Digital Wellness Programme

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

SECONDARY SCHOOL TEACHERS' MANUAL

Digital Wellness Programme

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

SECONDARY SCHOOL TEACHERS' MANUAL

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 - SECONDARY SCHOOL TEACHERS' MANUAL

October 2015

ISBN: 978-1-928261-68-1

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

FOREWORD

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 is meant to enhance not only your ability to manage your online activities in ways that will benefit you but also to enable you to teach learners in your classes to do the same. Focusing on *cyber wellness,* it tells you what cyber wellness is, why it is important and which values are crucial to its creation. It also includes a whole range of activities which you could use to develop in senior and further education phase learners an awareness of their responsibilities as citizens of the digital world.

In addition to the *Teacher's Manual,* you would have received a *Learner's Activity Book* and a *Resource and Concepts* booklet. Both these are meant to supplement and support what is in your *Teacher's Manual.* The *Learners' Activity Book* contains short readings, followed by activities deemed suitable for learners in Grades 7 to 12. The *Resource and Concepts Book*, which consists mostly of definitions and explanations of acronyms and terms used in the digital world, is essentially a reference book for teachers – something like a dictionary or encyclopaedia, which explains or describes concepts and issues addressed in the other two booklets.

On completion of the activities included in these booklets, you and your learners ought to:

- *Be aware of* the opportunities and dangers associated with the use of the Internet
- *Know how to* protect yourselves and your electronic devices against these dangers and threats
- *Have* a basic knowledge of the laws governing Internet engagements as well as the legal consequences of transgressing these laws
- *Understand* the difference between responsible and irresponsible, ethical and unethical Internet behaviour

We trust that you will find these booklets useful and enjoyable and that they will help you and your learners to become valued and responsible citizens of the digital world!

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

LESSON 1: CYBER WELLNESS

A good way for teachers to start a programme on cyber wellness at schools is to create the opportunity for learners to reflect on their own knowledge, understanding and use of the Internet. A fun way of doing this at secondary school level is to give learners the opportunity of reflecting on and testing their own knowledge and understanding of digital travel and its responsibilities. You could, for example, give them a ***Cyber Wellness Quiz.*** Not only would it make them think about their own Internet behaviour but it might also give you, the teacher, a point of departure for further learning.

We have included two quizzes in this Manual – one for learners in Grades 7 to 9 and another for Grades 10 to 12. If you do not like them, please feel free to design your own, based on your in-depth knowledge of the learners whom you teach.

Regardless of whether you use your own quiz or the quizzes provided, we suggest that you prepare learners for the quiz by asking them to talk about ways in which the Internet has changed the world and the way in which people interact with others. You could perhaps jot down some of the answers on a flip chart, chalk- or white board if you want to, without judging or contesting their views. All you need to do is to facilitate a discussion on the digital world and digital citizenship.

Wrap up the discussion by pointing out that digital technology is all around us – at work, in school, in libraries, in our socialization with others, and even when we feel ill and want to know what might be wrong. Warn learners that, while the use of digital technology facilitates the immediate availability of information and social contact, not everyone uses it in an appropriate and lawful way.

Having introduced the notion of cyber wellness, refer them to Activity 1 in their Activity Books. Focusing on the quiz for the Grade concerned, explain what is expected of them, and them the approximate[1] time you will give them to complete it.

Please note:

The answers to the Grade 7 – 9 Quiz are highlighted in the *Teacher's Manual*; the answers to the Grade 10 – 12 Quiz can be found in Section 4 of the *Resource and Concepts Book*,

Activity 1(a): Digital know-how quiz

(For learners in Grades 7 to 9)

Answer the questions below by circling the correct answer.

You have approximately 10 minutes to 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

[1] It should take the average learner between 10 and 20 minutes to complete the quiz, but please make allowances for learners with disabilities and other barriers to learning.

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. Upload or 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 quiz

(For learners in Grades 10 to 12)

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

You have approximately 20 minutes to complete the quizz 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?

Debriefing

When the time is up, go through each question with the learners, asking them to indicate what they answered and why they think their response is appropriate. Then, if they were on the wrong track, share your answers with them.

Plenary discussion

Follow up the quiz with a plenary discussion of "Cyber Wellness" - as a concept and a way of life. We suggest that you start by first focusing on ***"wellness"***in general *(talking about aspects such as health, wealth, happiness, safety and security)*, and then relating these to ***"cyber wellness.*** Ensure that learners understand the composite nature of the term – *wellness* - since it refers to a person's *overall* condition, that is, to the person as a *whole.*

Applied to the digital world, "cyber wellness" would imply an awareness of and alertness to the fact that the choices people make and/or the decisions they take (regarding how and with whom they want to communicate on the Internet) could affect their health, wealth, happiness and safety as well as the safety and security of their devices.

Wrap up the discussion by referring learners to **Activity 2** (in their Activity Books). Tell them to read and carry out the instructions for the activity as set out in their Activity Books. Also give them an indication of how much time they have to complete the activity.

Activity 2: Digital wellness

Study **Table 1** below. The aspects of your life that could be negatively affected by the way in which you or others behave on the Internet are listed in the left hand column. The right hand column consists of a number of specific Internet behaviours that could negatively affect specific aspects listed in the left hand column.

Your job is to:

First match the specific behaviour in the right hand column to the appropriate aspect in the left hand column, and

Then explain, in writing, in the appropriate space below the table, how this behaviour would affect the aspect with which you matched it.

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

Appropriate matches would be:

- Health – Gaming addiction
- Wealth - Phishing
- Happiness – Cyber bullying
- Safety – Cyber predators
- Security- Pop-up advertisements

How they relate to each other would differ. Discuss these differences with learners when they give their feedback.

Wrap up the activity by emphasizing the importance of keeping ourselves and our devices safe from internet threats. Point out that the first step to doing so is to master the jargon / language of the digital world. Other steps would be to protect their devices against infection and/or attacks by other users, and behaving in such a way that it would be difficult for anybody else using the Internet to 'attack' or cause them harm. Tell learners that the 'sessions' or 'lessons' on cyber/digital safety and information ethics in which they are going to participate are meant to assist them in doing all of these.

LESSON 2: CYBER-SPEAK

Briefly talk about the power of language in general – what one can do with words, how difficult it is to understand someone who speaks or writes in a different language, and how people appreciate it if someone else takes the trouble of learning even the basics of their language – like *greetings*, *'please'* and '*thank you'*, *'how are you'*, etc.

Tell learners that, 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 this world. Then display, on a poster or a power point slide *(see Figure 1 for an example),* one of the terms that you are going to use in teaching learners about digital safety and security. Ask learners to give examples of incidences that illustrate the occurrence of actions associated with this term / concept.

CYBER CRIMINAL

Definition

A cyber criminal is someone who accesses someone else's mobile phone or computer with the intention of doing harm to either the device or the person using the device.

<u>Examples</u>: hackers, crackers, identity thieves, phishers, sexual predators

Figure 1

Refer learners to Section 2 of the *Resource and Concept Book,* which describes and explains terms / concepts used in discussions on digital matters.

Activity 3: Cyber-speak

Divide learners into small groups. Each group has to select a term / concept from the list and then design a poster or flash card similar to the one you used as an example.

The instructions for the design of the flash card / poster are set out in their Activity Books. Alert them to the fact that their designs will be evaluated against three criteria, namely *accuracy, clarity* and *creativity*.

When learners are done, give each group some Prestik and ask them to display their designs on the wall. The different groups then walk around the class (like they would in an art gallery) evaluating the designs of the other groups in terms of the three criteria given to them.

LESSON 3: CYBER THREATS

Introduce this session / lesson by creating an awareness of the benefits associated with digital citizenship. Talk with learners about the many opportunities opened up by the Internet, opportunities that they might never have had otherwise – viewing places to which they have never travelled, communicating with people across the globe, having access to information on anything they want at any time of the day or night, et cetera. You might like to give them the opportunity of sharing with you and their fellow learners some of ways in which they have already availed themselves of opportunities like these.

Having highlighted the benefits, shift your focus to the threats learners could face as digital citizens. Point out that, while the opportunities are great, the Internet is also full of risks, threats and/or dangers. You could, for example, illustrate your point by drawing an analogy / comparison between the virtual cyber/digital space and physical spaces like houses, cars, roads, or the ocean, whatever is most familiar to the learners with whom you are having this discussion. You could point out that, although we assume that these “spaces” are safe, this is not necessarily the case. A house or car could, for example, be burgled - even if all the doors and windows are closed; a car could be involved in an accident - although the driver goes out of his 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.

Point out that learners might, in their travels through digital space, stumble across a website that displays inappropriate content, find that their e-mail or social networking account has been hacked and/or misused, realize that someone has misinterpreted what they posted and responded with hurtful comments, or discover that they have been embarrassed by photos or information associated with their online profiles.

Conclude the discussion by referring learners to Activity 4 in their Activity Books. Read the instructions with them, explaining exactly what they should do. Also tell them how much time they have to complete the activity.

Activity 4: Cyber threats

Table 2: Internet Threats

<table>
<tr><td colspan="3"><b><i>Online Activity 1:</i></b>
<i>Posting personal information (name of school, phone number of physical address) on media sites</i></td></tr>
<tr><th>STOP</th><th>THINK</th><th>CONNECT</th></tr>
<tr><td>What are the risks?</td><td>How could this affect my safety or that of my family?</td><td>Should I go ahead and do this?</td></tr>
<tr><td>People other than friends and family could find out where I live and study.</td><td>It could lead to criminal acts such as theft or burglary at my house.</td><td>I will not post personal information on social media sites.</td></tr>
</table>

<table>
<tr><td colspan="3"><b><i>Online Activity 2</i></b><i>:</i>
<i>Clicking on a link in your e-mail, or a Facebook post or smart phone message that announces a funny video of you.</i></td></tr>
<tr><th>STOP</th><th>THINK</th><th>CONNECT</th></tr>
<tr><td>What are the risks?</td><td>How could this affect my safety or that of my family?</td><td>Should I go ahead and do this?</td></tr>
<tr><td>My computer might be infected by malware.</td><td>Is this link connected to a trusted source or is it suspicious?</td><td>Only if I am sure it is a trusted source, e.g. if there are no grammatical or spelling errors, awkward messages or grand announcements of huge wins or inheritances on it.</td></tr>
</table>

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?
My device may be infected with malware	No risk to people but possibly to my computer	Not unless I am sure it is a reputable one.

Online Activity 4:
Researching various web sites on environmental 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?
My computer might be infected by malware	None that I can think of	Provided I have a good anti-virus program this is be a good idea since the Internet could be a valuable source of information on a range of topics.

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?
It could draw unwanted attention from people I don't know.	Unwanted attention to me and my family could become dangerous if the people who see the selfies are dangerous.	Under no circumstances

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?
The people may be criminals, sex offenders or other deviants	My family and I could be emotionally and physically harmed if the people are criminals, sex offenders or other deviants	Under no circumstances

Wrap up this lesson by comparing learners’ answers with the suggested answers in your Teacher’s Manual. If learners are off track, give them time to adjust their answers; if their answers are better than the ones in your manual, adjust your answers.

LESSON 4: DIGITAL SAFETY AND SECURITY

Remind learners of the earlier analogy between real life spaces and the virtual space of the cyber world. Highlight the fact that, because people are aware of the risks they run when moving around in actual, real-life spaces (houses, cars, etc.) they take special precautions to protect themselves. Ask them what steps they, their parents, or the authorities take to try and make these places safer. Possible answers could include:

- ***For a house*** - burglar bars, alarms, security services (like Chubb or ADT), CCTV cameras, not building a house too close to a river or an ocean.
- ***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.

Share with learners the view that, in order to move around safely in cyber space, our digital 'vehicles' (that is, our smart phones and computers) not only need to be in good condition but should also be protected against cyber / digital thieves, burglars and other predators. Indicate that the implications are that we should:

i. Know the risks/threats that digital travel poses to our electronic devices.
ii. Take the necessary steps to protect our devices against all forms of 'attack'
iii. Avoid exposing our devices to places and spaces that are unsafe

iv. Be extremely careful about whom we allow into our social space and/or to whom we give access to our devices

v. Conduct ourselves in ways that will not harm our reputation, threaten our safety or pose a risk to our devices

Ask learners what they do to protect their devices. Then invite them to join you in looking at ‘experts’ advice on what Internet users should do to protect their devices. Refer them to ***Activity 5*** in their Activity Books. Read and discuss with them the experts’ advice on smart phone protection, replicated below for your convenience.

Activity 5(a): Smart phone safety and security

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 information. They also make it possible for users to take photos and videos that are fun. The flip side of these benefits is that smart phones also create opportunities for bullying and the posting of suggestive photos or videos *(sexting).*One of its most remarkable features is that it includes GPS tracking which makes it possible for anyone who wants to 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 pose the risk of a child being tracked by potential kidnappers or other adult predators. It becomes even more dangerous if photos are tagged because *geotagging* reveals precisely when and where the photo was taken.

Smart internet users **STOP** and **THINK** *before* they **CONNECT**. If you want to be **SMART**, you should also:

- ➢ **STOP** to consider the risks you 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 and others' safety.
- **CONNECT** only if the risks are minimal or non-existent.

Smart users also:

- ***Install Security Software*** to protect their phones against *malware* attacks. Most malware apps also come with anti-theft options. They could, for example, use the McAfee Mobile Security app (https://www.mcafeemobilesecurity.com/), which is a reputed security app, to protect 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. Doing so might 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 it with a PIN code or Pattern Lock. This ensures that even if their phone is stolen, the thief cannot immediately access information on it. They could install security software which '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 below.

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

Give learners the opportunity to comment on or ask questions about the reading. Then ask them to help you formulate a list of ***Safety Rules for Smart Phone Use*** that could be displayed in class. Jot down down their suggestions on the chalkboard or a flip chart. Ask for volunteers to design the Safety Rule poster, or do it yourself. Make sure, though, that it is displayed on the classroom wall before the end of the week.

Activity 5(b): Computer safety and security

Initiate a discussion on talking about the evolution of computer functions and roles – from being used for work purposes only to being used for the generation, accessing and sharing of all kinds of information - texts, photos, pictures, music, etc. Tell learners that, without the proper tools, it would be impossible for so-called cyber /digital citizens to socialize with others, or to access and download information from the Internet. It is important, therefore also to keep these devices safe from cyber threats.

Remind them of the focus of the previous session / lesson - ***Smart Phone Safety***. Then tell them that this lesson is about ***Computer Safety***. Ask them what they think the most obvious threats to the safety of their computers are and which steps they think one could take to eliminate or minimize these.

Having heard what learners have to say, refer them to Table 3 which deals with computer risk management. Read through the table *(replicated here for your convenience)* with them, focusing on clarifying and illustrating with examples the terms and concepts in Column 1 and then reflecting critically on the safety tips in Column 2.

Table 3: Computer Risk Management

Obvious Risks	*Tips for safeguarding computers*
Malware infection *(Spend some time discussing different types of viruses and what they do to computers – see Resource and Concepts Book for descriptions of these).*	Ensure that the software on your computer is current. The best way to do so 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 before opening.
Illegitimate access to a computer *(Spend some time talking about hacking, cracking, spying, etc. and the dangers associated with these – see Resource and Concepts Book for explanations of these)*	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 *(Talk about links, pop-ups, messages that talk about grand prizes, inheritances, or warn the user against viruses.)*	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.

Activity 5(c): Smart questions and conversations

Having talked learners through the table, instruct them to respond, in writing, to **the Smart Questions and Conversations** following the table *(replicated below for your convenience).* Tell them how much time they have in which to complete the task, or give it to them for homework.

1. Is your smart phone safe? Are you a smart user? If so, what do you do to keep your smart phone safe? If not, what could you do in future to keep it safe? Remembering what you have just read, use the space provided below to answer these questions.
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. Use your own experience as well as the information in **Table 4** below to design a series of Computer Safety Signs (similar to road signs) that could be posted on the walls of the classroom or computer laboratory so that other learners will recognize the dangers and take the necessary steps to avoid them.

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, in *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 address this. Log in to *(consumersecuritysupport.microsoft.com)*

LESSON 5: SOCIAL MEDIA SAFETY

Start this lesson/session by reminding learners of the Internet threats which they read about earlier. Tell them that activities which follow focus specifically on risks associated with social media interaction.

Refer them to **Activity 6** in their Activity Books.

Activity 6: Rather safe than sorry

A. Read the text on *Social Media Mayhem* (replicated here for your convenience) with them, explaining words, concepts or ideas which you know the learners in your class 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[2] 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.

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

B. Having read the text, ask learners to share, either during a plenary session or in smaller groups, any unpleasant experiences they, or someone they know, have had as a result of social media interactions with other Internet users.

C. Using the plenary discussion or feedback on group discussions as well as the ***Prohibitions List*** in the text box below (not included in Learner's Activity Books) to talk about the different areas of their lives (health, wealth, self-esteem, social life, etc.) which could be affected by their online reputation.

D. On completion of the discussion, task groups of learners with the creation of posters that graphically reflect (cartoons, collages, drawings, etc.) one of the affected areas. Display these on the classroom wall as reminders of the effect that a bad online reputation could have on a person's real life reputation.

PROHIBITIONS LIST

i. Never post you 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 only 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.

LESSON 6: RISK MANAGEMENT

Briefly explain that *risk management* is a term commonly used in government offices and the business world. Risk managers have to anticipate risks / problems that might occur in certain situations and then work out plans to minimize or prevent the risks from occurring.

Refer learners to **Activity 7: Risk Management.**

Activity 7: Risk Management

Tell learners that the next activity requires them to pretend that they are on-line risk managers. They will therefore have to study the scenario described in Column 1 of Table 5, write down in Column 2 the risk associated with the action/s described in the scenarios, and then choose, from the techniques in column 3 the ones most likely to prevent the risk associated with each of the scenarios.

(Please note that the completed table - with the correct answers - are provided in the Teachers' Manual only. Learners' Activity Books do not have these)

Make sure that learners know exactly what they have to do, how much time they have available to do it, and that they can decide whether they want to do this activity on their own, in pairs or in a group.

Table 5: Risk management scenarios

Scenario	***Name of identified risk***	***Prevention technique***
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.	Cyber bullying	Keep screenshots of content posted as evidence of harassment and report the incident to a parent or person of authority. Register an official complaint.
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.	Cyber predator	Block the user who is making you feel uncomfortable with his/her comments and/or requests for personal information
Nozipho is a registered member of an online tutoring web site. She recently received an e-mail requiring her to update all her personal information on their web site, using the link provided. If she has not done this within a week she would be blocked from the site permanently.	Identity theft and/or phishing	Ignore any intimidating or supposedly official messages that direct you to a link and require the updating of personal information.
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.	Gaming addiction	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.

***Note**: Answers appear in Teachers' Manual only.*

Once everybody has completed the table show, or orally share, the responses in your table with learners – theirs have only the scenarios in them – allowing them to compare their answers with yours and to comment on or add to what you have shown them. Adjust *your* answers to accommodate their responses if you agree with them OR, if you think your response is better, persuade them to adjust theirs.

LESSON 7: DIGITAL/CYBER LEGISLATION

Introduce this session / lesson by asking learners whether they know of any laws in their country that have the protection of digital citizens as purpose. If they do, ask them to briefly tell the class what the laws stipulate and what the legal consequences are for people who break these laws. If they do not know, tell them yourself – this might require you to do some surfing on the Internet since each country has its own laws and/or regulations that deal with media in general and, sometimes, with Internet media matters.

Having done so, refer and talk learners through **Table 6** (in their Activity Books), which would give them an indication of what happens to cyber criminals in India, and ask them to indicate, with reasons, whether or not they regard the legal consequences of each as appropriate or not.

Table 6: Cyber crime and its legal consequences in India

Cyber crime	Description	Punishments
Cyber stalking	Stealthily following a person, by tracking his/her 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.

If you are teaching in South Africa, give them a sense of the status quo here by naming and indicating the purpose of each of the following pieces of legislation. 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):.***

You could even briefly summarize each of these if you think that this would be useful or, if you are dealing with Grade 10 to 12 learners, ask them to do the surfing and report back to class.

You could also display a summary of the ***Protection of Harassment Act*** (in the text box that follows), indicating its significance in relation to cyber safety issues discussed in the preceding session. Emphasize that the three key features of this Act that makes it significant, are (a) its definition of harassment, (b) its potential to protect teenagers against cyber bullying, and (c) that it provides victims of cyber bullying with an inexpensive civil recourse that is meant to stop most forms of harassment, also e-harassment. Ask learners to relate what is in this Act to the cyber safety readings and scenarios discussed in the previous session / lesson.

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 media content 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 the perpetrator 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.

Conclude the discussion by dividing learners into small groups (5 to 6 per group) and then refer them to **Activity 8**. The activity requires them to first read the imaginary scenarios - similar to ones they might face in the real world - and then answer in writing the questions following each scenario. Encourage them to use the insights they have gained thus far in deciding how *they* would have reacted to these scenarios.

Activity 8: Social media scenarios

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?*

Possible answers

She should not respond to any of the mean messages – that will only make matters worse because bullies like these thrive on attention. She should, however:

- Print the messages out as evidence
- Show the messages to her parents or some other trusted adult. They can help!
- Block the bullies' e-mails
- Remove the bullies' names from her Friends List.

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 her 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.*

Answers

User names and passwords are private information. The only people that should have access to your ***Skype, Facebook, E-mail, Instagram*** or other accounts are you, your parents and/or other care-givers.

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 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 made him feel very clever and special. As time went on he spent more and more time with his online friends 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 members of the online forum. 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 meeting or telephone conversation with Thomas 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 him 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 safety rules you discussed in class 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 specially 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.
6. What lessons learnt from Thomas's story could you, as educators use in protecting your own children or learners in the classes you teach against gaming and other cyber addictions?

Answer

There are no correct of incorrect answers here. What you want is for learners to critically reflect on the situation, to give informed opinions on what went wrong and why, to understand and to be able to use what is described in this scenario as basis for handling similar situation in their own homes and/or at school.

Ask the groups to share their responses to the questions on the different scenario during a plenary session *(possible answers have been included in the Teacher's Manual).* If the responses of different groups are not the same, ask learners to suggest possible reasons for the differences and to reach consensus about the most appropriate response. If responses are completely off track, share with them the responses provided in your manual, otherwise commend them for sharing their insights with all present.

Information ethics

Introduce the lesson / session by telling learners that the focus in this lesson / session now shifts from ways in which one could protect oneself against *cyber risks created by other internet users to* the way all Internet users *should* behave and *why* this kind of behaviour is crucial to the creation of a healthy and safe digital culture.

Spend some time talking about *etiquette (manners) in general,* making it a point to give learners from different cultures the opportunity of sharing with others what is regarded as good manners in their culture, and to let them reflect on the possible reasons for cultural differences if there are any.

On completion of the plenary discussion, refer learners to **Activity 9.**

Activity 9: The Frog and the Scorpion

Read the fable *(The Frog and the Scorpion)*with them - as dramatically as you can. Then either discuss possible answers to the questions following the fable or allow learners to do so in small groups.

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. S/he 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 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 stung 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."

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

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. an experience in which 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, *"This is what we do in my culture",* or *"In my culture we ……..."*
9. If you have, what are you suggesting about values? Are you suggesting that different people have the right to insist on living in accordance with their own values even if it harms other 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?

Wrap up the discussion by highlighting some of the moral issues informing the fable –things like *compassion*, *honesty*, *integrity*, and accepting *responsibility* for one's actions.

Ask learners what the rules for good behaviour are in their homes and then help them unpack the values on which these 'rules' are based.

Give learners the opportunity of telling the class about incidents when they transgressed the rules of their homes – what 'crime' they committed and what the consequences were.

Use learner responses as basis for the introduction to *moral dilemmas*, explaining a moral dilemma as a Catch 2 situation. Explain that, in such situation, a person has to choose one of two options and that, whatever choice they make would have consequences for them and all the other people involved.

Illustrate the difficulty of choices like these by referring to real-life dilemmas like the ones below *(feel free to choose your own, ones that will have relevance for the learners in your classes).*

- King Henry IV of England decided to divorce the queen because she could not give him a male heir. Thomas More, a British scholar, confidant and friend of the king refused to support the king's decision.

He argued that divorce was against the doctrine of the Catholic Church and that, even though Henry was the King, he should obey God's laws. Because of this Thomas More lost all his property and was publicly beheaded for his resistance.

- During World War II, ordinary French people risked their lives by joining the *French Resistance* movement, which dedicated itself to smuggling Jews out of Germany through underground tunnels and dark forests in order to save them from being thrown into gas chambers or from being buried in mass graves.

- Nelson Mandela 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.

- A now well-known South African professor agreed, not so long ago, to help his mother "die with dignity" by giving her an overdose of sedatives even though it meant that he could lose his job, become a social outcast or even land in prison.

Ask learners to comment on the actions taken by these persons, considering how *they* might have felt if they had not taken the action they did. Use their responses as basis for an explanation of *information ethics dilemmas.* You could, for example, explain it as a situation in which a person has to decide ***whether or not*** to reveal or censor a specific piece of information. Point out that in making such a decision a person might have to make a choice between his/her personal values and the law, or between what is best for an individual or a group. In order to illustrate this, you might want to tell learners about Snowden, an American citizen who made the news because he revealed sensitive information on the behaviour of American troops in Afghanistan and other war zones because he believed it was for the 'common good' or citizens to know what was really going on.

Conclude the discussion by referring learners to Activity 9. Read and explain the instructions, making sure that they understand what to do in each step. Tell them how much time they have for each step, and then let them start.

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. Having read the scenario describing the dilemma, learners have to reflect on the options open to the person experiencing the dilemma. It is important, though, that they follow the procedural protocol exactly as described in the instructions that follow.

Instructions

- 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

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 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' 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 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 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 on which one can post anonymous comments and pictures. 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 hedecided 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 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?*

Note:

There are no correct or incorrect answers here. The purpose of the activity is to get learners to reflect on their own values (Question 5) and their vulnerability to peer pressure (Question 6). What is important, and what you should focus on in the discussion of learners' answers is that their responses to each question should be values-based. In other words, their decisions should reflect a knowledge of information ethics.

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 taught and how much your learners now know about digital citizenship and the issues related to being a digital citizen, give them a creative assessment task that will test their knowledge and understanding of and their commitment to safe, responsible and ethical behaviour on the Internet *(see learning outcomes in the Introduction and Orientation to this manual).*

Allow learners to choose which of the tasks below they want to do – their choice will reflect their unique learning style – or design your own tasks,ones you think are more appropriate to the learners in the classes to which you have taught this course.

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.

Thank you for being an agent for responsible and ethical change.

We trust that you and your learners benefited from the readings and enjoyed most of the activities.

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. (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 261681

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

IFAP
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