Digital Wellness Programme

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

ACTIVITY BOOK FOR WORKSHOP PARTICIPANTS

Digital Wellness Programme

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

ACTIVITY BOOK FOR WORKSHOP PARTICIPANTS

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 WORKSHOP PARTICIPANTS

October 2015

ISBN: 978-1-928261-67-4

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 CONTENTS

INTRODUCTION AND ORIENTATION

Welcome to this workshop on *Cyber Safety* and *information Ethics*. Competence in the use of information communications technology (ICT) is not only critical to the development of a literate African information society but also to the continent's global competitiveness. The rapid development of and increased access to information communications technologies have many advantages: immediate and uninterrupted access to information, communication with people all over the world, opportunities to buy and sell articles from the comfort of one's home, and many more.

The use of these technologies is not without problems, though. Unless users are aware of the opportunities as well as the risks entailed in using information communications technologies (ICTs), and know how to protect themselves and their devices against cyber threats, their own safety and the safety of their devices could be in danger. They could literally be 'attacked" by viruses, hackers, cyber bullies and a range of predators whose sole purpose is to harm them. In addition, unless "cyber citizens" know how to conduct themselves in this virtual, cyber world, they might inadvertently undermine the values and/or transgress the laws that are meant to regulate cyber interaction.

A critical aspect of e-literacy development is the introduction of a digital wellness component in schools. This can only happen if educators and learners are trained in the responsible use of information and information communications technology.

The workshop on *Cyber Safety and Information Ethics* is aimed at sensitizing educators and other interested parties to some of the dangers they could face in cyber space and to provide them with the knowledge and skills to protect themselves and others against cyber dangers / threats. More specifically, the workshop is aimed at providing those who attend it

with a basis/platform from which they can take steps to safeguard themselves and others against the dangers of the Internet.

In order to achieve these aims the workshop focuses on ***five themes*** – *Digital Citizenship, Cyber Security, Cyber Safety, Cyber Crime,* and *Information Ethics (see Figure 1)*

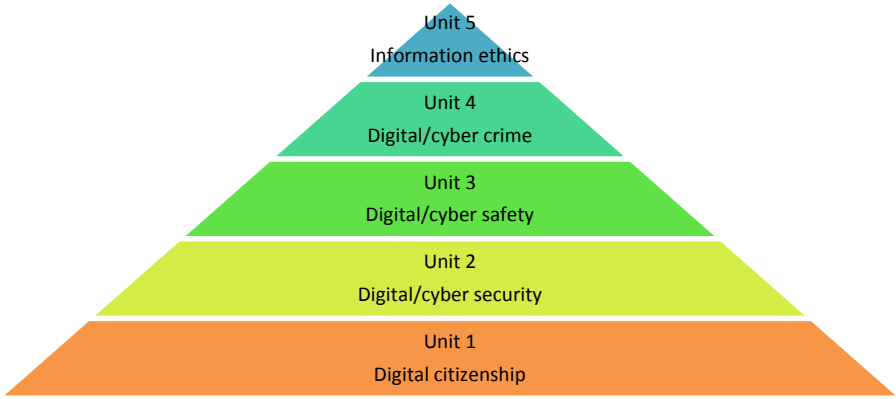

Figure 1: Workshop structure

The themes are covered in different units, each comprising one or more sessions focusing on specific aspects of the theme being covered.

- Each session starts with a ***plenary discussion*** where the facilitator introduces participants to the theme concerned and gives them the opportunity to ask clarification questions and/or comment on issues raised during the plenary discussion.
- The plenary session is typically followed by one or more ***group activities*** in which participants are given the opportunity of applying the knowledge and insights they gained during the plenary session to actual situations.
- Each group activity is followed by a plenary ***debriefing*** session in which participants give feedback on their group activity.

- The session ***ends*** with the facilitator pulling all the loose ends together and introducing participants to the issues that will be discussed in the next session.

In order for you to get the greatest benefit from the workshop we ask you to participate actively in all the activities, to openly share your knowledge and experience with your facilitator and fellow participants, and to ask when there is something you do not understand. We trust that, if you do this, you will not only find the workshop informative but will also enjoy and benefit from the experience as a whole.

Prof Theo Bothma
Department of Information Science
University of Pretoria
October 2015

Activity 1: Ice-breaker

For this activity your facilitator will divide you into two groups. Each group will receive two envelopes, one containing strips of paper with terms that are commonly used in the world of information communications technology and the other containing the definitions of these terms.

Your job as a group is to ***match*** each term with its definition as quickly as you can.

Use your own knowledge as well as your *Concept Book* for this activity.

When both groups have completed the activity your facilitator will show you the correct answers and give you an opportunity to comment and ask further questions should you wish to do so.

The space below could be used for the making of comments or notes on the activity, the recording of questions you might want to ask now or later, and/or the knowledge gained in the discussion that follows the activity.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

UNIT 1: DIGITAL CITIZENSHIP

Introduction

Cyber space, like any other actual/ real space - a road, a house, the ocean, et cetera - poses a number of threats to the people moving around in it. Accidents could happen when one is walking or driving on a road; one's house could burn down, be flooded or burgled; one could drown or be attacked by sharks while swimming in the ocean.

Because we are aware of these risks, we take special precautions to protect ourselves: we follow the rules of the road, drive defensively, and avoid using our cell phones while driving; we install burglar bars or gear locks and alarms in our cars and houses to protect us against thieves and murderers; we do not build our houses too close to the ocean so as to avoid flood risks; we do not swim in the ocean when the water is rough, and we avoid areas identified as shark-infested.

The same holds true for our cyber activities: that is, when we are aware of the risks associated with cyber navigation we can take the necessary precautions to safeguard ourselves and the information communications devices we use against **hackers, phishers, viruses, cyber bullies, sexual predators, and those who want to steal our identity or intellectual property.** We could for eg. protect our own cyber profile by not posting anything on the Internet that could ruin our reputation, open us up to legal action, or make us ill.

In the world of letters and books a literate person is one who can read and write with understanding. In the ICT world a person's literacy level is determined by the extent to which s/he is able to access information from cyber space, process it to serve multiple purposes, and disseminate to others by means of ICT devices. Unfortunately not all of us are at the same level as far as this is concerned. One of the reasons for this difference

could be that the kind of information with which we work and the purposes for which we use ICTs on a daily basis are not the same. Another reason – said tongue in cheek – is that we are not all fortunate enough to have parented cyber whizz kids who seem to have been born with a complete set of cyber savvy genes!!!

If we are to reap the greatest benefit from being a citizen of the digital world we have to accept the responsibilities of citizenship. First of all, we should make sure that we know and understand ICT jargon *(that is, the language people use when they talk about information and information communications technology).* Second, we should make sure that we know which risks are associated with the use of ICT. Third, we should know what we can do to minimize these risks. Last, we should take the necessary steps to protect ourselves and our ICT devices against these risks.

If you are to receive the maximum benefit from this workshop, that is, if the workshop is to help you move to a new level of cyber literacy, your facilitator needs to know what the average cyber literacy level of the group is so that s/he can adapt activities to these levels. Activity 2 is aimed at helping your facilitator do this, with your help, of course.

Activity 2: Cyber Savvy Research

For this activity you must pretend to be a *researcher*. Your job is to help the facilitator find out what your group already knows about cyber safety and information ethics. In order to do so, each of you has to interview ***one person*** in the room whom you do ***not*** know and/or with whom you would **not** normally associate, and then allow that person to interview you in turn.

The purpose of the interview is ***not*** to assess how cyber savvy individual participants are. Its purpose is simply to determine the cyber savvy level of ***the group*** as a whole. Do ***not***, therefore, write the name of the person you interview on your questionnaire.

Please follow the interview protocol below rigorously to ensure that the information /data you collect is valid, ethical, and objective.

Interview Protocol

1. *Ask only the questions appearing in the questionnaire when conducting your interview. Do not add any questions of your own.*
2. *Stay neutral. Do **not** comment on the answers given by the person being interviewed and do **not** give any indication of what **you** would have answered. Simply ask the questions and record the answer in the appropriate column.*
3. *Starting with Question 1, first ask the person being interviewed the part of the question that requires a simple **Yes** or **No** answer, and record his/her answer in Column 2.*
4. *When you have recorded this answer, ask him/her the applicable second part of the question. Jot down, in Column 3, the essence of the person's answer – i.e. key words only - that will help you remember what he/she said.*
5. *When you have completed the interview, allow your partner to interview you. Do not let the answers your partner gave influence your answer.*
6. *Do not write anything in the open spaces following the data analysis and interpretation questions. You will have the opportunity to do so at different stages of the workshop.*

CYBER SAVVY QUESTIONNAIRE

	Questions	Yes / No	Reason / Explanation
1.	Do you have a personal computer and/or mobile phone? If not, why not?		
2.	Is access to your computer or mobile phone protected by a password or pin number? If not, why not? If yes, indicate whether you use a password or pin number.		
3.	If you have a computer, have you installed a dependable anti-virus program on it? If not, why not? If yes, is your firewall always turned on or only sometimes?		
4.	Do you use these devices for Internet surfing? If yes, to what purpose? If no, why not?		
5.	If you have a mobile phone, does it have a GPS tracking device? If so, when do you turn it on?		
6.	Do you know how to distinguish between a legitimate/safe and illegitimate/unsafe web-site? If yes, indicate how you do this.		
7.	Have you on occasion clicked *Agree, OK* or *I accept* in banner advertisements, pop-up windows of warnings on web-sites? If yes, why? If no, why not?		
8.	Have you ever downloaded applications, music, games or videos from web-sites? If no, why not? If yes, indicate which.		
9.	Have you ever used a search engine to check your on-line reputation? If no, why not? If yes, were you happy or unhappy with what you found? Why?		

10.	Do you use *Facebook, Twitter,* or *Whats App, etc.* to communicate socially with others? Why/why not?		
11.	Do you use free Wi-Fi in places like shopping malls, etc. Why/why not?		
12.	Have you or someone you know ever been harassed, intimidated or victimized on a social media network? If yes, briefly indicate what happened.		
13.	Do you use a flash drive / memory stick to store or transfer information? Why/why not?		
14.	Which of the following best describes you as a user of information communications technology - a *technophobe*, a *tech addict*, or a *tech user*? Give a reason for your answer.		

Data analysis and interpretation

1. How savvy do you think the person you interviewed is about protecting his/her ICT devices against cyber risks if you compare his/her responses with those of the target group as a whole? Give a reason for your answer.

_____

_____

_____

_____

_____

2. What advice would you give your interviewee regarding ways of protecting his/her ICT devices, him/herself against cyber threats?

_____

_____

_____

_____

_____

3. How savvy do you think the person is about his/her own safety in cyber space compared to the target group as a whole? Give a reason for your answer.

_____

_____

_____

_____

_____

4. What advice would you give your interviewee regarding ways of protecting him/herself against ICT users who threaten his/her safety?

_____

_____

_____

_____

_____

5. How savvy do you think the person is about information ethics if you compare his/her responses to the responses of the the target group as a whole? Give a reason for your answer.

_____

_____

_____

_____

_____

6. What advice would you give your interviewee about his/her Netiquette? Give reasons for your answer.

_____

_____

_____

_____

_____

UNIT 2: DIGITAL/CYBER SECURITY

Introduction

Most road accidents are caused by drivers who either don't follow the rules of the road or travel in vehicles that are not roadworthy. Being alert to such behaviour might convince you to drive defensively, in the hope that this will keep you safe. The same can be said of cyber safety. Unless the devices you use on the 'cyber highway' are safe and unless those on this 'highway' behave responsibly, chances are that cyber 'accidents' will escalate.

The days when computers were used for work purposes only have long since passed. Nowadays they are used to share all kinds of information - general as well as personal – in the form of texts, photos, pictures, music, etc. While this is very convenient, it is not necessarily one hundred percent safe to do so. People who are not aware of what the risks are and of how they can circumvent these run the risk of exposing themselves to cyber predators and/or of harming their own on-line reputation due to the manner in which they interact with others in virtual cyber space.

Without the proper tools it would be impossible for so-called cyber citizens to socialize with others and/or to access and download information from the Internet. It is important, therefore, also to keep these devices safe from cyber threats. Microsoft[1] suggests that the best way to do this is to:

- Ensure that the software on your device is not outdated
- Install only legitimate anti-virus and anti-spyware programmes
- Never turn off the firewall on your device
- Use secret pin numbers or strong passwords to restrict access to your device

[1] Microsoft, 2014: *Digital Citizenship starts with you.*

- Be extremely discerning about the information you download or the links you create
- Never click *Agree*, *OK* or *I accept* in banner ads, pop-up windows, warnings or offers to remove spyware or viruses from your computer
- To use flash drives cautiously to avoid malware infection

Activity 3: Risk Management

Now that you are familiar with some of the most common terms used by the ICT community and have a sense of your own and the group's level of savvy literacy it is time to talk about the risks associated with the use of the Internet and what you could do to protect your devices against these risks.

For this activity your facilitator will divide you into 2 groups and allocate one of the tables that follow to each group.

In your group, read the tips that McAfee and Microsoft give for protecting the device which is the focus of your group's activity.

Remember to use your *Concept Book* if there are any terms that you do not understand.

Now study the table allocated to your group. It consists of ***4*** columns:

- Column 1 names the ***risks*** that you or your device are exposed to in cyber space
- Column 2 tells you ***what*** you could do to keep yourself or your ICT device safe
- Column 3 contains questions on ***how*** you should go about carrying out the recommendations made in Column 2.
- Column 4 is empty.

Your task, as a group is to discuss the questions posed in Column 3 with a view to reaching consensus on what the correct answer is.

Use your own experiences in this regard and/or the safety tips preceding the table to help you complete the columns concerned.

Once you have reached consensus on the answer to a particular question each member of the group should write the answer next to the question, using Column 4.

When both groups have completed the task your facilitator will run you through possible answers and give you the opportunity of adding these to your tables if this is necessary.

McAfee[2] advises those with mobile phones to:

i. Set a pass code and configure it to automatically lock after a certain period of time. Keep this pass code secret.
ii. Log out of your accounts like e-mail and Facebook when not in use
iii. Read the user rating before downloading or installing apps. If the ratings are minimal or negative you should not install it.

[2] McAfee, cited by INTEL 2014:2.12

Table 1: Mobile Protection[3]

Risk	***Risk management***	***Risk management questions***	***Risk management answers***
Malware infection and attacks	Install reputable security software as protection	*How do I do this?*	
	Avoid downloading apps from untested sites.	*How would you know whether or not an app store is reputable?*	
Undesirable access to your private or personal information	Explore and customize settings on your phone.	*How would you do this?*	
	Lock your phone with a pin code or pattern lock.	*Why should one do this?*	
Access to your phone	Do not use public Wi-Fi to shop or access e-mails. Rather use your network provider connection.	*Why not?*	

Microsoft provides advice on what you could do if you run into the following problems:

i. If you encounter 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*).

[3] Information in this table is derived from the 2014 INTEL *Education Wellness Curriculum*, Version 2.0, pp 2.11/2

ii. If someone takes over your e-mail account, change your password immediately (if possible) and report the incident to your e-mail provider.

iii. If you experience continued harassment or physical threats report them to the local police.

iv. If 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.

v. Create standard user accounts to decrease your vulnerability to hackers and maintain control of your personal computers (at home) *(aka.ms/user-accounts)*

vi. If your computer isn't running as expected (it's unusually slow or crashes frequently) it may have malware. Microsoft can help you address this *(consumersecuritysupport.microsoft.com)*

vii. Find more information on how to protect yourself, your learners and your family (on *microsoft.com/security*)

Table 2: Computer Protection[4]

Risk	***Risk management***	***Risk management questions***	***Risk management answers***
Malware infection	Ensure that the software on your computer is current	How do I do this?	
	Install legitimate anti-virus & anti-spyware programmes & never turn off your firewall	Where do I get these?	
	Use flash drives / memory sticks cautiously	Why?	
Restricting access to your computer	Create different, strong passwords for different sites and keep them secret.	What does a strong password look like?	
Harm to your computer, your privacy and your reputation	Be extremely discerning about the information you download or the links you create	How do I know what to avoid or choose?	

[4] Microsoft, 2014: Digital Citizenship starts with you.

UNIT 3: DIGITAL/CYBER SAFETY

Introduction

Everyday more and more people communicate with each other by means of social media, whether this be on their mobile phones or on their computers. **Facebook, Twitter, What's App,** and **Linkedin** are some of the social media sites that are regularly visited by those who have access to the Internet. While these sites make it easy for Internet users to share ideas, information, photos and pictures with other Internet users they also create the opportunity for users to voice their anger, share their dreams and fears, and/or intimidate, bully or harass other users on the site.

Experts in the fields of Information Technology and Behavioral Psychology have done quite a bit of research on the reasons why people are much more inclined to "speak their minds" and/or to "attack" other users on the Internet than they would be to do so in real life. What they found was that, because the Internet is a "faceless" entity, people find it easier to "open up" to others, sometimes to evoke sympathy, and sometimes to offload their anger on someone they need never look in the eye.

Because Internet users can communicate with other users without being interrupted, as is the case in face-to-face interaction, the temptation to say exactly what they want to without considering the consequences is much greater. In short, social media sites, so these experts found, give the "voiceless people" of society, those who feel oppressed by societal norms and values, the opportunity of venting their frustrations. Of course, not everybody who reads communications like these will agree with what is being said. They will most probably respond with an opinion or perspective of their own and, if both parties are equally frustrated, these to and fro conversations could turn into a vicious cyber "cat fight".

Another tendency, uncovered by these researchers, is that many social network users adopt a new persona which is radically different from their real world personalities. A person who is very shy, very meek and mild, or very lonely, could, for example take on the persona of someone who is outgoing, assertive, confident, and popular because this is the way that s/he would like to be. The adoption of such a persona is especially evident in virtual spaces like *Second Life*, where users can live, work, visit and trade as a self-created avatar because the actual user remains anonymous and is free to say or do whatever s/he wants to.

Dr Azadeh Aalai, a professor in Psychology at the University of Montgomery in America, gives a number of reasons for the increase in aggression on social network sites. Dr Aalai says that one of the reasons could be that most of us have been taught from an early age onwards to control our temper and, by implication, not to express our feelings of anger or frustration. When you are then given the opportunity to do so, as is the case on social media, you do so openly and fearlessly.

Another reason, according to him, is that people in this day and age experience extremely high levels of stress, do not sleep enough and, consequently, "burn out" more quickly. Because of this they are much more inclined to give free voice to their anger and frustration. Modern societies are, moreover, constantly exposed to aggression by the media and by the behaviour of public figures. Since none of these are formally regulated the message that comes across is, "Don't worry about the consequences of what you say: there aren't any!"

Experts urge users of social media networks to be aware of these risks and to always take the necessary steps to protect themselves, first against any form of victimization, second against the temptation to "over-share" information about him/herself, third, against being drawn into vindictive gossiping, racist comments and 'attacks' against other users and, finally,

against becoming addicted to these or any other sites with the potential of isolating them from reality.

Summarized, adapted and freely translated from Vrouekeur, 1 June 2012.

a. Have you, or anyone you know ever been harassed, victimized, or threatened via the Internet, whether this was on social media networks or by e-mail? Do you know someone who seems addicted to surfing a particular Internet site *(Google medical pages, or gaming, for example)*? If you like, you could briefly share some of these experiences with the rest of the group during the plenary session.

b. Now study *Table 3.* Your facilitator will talk you through the risk management strategies in the table and, where applicable, demonstrate on his/her laptop what you could do to manage these risks in such a way that your own safety is not threatened.

c. Use the open space under the table to take notes on things your facilitator says which you would like to remember in future.

Table 3: Protecting yourself against cyber risks

Risk	***Risk management***	***Risk management questions***	***Risk management answers***
Harm to your reputation	Determine your on-line reputation	How do I do this?	Use search engines to scan your reputation – in blogs and social networks
	Protect your reputation		Don't post anything on line that you won't put on a post card

Invading your privacy	Take control of your social network profile	By doing or not doing what?	Use *Settings/Options* to block or give access to your network
			Never post personal information that could put you at risk

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Activity 4: Playing it Safe[5]

In this activity you are given the opportunity of applying your knowledge of cyber safety to a number of imaginary situations – listed in Table 4 - where someone's safety might have been at risk.

What you have to do is to ***study*** the description of the threat (in Column 1), give it a ***name*** (in Column 2), and ***match*** it with one of the prevention strategies (in Column 3).

Some of you might want to do this activity in groups, some in pairs, and some on your own. All these options are allowed provided that you finish the activity in the time allocated to it.

You might also want to read Microsoft's[6] additional safety tips below before you start with this activity.

i. Listen to and trust your instincts – if something feels uncomfortable or alarms you regard that as a warning and do something to stop it.
ii. Immediately report physical threats, intimidation or attempts at exploitation to the police and the carrier. Also block the caller.
iii. Share your phone number only with those you know and trust. Do not put it on social pages or use it to enter content.
iv. Do not make, send or accept provocative texts, photos or videos. Once they are shared they can be forwarded to anyone, even years in the future.
v. Do not reveal too much learner, teacher or member information on school and club sites.

[5] This activity appears in a slightly different format in the Intel Education Digital Wellness Curriculum, Version 2.0, p. 2.9 – 2.10. Intel Corporation 2014
[6] Microsoft, 2014: *Teach Kids Mobile Safety*

Table 4: Managing cyber safety threats

Description of cyber threat	***Name of threat***	***Prevention strategy***
Farouk created a web site, posted mean comments on it and uploaded embarrassing pictures of Anant on it 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 and 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.		*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.*
Nozipho is a registered member of an online tutoring web site and has recently received an e-mail with an update 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.		*Keep screenshots of content posted as evidence of harassment and report the incident to a parent or person of authority. Register an official complaint.*
Thabo started playing *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 responses if 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 5: Cyber Safety Scenarios

In this activity you are required to apply what you have learnt about cyber safety to the case studies hat follow. Your facilitator will tell you how to do this.

Scenario 1

Susan, a Grade 7 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? Why?

_____

_____

_____

_____

_____

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. *What is the threat here?*

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

4. *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 with a keen interest in debating activities. 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 began 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 and the strategies he used 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 because 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 with Thomas so that they could work out a solution together. 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 mind 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. To which of the threats mentioned in the ***Prohibitions List*** (Appendix 1) did Thomas submit? Explain, or give reasons for, your answer.

   _____

   _____

   _____

   _____

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

   _____

   _____

   _____

   _____

   _____

3. Why, do you think, was he particularly vulnerable to this 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.

_____

_____

_____

_____

_____

6. What lessons learnt from Thomas's story could you, as educators apply to your own children or to learners in the classes you teach?

_____

_____

_____

_____

_____

UNIT 4: CYBER CRIME

Introduction

You would have noticed that all the sessions up to now focused on what you could do to ***protect*** yourself and your devices against potential risks / threats. In this, and the next, session the focus shifts to ***how*** you should conduct yourself while in cyber space and ***why*** you should behave in this way. This session focuses specifically on behaviour that is regarded as ***illegal***; the next session focuses on behaviour that is regarded as ***unethical***.

A number of countries in other parts of the world already have strict laws in place to control cyber crime. If you study the table that follows you would see, for example, what legal action is taken against cyber criminals in India. Your facilitator will give you the opportunity to voice your opinion on the appropriateness or not of these consequences and ask you what you would like to see in Acts on cyber crime in your own country.

Table 5: 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 a fine up to 2 takh
Cyber pornography *(including child pornography)*	Publishing obscene content in electronic form	10 years and/or a fine up to 10 takh
Intellectual property crimes	Source code tampering, piracy, copyright infringement, etc.	3 years and/or a 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 a fine up to 2 takh
Phishing	Net banking and financial fraud	3 years and/or a fine up to 2 takh
Invading privacy	Unauthorized access to a computer	2 years and/or a 1 takh fine

Adapted from Intel Education Digital Wellness Curriculum, 2014.

Your facilitator has already told you about the ***Protection of Harassment Act*** in South Africa. Other South African Acts proclaimed with a view to regulating electronic communication and other information-related matters are 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).* *(You might find it interesting to look up these Acts on the Internet to see exactly what they say.)*

There is, however, no South African law dealing specifically with *social media transgressions*. Consequently the criminality of cyber transgressions, including social media interaction, and the action taken

against transgressors are informed by Constitutional and Common Law principles. Some of the Acts whose principles have served as basis for legal action against cyber transgressors include the ***Employment Act, Consumer Act,*** and the ***Protection of Intellectual Property Act.***

Activity 6: Crime or not?

Instructions

1. Quietly read, or have someone in your group read out loud, the case study allocated to you by your facilitator.
2. Then, bearing in mind the discussions on cyber legislation, discuss each of the questions associated with your case study with a view to reaching consensus on the answers.
3. If your group agrees on the answer to a particular question, write that answer in your own ACTIVITY BOOK. If the group disagrees, indicate the disagreement in your ACTIVITY BOOK, indicating what you think the answer should be and why.
4. Please note that each person must write down an answer to each question since the next activity will require you to discuss your case study and the answers to the questions your group gave with someone from another group.

Case study 1 (Group 1)

Two employees working for the same organization were dismissed because they had posted derogatory comments about the organization on Facebook. The employees challenged the fairness of their dismissal at the CCMA on the basis that their constitutional right to privacy had been undermined.

Questions

1. *What do you think the CCMA judgment was – that the dismissals were fair or unfair? Give reasons for your answer.*

_____

_____

_____

_____

_____

2. *Does this case have any implications for you as a teacher, school principal or employer? Explain your answer.*

_____

_____

_____

_____

_____

3. *Does it have any implications for learners or employees? Explain*

_____

_____

_____

_____

_____

4. *Based on your answers, do you think there is a need for an e-learning or ICT policy in your school or workplace? Give reasons for your answer.*

_____

_____

_____

_____

_____

Case study 2 (Group 2)

A radio station employee was dismissed because he criticized the Board of the organization and claimed that the station manager was a criminal.

Case Study Questions

1. *What do you think the CCMA judgment was – that the dismissal was fair or unfair? Give reasons for your answer.*

_____

_____

_____

_____

2. *Does this case have any implications for you as a teacher, school principal or employer? Explain your answer.*

_____

_____

_____

_____

_____

3. *Does it have any implications for learners or employees? Explain*

_____

_____

_____

_____

_____

4. *Based on your answers, do you think there is a need for an e-learning or ICT policy in your school or workplace? Give reasons for your answer.*

_____

_____

_____

_____

_____

Case study 3 (Group 3)

The CEO of a particular organization accessed an employee's private G-mail e-mail account while she was on leave. He found e-mails on internal organizational matters between her and former employees as well as between her and outsiders not associated with the organization at any time. He then brought various charges against the employee, thus bringing her name in disrepute.

The employee contested the charges, claiming that not only was her right to privacy undermined but also that her employer contravened the RICA Act by accessing her private account.

Case Study Questions

1. *What do you think the CCMA judgment was – did the employer invade her right to privacy and/or contravene RICA?*

_____

_____

_____

_____

_____

2. *Does this case have any implications for you as a teacher, school principal or employer? Explain your answer.*

_____

_____

_____

_____

_____

3. *Does it have any implications for learners or employees? Explain*

_____

_____

_____

_____

4. *Based on your answers, do you think there is a need for an e-learning or ICT policy in your school or workplace? Give reasons for your answer.*

_____

_____

_____

_____

_____

Case study 4 (Group 4)

A group of "cyber crackers" recently attacked the web-site of a well-known South African entertainer. He discovered this one Friday when the group tweeted, "You will be happy to know we are currently running miniop against the Racist X".

On Saturday the attack continued with the following tweet: "Protest against Racist X still hitting hard. We will resume it tomorrow, with double punch". Tweet dreams # Africa.

The attack involves bombarding the service provider of the web-site with so much "traffic" that its usual visitors cannot gain access to the site. As soon as the attack stops the site opens up for its usual visitors.

Case Study Questions

1. *Which legal steps do you think the entertainer could take?*

_____

_____

_____

_____

2. *What do you think his chances are of winning the case should he decide to make a case against these crackers? Give reasons for your answer.*

_____

_____

_____

_____

3. *Does this case have any implications for you as a teacher, school principal or employer? Explain your answer.*

_____

_____

_____

_____

_____

4. *Does it have any implications for learners or employees? Explain*

_____

_____

_____

_____

_____

5. *Based on your answers, do you think there is a need for an e-learning or ICT policy in your school or workplace? Give reasons for your answer.*

_____

_____

_____

_____

_____

UNIT 5: INFORMATION ETHICS

Introduction

Before we talk about ***"information ethics"*** we first have to agree on the meaning of each of the words that make up this term. You will remember that the very first activity you did in this workshop – apart from the ice-breaker – was to collect ***"information"*** on a fellow participant's level of cyber knowledge and expertise. In the sessions dealing with cyber security and cyber safety you were given ***information*** on cyber threats and ways of minimizing these. In the next session you were given ***information***, albeit minimal, on laws that could be used to deal with cyber crimes as well as ***information*** on CCMA judgments relating to specific cyber transgressions.

While the kind of information in each of these sessions was different they all had one thing in common. They were all factual in nature, that is, it was possible to check the truth and/or accuracy of each of these pieces of information. People's opinions on or perspectives on issues, situations and other people cannot be checked in the same way because they are usually determined by the person's upbringing, religious or political orientations, the situation or context within which the person finds him/herself and his/her personal bias. ***When we talk about information, we are therefore referring to things that have been verified /proved to be accurate or true.***

Defining ***ethics*** is not so easy, therefore we would like to illustrate its meaning by means of a short fable. Your facilitator will first read the fable to you and then give you the opportunity to voice and defend your opinion on the ***ethics /morality*** of the characters in the fable. Based on the ensuing discussion you will then, in conjunction with your facilitator, have to ***write a definition*** of ethics that satisfies the majority of participants in this workshop.

The scorpion and the frog

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, because I fear 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 and 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 and would not do a thing like that. I know that it would mean the end of both of us."

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 a sting in his back as the scorpion stung him.

"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***

Having read the fable – we hope you enjoyed it as much as we did – consider the following questions as part of the plenary discussion on ethics/morality.

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

   _____

   _____

   _____

   _____

   _____

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

   _____

   _____

   _____

   _____

   _____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

7. 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.

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

11. 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

_____

_____

_____

_____

_____

12. 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.

_____

_____

_____

_____

13. 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?

_____

_____

_____

_____

_____

14. 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 7: Information ethics code of conduct

For this activity your facilitator will divide you into different groups, some consisting of classroom teachers or employees only, some of school principals or employers only and some consisting of equal numbers of both.

Each group has to:

1. First discuss the values they think should inform e-learning and the human rights that should be actively protected in e-learning situations and/or schools where e-learning has been introduced.

2. Secondly, based on the outcome of the group discussion:
   - *Groups consisting of classroom teachers or employees only should, as a group, draw up a code of conduct for the use of information and ICT in their classrooms or places of work. The rules included in the code should reflect a commitment to values as well as respect for other user's human rights.*

   - *School principal or employer groups should, as a group, draw up a code of conduct for the use of information and ICT as a means of school or work place management. The rules included in the code should reflect a commitment to values as well as respect for other users human rights.*

3. On completion of its Information Ethics Code of Conduct each group should post it on the wall where everybody can see and comment on its quality and possible effectiveness.

Having done Activity 7, how would you define ethics? Do you think it is important for people to behave in ethical ways? What is the relationship between an ethical code and a law?

Before you answer these questions, read what the philosophers – people who spend their lives trying to determine the truth about life, human nature, religion, et cetera – have to say about morality/ethics.

> *Throughout the ages philosophers have asked themselves, 'What is morality? Is it obedience to the law? Is it the same as integrity? Who decides what is moral or not?" Some philosophers would argue that it is the kind of behaviour that all "rational/logical people" would regard as normal, or the norm; others would argue that morality is the same as obedience/ adherence to the rules or prescripts governing the behaviour of people (Gert, 2002, cited in Pentz, 2010).*
>
> *In both these cases it is clear that a person's morality (or ethics, which is just another word for morality) is assessed against certain accepted standards. Which leads us to the next question: 'Who determines the standards – the Church, the government, the 'people' (society) or individuals? Notwithstanding years of philosophizing the answer to this question keeps on changing. People's values – that is, their sense of what is moral or not – change over time, as they become older and/or wiser, richer or poorer, more or less powerful in their community, workplace or society. Eventually each person would have developed his/her own set of values / morals, his/her personal code of ethics. And it is the extent to which each person behaves in accordance with his/her personal code of ethics which determines his/her morality.*
>
> *But what happens if a person's own code of ethics differs from the values encapsulated in a country's social contract – its Constitution – or laws?*

Then, according to philosophers, theologians, and psychologists, the person will find himself in a moral dilemma – a Catch 22 situation,

between the frying pan and the fire. Whichever choice s/he makes, will have both positive and negative consequences.

There are many examples of moral dilemmas in the history of the world.

- Think of Thomas More, a British scholar and confidant of King Henry IV. He refused to accept the king's decision to divorce the queen because she could not give him a male heir. More argued that divorce was against the doctrine of the Catholic Church and, even though he was the King, Henry should obey God's laws. Thomas More stuck to his decision even though he lost all his property and was publically beheaded for his resistance.

- Think of the French Resistance during World War II. People from all walks of life who joined the *Resistance* risked their lives and the lives of their friends and family by smuggling Jews out of Germany through underground tunnels and dark forests, simply to prevent them from dying in gas chambers or from being buried in mass graves.

- Think of Nelson Mandela, who refused to submit to apartheid laws even though he knew he might be sentenced to death. He wasn't but he did spend the larger part of his life in a maximum security prison on Robben Island.

- Think of the UCT professor, a South African, who not so long ago agreed to his mother's request to let her "die with dignity" by giving her an overdose of sedatives even though it meant that he would lose his job, become a social outcast or even land in prison.

Would you say these people were simply stupid or was their behaviour an indication of their morality?

Do you think that there might be people in your country whose values conflict with the values of the Constitution and/or the laws of the country concerned? In South Africa, for example, it is legal to have an abortion although there are many religions that forbid this. Is this fertile ground for a moral dilemma?

Read the case study in the text box that follows and then decide.

Susan Tshabalala is a devout Catholic. In terms of her religion all life is sacred. Catholic women may therefore not take any steps to prevent them from falling pregnant or have an abortion if they are not not ready or able to give birth to a baby. The public hospital where Susan is a maternity nurse performs abortions. Susan knew this when she started working there but was not worried because the abortions are done by doctors, not by nurses.

One day, at one of their regular staff meetings maternity nurses were told that, in future, they would have to assist the doctors with abortions since the demand for this has increased to the extent that doctors can no longer cope on their own. Susan refused. She knew that the abortions were legal in South Africa but, according to her, they were immoral and she could not and would not be part of what she regarded as murder.

1. What do you think will happen to Susan because she refused? In other words, what would the consequences of her action be?

   _____

   _____

   _____

   _____

2. How do you think Susan would feel if she agreed to help with abortions? In other words, what would the consequences of her actions be in this case?

_____

_____

_____

_____

_____

3. What would you have done if you had been in Susan's shoes? Give reasons for your answer.

_____

_____

_____

_____

_____

Examples of moral dilemmas in the sphere of *Information and Information Communications Technology* are also becoming more and more common. The most famous of these is the one in which an American citizen who 'cracked' the FBI network, uncovered "sensitive" information regarding the behaviour of American troops in Afghanistan and other war zones, and posted these on the Internet for all to see.

Can you remember what happened to him? Did he apologize or retract what he said? What does this say about him – was he a criminal or an ethical person?

Activity 8: Information ethics dilemmas in education

In this activity your facilitator will allocate a different educational moral dilemma to each group.

Your job is to:

- 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.
- Once everybody has answered the questions in writing, group members should share and discuss their answers with one another.
- 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.
- Once the group reaches consensus about the most appropriate response the rapporteur should write down this answer.
- If the group cannot reach consensus the rapporteur must indicate this, giving reasons for the stalemate.
- Once all the questions and responses have been dealt with, answer the last question in writing.

Information ethics dilemma 1

(School principals and classroom teachers)

Mrs Jantjes is a Grade 12 English Language teacher. Much of her teaching is done using e-learning methods and devices. The learners in her class also use e-learning devices for learning and the preparation of assignments.

Having spent some time teaching learners how to analyze poems, Mrs Jantjes decided to set a test to see how well they had mastered this skill. She then searched the Internet for examples of poetry e-tests, with their answers. She chose one of these tests, with its completed memorandum,

to use as her own class test. She then stored both the test and the memorandum in a “Test Folder” on her computer.

In preparing learners for the test she told them that the test would be given to them in electronic format on the set date and that they could choose whether they wanted to hand in an electronic or a hard copy answer script. About half the class opted to answer in the traditional way, writing the answers on paper; the rest chose to submit their answers electronically.

On the day of the test Mrs Jantjes noticed that some of the learners who decided to hand in electronic answer scripts were finished in less than 20 minutes whereas others only finished after the learners who opted to submit pen and paper scripts.

Intrigued by this occurrence Mrs Jantjes first marked all the e-scripts, starting with the scripts of the e-writers who took ages to finish. To her horror she found that their answers to the questions were so similar that they must have copied from each other. She just did not know how they could have done that because they were not even sitting close to each other during the test.

She was even more shocked when she marked the e-scripts of the learners who had finished the test in 20 minutes or less. All their answers were exactly the same as the answers she had on her memorandum- word for word.

Mrs Jantjes realized that the first group of learners must, in some or other way, have established some form of electronic communication with one another during the test, thereby enabling them to share answers. The second group, on the other hand, must, in some or other way, have gained illegal access to her computer and her Test Folder.

Mrs Jantjes considered handling the matter herself but did not know how to. She decided therefore to report the matter to the principal.

Questions

1. *Was Mrs Jantjes behaving ethically when she downloaded the test paper from the Internet? Give reasons for your answer.*

   _____

   _____

   _____

   _____

   _____

2. *What is the dilemma Mrs Jantjies now finds herself in? In other words between what and what does Mrs Jantjes have to choose?*

   _____

   _____

   _____

   _____

   _____

3. *What makes the dilemma a 'moral' one?*

   _____

   _____

   _____

   _____

   _____

4. *Do you think Mrs Jantjes made the right decision? Give reasons for your answer, with specific reference to the possible consequences of the action that she planned to take.*

_____

_____

_____

_____

_____

5. *What would have happened if she had handled the matter herself?*

_____

_____

_____

_____

_____

6. *What would you have done if you had been in Mrs Jantjes's shoes? Give reasons for your answer.*

_____

_____

_____

_____

_____

7. *Did the group discussion changes your perception of what Mrs Jantjies should 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

(One group of classroom teachers and one group of principals)

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 he needs to do to open the e-mail, is to 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 open 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' one?*

_____

_____

_____

_____

_____

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 against 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 3

(Classroom teachers only)

Sipho is a grade 9 learner in a public school which 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?*

_____

_____

_____

_____

_____

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 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 4

(School principals or classroom teachers)

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 movies for free 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?*

_____

_____

_____

_____

_____

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 they 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?*

_____

_____

_____

_____

_____

APPENDIX 1 - PROHIBITIONS LIST

i. Never post your ID, password, pin numbers, home address, photos, or contact details on the Internet or social networks.

ii. Do not place *any* pictures on your computer or phone that you would not want others to see.

iii. Do not post personal photos of yourself or your family on a social network of any kind.

iv. Try not to make friends with strangers online - include in your friends list ony people you already know.

v. Do not confide any secrets, hang-ups, or other personal problems to someone on a social network, no matter how sympathetic they may seem. What is posted goes round …and round…… and round, forever!

vi. Always be suspicious of 'deals' or 'winnings' that sound too good to be true – they usually are!

vii. Do not open e-mails dropped into your SPAM folder – delete them immediately.

viii. Regularly review and adjust – if necessary - the access status of your social network.

ix. Do not respond to any message that makes you feel uncomfortable, afraid or even angry – the best way to get those who sent it to stop is to ignore their messages and/or to stop them from making contact with you by "blocking" them or changing your social media account.

x. If you receive such messages on a "chat room", leave the "room" immediately.

xi. Do not ignore continued harassment or physical threats - report them to the local police as soon as possible,

xii. Do not let other persons use your mobile phone unless you disabled your GPS for social networking applications.

xiii. Beware of cyber addiction – keep track of the time you spend on the Internet. If it takes up most of your day cut down – there is still a real world out there, with people who care for and want to be with you.

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. Concepts in 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. (2008). 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 261674

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