolutely clear and understandable.

Each flashcard / poster should include at least:

- The term / concept
- A short definition of the term / concept concerned
- A picture or symbol that graphically illustrates the meaning of the term / concept concerned

Having completed your flash card / poster, display it on the wall of your classroom for other learners to inspect and evaluate. You will also have the opportunity of inspecting and evaluating other learners' posters theirs against the criteria indicated by your teacher.

Activity 4: Cyber threats

(For learners in Grades 7 to 12)

By this time you know that the Internet is full of opportunities which might never have been available to you if there had been no Internet. You might not, for example, have been able to learn about places to which you have never travelled, to communicate with people across the globe, to get information on anything you want at any time of the day or night, and so on.

What we should all remember, though, is that these benefits do not come without risks. Although the digital world is a virtual space it has many similarities with physical spaces and places. Your house, which is a physical space, could, for example, be burgled even if all the doors and windows are closed; your parents' car could be involved in an accident although they wentout of their way to drive safely; a pedestrian could be hit by a car or truck even if he crosses the road when the traffic light is green, and a person might drown in the ocean even if s/he is an excellent swimmer.

The same is true of virtual / digital spaces. You might stumble across a website that displays inappropriate content, find that your e-mail or social networking account has been hacked and/or misused, realize that someone has misinterpreted what you posted on Facebook or discover that someone has posted embarrassing photos or information about you on one or more social media sites.

In this activity you will learn about some of the threats you might face in cyber space. The procedure you have to follow is set out in the steps below.

- From the readings that follow, allocate a different one to each of the members in your group.
- Each person then has to spend a few minutes reading about the threat allocated to him/her.
- When everybody has finished reading, the person who read about the threat has to tell the rest of the group what s/he has learnt from the reading.
- When everybody has had a chance to share her/his understanding or the threat that s/he read about, the group as a whole has to discuss and answer the questions posed in the tables which follow the readings. The first table has been completed as an example of what you are expected to do.
- You have approximately 30 to 40 minutes to complete this activity.

Reading 1

Cyber Bullying – Cyber bullying takes place when a person sends or posts mean, threatening and intimidating messages to someone else. Examples of cyber bullying include abusive e-mails, malicious posts on social networking sites, inappropriate image tagging, uploading of embarrassing photographs, creating fake profiles on web sites designed to hurt another person, and so on. Cyber bullying has serious emotional consequences: those who are being bullied might feel depressed or anxious; their self-esteem might be undermined or they might even consider suicide or revenge.

Reading 2

Cyber Predators – Cyber predators are adults who exploit children and teenagers by means of Information communication tools such as mobile phones, chat rooms, social networking sites and even e-mail. Their main motive is sexual abuse. They fake attention, affection, kindness and sympathy in order to manipulate the children into thinking that they care about them. Once the youngster being targeted has taken the adult into

his/her confidence by sharing sensitive information, the adult arranges a personal meeting with the youngster. These meetings inevitably result in great emotional and, sometimes, physical harm to the youngster.

Reading 3

Gaming addiction - Gaming addiction is the excessive or compulsive use of online games at the cost of health, education, real life social interaction and even cleanliness. Left untreated, gaming addiction could lead to social isolation, mood swings, and an inability to cope with real life.

Reading 4

Identity theft – Identity theft is a fast-growing cyber threat. What happens is that a person makes unauthorized use of someone else's name and personal information – passwords, usernames, banking or financial data, etc. – to commit theft or other crimes. It often occurs through a data breach, virus or phishing scam.

Reading 5

Malware – Malware, short for "malicious software' is a term used to refer to software that is installed on a laptop, desktop computer or smart phone with a view to stealing passwords, deleting files or reformatting the hard disk of the device. Common examples of malware include viruses, worms, Trojan horse and spyware. Some of the ways in which malware spreads is if you open e-mails with harmful links or attachments, download infected mobile apps, or click on mystery links shared on social networking sites.

Table 2: Internet Threats

Online Activity 1: *Posting personal information (name of school, phone number of physical address) on media sites*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?
People other than friends and family could find out where I live and study.	It could lead to criminal acts such as theft or burglary at my house.	I will not post personal information on social media sites.

Online Activity 2*:* *Clicking on a link in your e-mail, or a Facebook post or smart phone message that announces a funny video of you.*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

***Online Activity 3**:* *Downloading songs and movies from popular file sharing sites*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 4: *Researching various web sites on environment protection for a school project or assignment*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 5: *Uploading revealing selfies on Twitter that you think make you look attractive*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 6: *Accepting friend requests from people you do not know*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Activity 5: Digital safety and security

Remember the earlier analogy between real life spaces and the virtual space of the digital world? Let's take the analogy a bit further. Because we, who live in the real world, are aware of the riskswe run by entering or inhabiting real-life places and spaces (houses, cars, etc.) we take special precautions to protect ourselves.

- ***For a car*** – steering wheel or gear locks, alarms, immobilizers, tracking devices, tinted windows, roadworthiness
- ***On the road*** – road signs, traffic rules, speed restrictions, defensive driving, not using a cell phone while driving, being alert to the possibility of other drivers doing something unexpected
- ***In the sea*** – not entering the ocean during high tide, not going too far in, swimming only in designated areas, presence of life guards, erection of shark nets

In order to move around safely in cyber space our digital 'vehicles' - smart phones and computers – also need to be protected - against cyber / digital thieves, burglars and other predators. Whether or not we choose the right protection depends on our knowledge of the risks/threats that digital travel poses to our electronic devices and the things we could do to protect them against digital 'attacks'. We should not, for example, expose our devices to places and spaces that are unsafe; we should be extremely careful about whom we allow into our space and/or to whom we give access to our devices; we should also conduct ourselves in ways that will not harm our reputation, threaten our safety or pose a risk to devices we use.

Let's looks at the potential dangers to and protection of the two devices most of us use for studying, working, socializing and entertainment, namely our smart phones and our computers.

(a) Securing your smart phone

Smart phones give users access to social networks, such as Facebook, as well as to games, videos and video chat sites, TV shows, music, applications *(apps)* and other content. They make it possible for users to take photos and videos that are fun, but also createopportunities for bullying, and the posting of suggestive photos or videos *(sexting). Geotagging of photos,* for instance, reveals precisely when and where the photo was taken, something that could be very dangerous because its GPS tracking system makes it possible for anyone who wants to do so to pinpoint the location of the phone. While this could be seen as a convenient and safe way for parents to keep track of their children's whereabouts it could also pose the risk of a child being tracked by potential kidnappers or other adult predators.

Be ***SMART*** – *STOP* and *THINK* about the risks ***before*** you *CONNECT*.

- **STOP** to consider the risks you they might face if you respond to a message, access a particular site, or post something on the Net.
- **THINK** about the impact that your actions might have on your own and others' safety.
- **CONNECT** only if the risks are minimal or non-existent.

SMART digital citizens (of all ages):

- ***Use Security Software*** to protect their phones against *malware* attacks. Most malware apps also come with anti-theft options. The McAfee Mobile Security app (https://www.mcafeemobilesecurity.com/), for example, is a reputed security app which protects the device, the data, and the person's privacy.

- ***Manage their phone settings***by exploring the settings and customizing them for location reporting, app installation, tracking online behaviour

and Wi-Fi networking. By selecting strict setting options they fend off undesirable access to their personal information.

- ***Avoid downloading apps*** that are not hosted at reputed stores. Downloading apps from untested sites may infect the phone with malware. When installing apps,they carefully review the terms and conditions of use to determine if they are giving someone access to information they might not want to share.

- ***Restrict access*** to their phones by locking these with PIN codes or Pattern Locks. This ensures that even if their phone is stolen, the thief cannot immediately access information on it. The owner of the phone could even use security software that 'wipes off' / deletes information on the phone, from a distance / by 'remote control'.

- ***Turn off public Wi-Fi*** – They do not use public Wi-Fi to shop or to access e-mails because these spots could give hackers easy access to their phones. Instead, they use their network provider connection as it is much more secure.

If all this sounds too complicated for you then just follow the McAfee's tips in the text box overleaf.

1. ***Set a pass code*** – which is known only to you - and configure it to automatically lock after a certain period of time.
2. ***Log out*** of your accounts (e-mail, Facebook, etc.) when you are not using them.
3. Do *not*, under any circumstances, keep *any**photos*** on your phone that you would not want others to see.
4. Read the ***user rating*** before downloading or installing apps and make sure that they are from trusted sources. If the ratings are negative, or if there aren't many ratings at all, it's a good indication that you should not install these apps.

McAfee's safety tips

(b) Securing your desktop / laptop computer

Table 3: Computer Risk Management

Obvious Risks	*Tips for safeguarding computers*
Malware infection	Ensure that the software on your computer is current. The best way to do this is to opt for automatic updating.
	Install only legitimate anti-virus & anti-spyware. These can be bought from a store or downloaded from a reputable website. Never turn off your firewall
	Use flash drives / memory sticks cautiously because they could carry viruses to your computer – *scan* them for those before opening.
Illegitimate access to a computer	• Create different, strong passwords for different sites and keep them secret. The more complex the password is the more difficult it is for someone else to decipher it. Do not use simple passwords like your name, telephone number, birth date, etc. Rather use a mix of letters, symbols, numbers and punctuation marks. • Create standard user accounts to decrease your vulnerability to hackers and maintain control of your personal computers (at home) *(aka.ms/user-accounts)*
Disabling a computer, invasion of privacy and harm to a user's reputation	▪ Be extremely discerning about the information you download or the links you create. Confirm the authenticity of the link with the sender and/or look for sites preceded by http(s) or with a padlock beside the address. ▪ Avoid pop-ups of any kind: they are dangerous. Press CTRL + F4 to remove them or, if that doesn't work, Alt + F4. • Never click *Agree*, *OK* or *I accept* in banner ads, pop-up windows, warnings or offers to remove spyware or viruses from your computer – they are meant to disable your computer.

C) Smart Questions and conversations

Remembering what you have just read, discuss and/or answer the questions that follow.

1. Is your smart phone safe? If so, what do you do to keep your smart phone safe? If not, what could you do in future to keep it safe?
2. Share, in a small group, some of the problems you have had with your computer, how this affected you, and what you did to 'fix the problem'.
3. Using our own and your group's knowledge and understanding of digital safety and security, as well as the information in the table below, design *Computer Safety Signs* (similar to road signs) that could be posted on the walls of your classroom or computer laboratory to help other alert other learners to the risks they might face in the world of computers.

Table 4: Troubleshooting

Problem	What to do
Scams, offensive material, content that aims to exploit or threaten you, or theft of your account,	Report it to your server (Look, for example, for *Report Abuse* in Microsoft services or software, or contact Microsoft at *www.microsoft.com/reportabuse*)
Someone takes over your e-mail account	Change your password immediately (if possible) and report the incident to your e-mail provider
Continued harassment or physical threats	Report these to the local police
Your identity is stolen or you have responded to a scam	Immediately change the password and PIN on all your accounts and report: • The incident to your credit card company, bank or health insurance company • The theft of your identity to the relevant government authority (Home Affairs, for instance) • Scams or fraud to the police or a legitimate, trustworthy crime investigation authority
Your computer isn't running as expected (it's unusually slow or crashes frequently)	It may have malware on it. Microsoft can help you addressthis. Log in to *(consumersecuritysupport.microsoft.com)*

Activity 6: Rather safe than sorry

Do you still remember the Internet threats you read about earlier? Well, the activities which follow focus specifically on risks associated with social media interaction.

A. Your teacher will read the text that follows with you, explaining words, concepts or ideas which you might not understand.

Social Media Mayhem

The use of social media sites and apps continues to increase, probably because it creates the opportunity for people to develop contacts, connect with friends, join groups based on common interests, share articles and personal information with others, and/or organize and host events. The problem is that these sites also create the opportunity for people to get rid of their frustrations by making racist, defamatory, abusive, provocative and inappropriate comments about other social media site 'visitors'. Apart from the psychological and/or emotional harm that such comments could have on those at whom they are aimed, they infringe the other person's rights to privacy and human dignity, primarily because they have the potential to damage the person's reputation.

There are three things you could do to protect these rights – *find out* what your on-line reputation is, '*fix*' / *correct* lies or misrepresentations in this regard, and take steps to *protect* it.

How does one do this?

- Use search engines to *scan* your reputation - in blogs and social networks - to find out how you are being represented.
- Do whatever is necessary to *fix*/correct it – the steps will be different depending on the type of site concerned. In certain

instance the only way in which you could fix it would be to take legal steps against those who misrepresented you in the first place.

- In order to *protect* your reputation in future, Microsoft[1] advises that you should:
  i. Make sure that your personal profile does not include any contact details or personal information.
  ii. Don't ever post anything that could put your privacy or reputation at risk.
  iii. Do everything possible to ensure that you connect only with people whom you know personally.
  iv. Listen to and trust your instincts – if something feels uncomfortable or alarms you regard that as a warning and do something to stop it.
  v. Immediately report physical threats, intimidation or attempts at exploitation to the police and the carrier. Also block the caller.
  vi. Share your phone number only with those you know and trust. Do not put it on social pages or use it to enter content.
  vii. Do not make, send or accept provocative texts, photos or videos because, once they are shared they can be forwarded to anyone, even years into the future, thereby posing a risk to your reputation for ever.

[1] Microsoft, 2014: *Teach Kids Mobile Safety*

B. Bearing in mind what you have read in the text, you might like to share some of the unpleasant experiences you, or someone you know, have had on social media.

C. To demonstrate your understanding of the issues discussed, you and our group must now design a poster which reflects (in the form of cartoons, collages, drawings, etc.) the negative impact that social media could have on a person's reputation. Once your poster is finished, please display it on the classroom wall as a reminder to other of the effect that a bad online reputation could have on a person's real life reputation.

Activity 7: Risk Management

Risk management is a term commonly used in government offices and the business sector and entails anticipating problems, and working out plans to prevent or manage these.

In this activity we would like you to pretend that you are on-line risk managers. What you have to do is to study the scenarios described in Column 1 of Table 5, write down in Column 2 the risk associated with the action/s described in the scenario, and then match the technique in column 3 with the risk it is most likely to prevent.

Table 5: Risk management scenarios

Scenario	*Name of risk*	*Prevention technique*
Farouk created a web site, posted mean comments on it and uploaded embarrassing pictures of Anant after they had a big fight. The web site invites other learners to state why they do not like Anant.		Ignore any intimidating or supposedly official messages that direct you to a link that require the updating of personal information.
Tina was in a chat room yesterday when a male user who had been friendly with her for some time asked her if she liked older men. He also expressed an interest in seeing her photograph.		Keep screenshots of content posted as evidence of harassment and report the incident to a parent or person of authority. Register an official complaint
Nozipho is a registered member of an online tutoring web site. She recently received an e-mail with a link that required her to update all her personal information on their web site within a week. Should she not comply she would be blocked from the site permanently.		Create a routine that limits the time you spend on your computer to a reasonable number of hours. Do not keep your laptop or desktop computer in your room.
Thabo plays *Conquer All* on his computer every night. Most of the time he continues with the game till 4 in the morning. At 6:30 he has to get up if he wants to catch the school bus. His teachers have noticed that he is always sleepy in class.		Block the user who is making you feel uncomfortable with his/her comments and/or requests for personal information

Once everybody has completed the table your facilitator will show you the responses that could be regarded as the most appropriate ones.Adjust your answers to accommodate these responsesif you agree with it OR, if you think your response is better, discuss this with your facilitator and the group during the debriefing session.

Activity 8: Digital / Cyber Legislation

Did you know that most countries have laws aimed at the protection of digital citizens, and that people who break these laws could be prosecuted? The table that follows gives you some idea of what would happen to digital / cyber criminals in India. Study the table and decide, in your group, whether or not you think the punishment of these criminals as set out in the table is fair or not. Give reasons for your answers.

Table 6: Cyber crime and its legal consequences in India

Cyber crime	Description	Punishments
Cyber stalking	Stealthily following a person, tracking internet chats	3 years and/or fine up to 2 takh
Cyber pornography *(including child pornography)*	Publishing obscene content in electronic form	10 years and/or fine up to 10 takh
Intellectual property crimes	Source code tampering, piracy, copyright infringement, etc.	3 years and/or fine up to 2 takh
Cyber terrorism	Acts of terror electronically propagated	Imprisonment of up to 7 years
Cyber hacking/cracking	Destruction, deletion, alteration, etc of computer resources	3 years and/or fine up to 2 takh
Phishing	Net banking and financial fraud	3 years and/or fine up to 2 takh
Invading privacy	Unauthorized access to a computer	2 years and/or 1 takh

Derived and somewhat adapted from Intel Education Digital Wellness Curriculum, 2014.

In South Africa the following laws are all aimed at protecting the safety and rights of Internet users. If you are a South African, you could ask your teacher to tell you what these laws say and how digital/cyber criminals will be punished if they break any of these laws.

- The *Protection of Information Bill*
- The *Act on Electronic Communication and Transactions,* and
- The Act on the *Regulation of Interception of Communication and Provision of Communication-related Information (RICA) (Act 70 of 2002)*
- The *Protection of Harassment Act (2013)*

The ***Protection of Harassment Act,***which is summarized in the text box below, is particularly important because it defines*harassment*, is meant to protect people, especially children, against cyber bullying, and provides victims of cyber bullying with an inexpensive civil recourse to most forms of harassment, also e-harassment.

If you are not a South African, ask your teacher to tell you about any laws in your country that are aimed at the protection of Internet users. Ask him/her to also tell you what happens to people who transgress these laws.

According to the ***Protection of Harassment Act (2013),*** any of the following actions constitute harassment:

- Threatening sms messages/remarks, or private Twitter messages, or e-mails to individuals
- Sending or sharing e-mails with offensive content (pornographic images, sexual preferences, race, etc.)
- Sharing of offensive, abusive or embarrassing media or content that has been manipulated to this effect
- Sexual advances made through any message or posting

According to the same Act:

- A person or persons to whom these messages are sent should immediately apply for a protection order from a clerk of court.
- The clerk of court will then issue a restriction order to the person responsible for the harassment.
- If this person (the sender) contravenes/ignores the order s/he would be guilty of an offence and would be liable to a fine or a maximum of 5 years imprisonment.

Using the knowledge and insights you gained from your readings, the activities you have done so far and the discussions you have had with your teacher and other learners, read the imaginary scenarios of children like you who have been harassed on social media sites. Then answer, in writing, the questions that follow each scenario.

You can decide whether you want to work on your own, with a partner or in a group in doing this activity.

Scenario 1

Susan, a Grade 8 learner at a primary school, regularly receives cruel e-mails and instant messages from a couple of other kids at school. Usually a confident, outgoing child, Susan is now scared to go to school because she is afraid that these kids are going to tease or bully her about her appearance and personality. She doesn't know what to do about the situation so she often bunks school without her parents' knowledge.

1. *What would you advise her to do?*

_____

_____

_____

_____

2. *Is there anything her parents or teachers could do to help her become her old self again? What advice would you give them in this regard?*

_____

_____

_____

_____

3. *What could Susan do to avoid being cyber-bullied by other users in future?*

_____

_____

_____

_____

Scenario 2

Fiona, a Grade 12 learner at a posh private school has recently opened a Skype account. Her best friend, Annemarie, who attends a public school, doesn't have one but would like to connect with Fiona on Skype. She asks Fiona for her username and password.

1. *Should Fiona give it to her or not? Give reasons for your answer.*

_____

_____

_____

_____

2. *Do you think it was responsible of Fiona's parents to allow her to open her own Skype account? Give reasons for your answer.*

_____

_____

_____

_____

3. *Why would the two girls want to connect via Skype? Could they not rather use another social media network? Give reasons for your answer.*

_____

_____

_____

_____

Scenario 3

Thomas Ogina is a bright secondary school learner. Although not an outstanding sportsman, he took part in school sport because many of his friends were keen sportsmen. One day one of these friends introduced him to online gaming. Thomas mastered the skills required for this kind of gaming in no time at all. Very soon he started to win many of his role-playing bouts. After a while he became so emotionally attached to his gaming avatar and to his ever increasing scores that he spent longer and longer hours hooked to the screen.

After a while he started joining online gaming groups. Their admiration when he told them about his high scores made him feel very clever and special. As time went on he spent more and more time with his online friends in the forum than with his old school friends. It went so far that he stopped hanging out with his school friends and even refused to take phone calls from them.

Then things started going wrong. Thomas had an argument with some long-time forum members. To "put him in his place" they started ganging up on him, sending him threats and harassing messages.

Although he was very upset about what was happening, Thomas did not want to tell his parents. He was afraid that they would restrict his use of the Internet. Instead, he confided in Peter, one of the forum members who

seemed particularly sympathetic to his situation. Peter suggested a private telephone conversation or meeting Thomas Peter so that they could work out a solution. Because Thomas now feels very alone – Peter being the only "friend" he has left – he is tempted to do as Peter asks but something somewhere in his says that this would be a mistake. Now he does not know what to do: should he listen to Peter or to his gut feeling?

1. Which of the rules in the ***Prohibitions List*** did Thomas ignore?

_____

_____

_____

_____

_____

2. Which signs were there that his gaming was having a negative effect on his personality?

_____

_____

_____

_____

_____

3. Why, do you think, was he especially vulnerable to this particular threat?

_____

_____

_____

_____

4. What, according to you, should he have done the moment his online friends started threatening and harassing him? Why do you say so?

_____

_____

_____

_____

_____

5. What would you advise him to do now? Should he take up Peter's offer, should he tell his parents, or are there other options? Give reasons for your answer.

_____

_____

_____

_____

_____

Activity 9: Information ethics

You would have noticed that all the texts you have read and all the activities you have done up to now focused on ways in which you could protect oneself against *cyber risks created by other internet users.* In the sections that follow the focus shifts to *you* as a user – what *you* could, and should, do to ensure that you do not in some way harm other users of the Internet.

What we would like you to do is read the fable about the Frog and Scorpion which follows. Your group can decide whether you want each one to read it silently, whether you want to take runs reading parts of it, or whether you want someone in your group to read all of it our loud.

Once you have read the fable, talk about the questions following it. There are no right or wrong answers to these questions. Therefore you do not have to write the answers down. Just talk about them, trying to reach some consensus about possible answers.

The Frog and the Scorpion

One summer afternoon there was a heavy storm over the Bushveld. The first sign was the deep rumbling of thunder. Very soon there were flashes of lightning all over. And then, so suddenly that there was no time to hide, the rain came down – not in tiny drops, but in streams, as if the dam walls of heaven had literally burst.

As small streams began to gather everywhere, a female scorpion found herself stranded on a rock. As she saw the water rising she realized that she might drown in the raging waters she started panicking.

At that moment a frog swam past, exhilarated that the long drought had eventually broken.

“Mr Frog,” the scorpion shouted, “would you be so kind as to allow me on your back and take me to higher ground. I am afraid that I might drown in the flood. You know, we scorpions cannot swim.’

The frog paused a moment and looked at the frightened scorpion on the rock. Then he shook his head. “No can do. You know scorpions have a lethal sting. If you were to sting me as we cross the stream, I would surely die.”

“Hey listen, Mr Frog. Why would I do that? You can see that I’m scared stiff of the flood. I know that it would mean the end of both of us if I were to sting you.”

The frog thought for a moment. What the scorpion said made perfect sense. He looked at the water rising and at the scorpion clinging to the rock. Hesitantly he moved closer and allowed the scorpion to get on his back.

Slowly he swam across the stream to safer ground. When they were about halfway he suddenly felt the scorpion stinging him in his back.

“Now why did you do that, Scorpion? Can’t you see that I will now die and both of us will drown in the water?”

“Well,” replied the scorpion, shrugging her shoulders, “that is what scorpions do”.

Nieuwenhuizen, 2007

What does the fact that the frog picked up the scorpion tell us about his *character*?

_____

_____

_____

_____

_____

1. Do you think the frog trusted the scorpion? Give reasons for your answer.

_____

_____

_____

_____

_____

2. Do you think that he would trust a scorpion again if he were to survive this experience? Give reasons for your answer.

_____

_____

_____

_____

_____

3. Have you ever had a 'frog experience", i.e. an incident when someone betrayed your trust or metaphorically stabbed you in the back? Without mentioning names, tell us about it and how it made you feel?

_____

_____

_____

_____

_____

4. What does the fact that the scorpion broke her word tell us about *her* character?

_____

_____

_____

_____

_____

5. Have you ever behaved like the scorpion? When? Why? How did it make you feel?

_____

_____

_____

_____

_____

6. What does she mean when she says, “That’s what scorpions do”? Do you think this is a valid reason for doing harm to someone else? Give reasons for your answer.

_____

_____

_____

_____

7. Have you ever said something like that? For example, “In my culture we ……..”

_____

_____

_____

_____

8. If you have, what are you suggesting about values – that people have the right to live in accordance with their particular values even if it harms people with different values?

_____

_____

_____

_____

_____

9. How do African value systems differ from value systems in the rest of the world, if at all?

_____

_____

_____

_____

10. Is it true that the presence and use of information communications technology has had an impact on traditional values? If so, is the impact positive or negative? Give reasons for your answer

_____

_____

_____

_____

11. Do you think that the scorpion would not have stung the frog if there was a law against scorpions stinging frogs? Give reasons for your answer.

_____

_____

_____

_____

12. Do you think that fear – of punishment, for example – is enough to make people behave? What if the laws or the concomitant punishment are unjust?

_____

_____

_____

_____

_____

13. What would happen if there were no laws and/or if there were laws but no punishment? Would this freedom of punishment be seen as a license to do injustices to others or are there other ways of creating a harmonious society?

_____

_____

_____

_____

_____

Activity 10: Information ethics dilemmas

Not all people live according to the same value system. Because of this a person whose personal values are different from the values of a group or society to which s/he belongs might often find her/himself in a situation where s/he has to decide whether to behave in accordance with her/his own value or those of the group concerned. When this happens we say the person finds her/himself in a moral dilemma, or a Catch 22 situation.

The dilemmas described below are all about the value systems informing the creation and sharing of information. As is the case with other moral dilemmas, the choice the person makes will have consequences for her/himself but also for the other people involved in the situation described.

In this activity our focus is on information ethics dilemmas, that is, on Catch 22 situations, in which someone has to decide what to do with the information with which she or he has been confronted.

To see for yourself how difficult it is to make ethical decisions like these, read the texts that follow. Each text describes a different dilemma.

Once you have read the text, answer the questions that follow the text in writing, following the procedures described below.

Procedure for reflection on information ethics dilemmas

1. Quietly read the moral dilemma scenario and then, without discussing it with anyone, write down your answer to each question, ***except the last one***, in the space provided.
2. Once everybody has answered the questions in writing, group members should share and discuss their answers with one another.

3. If group members' answers reflect different value positions those who agree should try and persuade the 'other side' to accept their point of view as the most appropriate one.
4. Once the group reaches consensus about the most appropriate response the rapporteur should write down this answer.
5. If the group cannot reach consensus the rapporteur must indicate this, giving reasons for the stalemate.
6. Once all the questions and responses have been dealt with, answer the last question in writing.

Information ethics dilemma 1

Farouk, a Grade 12 learner at a private school, receives an e-mail with a subject line that reads,

> *"You have just won R10,000. All you need to do is to open the e-mail, click on the link provided and enter the personal information requested."*

Knowing that his parents have made and are still making major sacrifices to keep him in this school because they want him to have a better future, he is very tempted to respond to the e-mail but is frightened that it is a hoax.

Questions

1. *What is the dilemma? In other words between what and what does Farouk have to choose?*

_____

_____

_____

_____

2. *What makes the dilemma a 'moral'/ 'ethical' one? (In other words, between which **values** does he have to choose?)*

_____

_____

_____

_____

_____

3. *What do you think the consequences would be if Farouk decided to open the e-mail?*

_____

_____

_____

_____

_____

4. *What do you think the consequences would be if he decided not to open it?*

_____

_____

_____

_____

_____

5. *What would you have done if you were in his shoes and why?*

_____

_____

_____

_____

_____

6. *Did the group discussion change your perception of what Farouk should or could have done? If so, what changes would you like to make to your original answer. If not, what is it that makes you stick to your original answer?*

_____

_____

_____

_____

_____

Information ethics dilemma 2

Sipho is a Grade 9 learner in a public school. The school encourages learners to use the Internet when doing research for assignments and to communicate with each other about personal and learning matters. One of Sipho's friends sent him a message with a link to a website where one can post anonymous comments on and pictures of one's classmates. Almost all of the postings and pictures already displayed on the site are either mean of embarrassing. Sipho's friend wants him to help start a rumour about another classmate whom the friend does not like.

Questions

1. *What is the dilemma? In other words between what and what does Sipho have to choose?*

   _____

   _____

   _____

   _____

   _____

2. *What makes the dilemma a 'moral' one? (In other words, between which **values** does he have to choose?)*

   _____

   _____

   _____

   _____

   _____

3. *What do you think the consequences would be if Sipho does what his friend asks?*

   _____

   _____

   _____

   _____

   _____

4. *What do you think the consequences would be if he decided to refuse his friend's offer?*

_____

_____

_____

_____

_____

5. *What would you have done if you were in his shoes and why?*

_____

_____

_____

_____

_____

6. *Did the group discussion change your perception of what Sipho should or could have done? If so, what changes would you like to make to your original answer. If not, what is it that makes you stick to your original answer?*

_____

_____

_____

_____

_____

Information ethics dilemma 3

Dick and Tracy have been friends for a long time and regularly communicate with each other on Twitter and Facebook. They recently discovered a file-sharing web-site that allows them to share music and games with their other friends. The site would enable them to download the latest music and coolest games for free. Another friend of theirs, Alexander, who is very fond of movies, has also sent them a message with a link to a website where they can download free movies that have not yet been released on video.

Since neither of them receives a great deal of pocket money they are very tempted to download all their freebies. Both of them are quite religious, though, and are not sure whether the Church they belong to would regard this as stealing. Could you help them make a decision?

Moral dilemma questions

1. *What is the dilemma? In other words, between what and what do Dick and Tracy have to choose?*

   _____

   _____

   _____

   _____

   _____

2. *What makes the dilemma a 'moral' one? (In other words, between which **values** do they have to choose?)*

_____

_____

_____

_____

_____

3. *What do you think the consequences would be if Dick and Tracy decided to download the freebies?*

_____

_____

_____

_____

_____

4. *What do you think the consequences would be if decided against downloading the freebies?*

_____

_____

_____

_____

_____

5. *What would you have done if you were in their shoes and why?*

_____

_____

_____

_____

_____

6. *Did the group discussion change your perception of what Dick and Tracey should or could have done? If so, what changes would you like to make to your original answer. If not, what is it that makes you stick to your original answer?*

_____

_____

_____

_____

_____

Activity 11: Creative Assessment Task

You have now come to the end of the Digital Wellness and Information Ethics course. To determine how well you have understood the issues discussed and to see how creative you are, we would like you – as an individual, a pair, or a group, to do ***one*** of the following activities.

1. Write an ***article*** for a newspaper in which you (a) warn people against the dangers lurking in cyber space or (b) motivate people to behave ethically in their interactions with others in digital space.

2. Compose a ***song*** in which you (a) teach people how to protect themselves or their devices against digital threats, or (b) teach them Netiquette.

3. Create a ***collage*** or ***painting*** which illustrates either unsafe/unethical or safe/ethical digital behaviour.

4. Design a ***board game*** (something like *Monopoly* or *Trivial Pursuit*) in Digital Wellness or Netiquette.

The choice of activity is yours and yours only but your teacher will give you a mark for it and, if your teacher is blown away by your insight and creativity, s/he might even give you a prize.

Good luck! We hope you enjoyed this course and that your final product is going to be AMAZING!

BIBLIOGRAPHY

Balkin, J. (2004). *Digital speech and Democratic culture: A theory of freedom of expression for the Information Society, Paper 240.* Retrieved March 23, 2013, from Faculty Scholarship Series: http://www.yale.edu/lawweb/jbalkin/telecom/digitalspeechanddemocraticculture.pdf

Blackburn, S. (2005). *Oxford Dictionary of Philosophy* (2nd ed.). Oxford: Oxford University Press.

Intel Corporation, 2014. Intel Education Digital Wellness Curriculum

Le Sueur C, Bothma T, & Bester C 2013. Conceptsin Information Ethics.An Introductory Workbook.

Pretoria. Ithuthuko Investment Publishing

Microsoft, 2014: Digital Citizenship starts with you. www.stopthinkconnect.org

Microsoft, 2014: Teach kids online security basics. www.safety&securitycenter

Microsoft, 2014: Help Kids Stand Up to Online Bullying. www.lookbothways.com

Nieuwenhuize. J. (2007). Values and Human Right in Education. Pretoria. Van Schaik Publishers.

Scott, J., & Marshall, G. (2005). *Oxford Dictionary of Sociology.* Oxford: Oxford University Press.

Singer, P. (1991). *A Companion to ethics.* Oxford: Blackwell Publishing.

Turilli, M., Vaccaro, A., & Taddeo, M. (2012). The case of online trust. *Knowledge, Technology & Policy, 23*, 333-345.

Velasquez, M. (1998). *Business ethics, concepts and cases* (4th ed.). New Jersey: Prentice Hall.

Digital Wellness Programme

Intel Education and ACEIE collaborated to provide critical cyber wellness content to all citizens (students) of Africa to prepare them on the basics of safe and ethical online presence for today's digitally immersed world.

The Intel® Education Digital Wellness Programme is a free initiative that utilizes resources from Intel Security as well as Intel Education to train Communities, Parents, Educators and school aged children on ways to stay safe and secure and maintain good ethics in their online behavior.

Localization was done by ACEIE based at the University of Pretoria in consultation with the Departments of Post and Telecommunication services and Basic Education, as well as the Information for All Programme of the UNESCO office.

For more information with regards to Cybersafety, please review:
www.mcafee.com/onlinesafety

www.up.ac.za/aceie

9 781928 261698

United Nations Educational, Scientific and Cultural Organization

Information for All Programme
National IFAP Committee for South Africa

telecommunications & postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie

basic education
Department:
Basic Education
REPUBLIC OF SOUTH AFRICA

intel Education

African Centre of Excellence for Information Ethics