Digital Wellness Programme

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

MANUAL FOR WORKSHOP FACILITATORS

Digital Wellness Programme

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

MANUAL FOR WORKSHOP FACILITATORS

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 - MANUAL FOR WORKSHOP FACILITATOR

October 2015

ISBN: 978-1-928261-66-7

Authors / 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

Thank you for agreeing to facilitate a workshop on ***Digital Safety and Information Ethics***. As you probably know, competence in the use of information communications technology (ICT) is not only critical to the development of a literate African information and knowledge society but also to the country's global competitiveness. It is important, therefore, not only to sensitize as many people as possible to the opportunities created by information communications technology but also to equip them with the skills to use such technologies safely, responsibly, and ethically.

One could safely say that most people are aware of the opportunities created by information communications technology, hence the widespread use of mobile phones. Always having a phone with you not only makes it possible to communicate and/or stay in contact with other people where-ever you go but also, if it is a smart phone, always having easy and immediate access to information on just about everything.

While most people are aware of the benefits associated with the use of these technologies they may not be as aware of the associated dangers and threats and/or the steps they could take to protect themselves against these. Do they know, for example, how to protect themselves against 'attacks' by viruses, hackers, cyber bullies and other predators whose sole purpose is to harm them and/or to disable their devices? Do they know that, as is the case in the real world, life in the digital world is also governed by rules, regulations and legislation? Do they know what these rules and regulations are and what might happen to them if they choose to ignore the restrictions these impose?

This workshop has been specifically designed to train interested parties who might like to facilitate workshops on issues like the ones mentioned above. The content selected for the workshop should raise awareness of the importance and impact of information communications technology in

the development of mature and responsible knowledge and information societies in Africa.

The primary aims of the workshop are to:

- Sensitize workshop participants to the opportunities and threats associated with digital citizenship
- Equip workshop participants with the knowledge, understanding, skills and attitudes they would need to effectively facilitate workshops on digital safety and information ethics matters
- Create opportunities for workshop participants to critically discuss (with one another) digital issues like the ones mentioned earlier
- Equip workshop participants with the requisite knowledge, skills and values to survive and thrive in the digital world
- Introduce workshop participants to ways in which they could help others in their particular spheres of interest to become safe and responsible digital citizens

Because participants at the workshop are being trained as facilitators, they should, on completion of the workshop, be able to demonstrate that they:

- Are aware of both the opportunities created by and the dangers inherent in the use of digital technology.
- Know *and* can explain to others what the terms *digital citizenship, digital security, digital safety, digital crime,* and *information ethics* mean.
- Are critically aware of *and* can facilitate critical discussions on *digital issues* addressed in the workshop.
- Are committed to the safe and responsible use of information communications technology *and* the development of responsible *digital citizens* in their particular spheres of influence.

In order to help workshop participants develop this type of competence the workshop focuses on ***five inter-dependent thematic units*** *(see* ***Figure 1*** *below),* each focusing on one or more of the issues mentioned earlier.

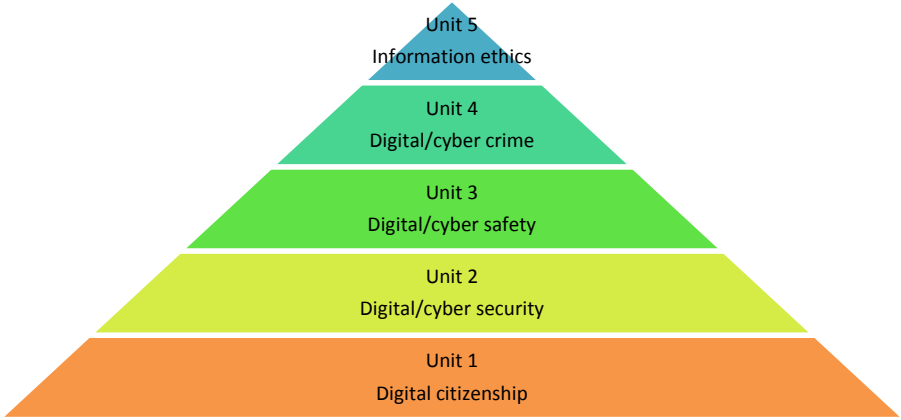

Figure 1: Workshop structure

The content and activities included in each unit should be covered in one or more ***sessions.*** Each session consists of a mix of plenary discussions, readings, individual and group activities.

- *Plenary sessions* are used to introduce the theme, clarify concepts, stimulate discussion or critical reflection and tie up loose ends.
- *Readings* are used as introductions to either plenary discussions or group activities and are meant to stimulate critical reflection of the issues raised in the reading.
- *Group activities* give participants the opportunity of debating issues raised and/or using their knowledge and understanding of issues to identify and solve actual and imaginary information and information communications technology problems

The time allocated to each session is a reflection of the envisaged time needed to complete these activities.

Because the ***themes*** addressed during the workshop are inter-dependent *all five themes* must be covered in every workshop even if there is not enough time to do all the ***activities***. In such cases the facilitator would have to decide which *activities* to cut out, change or replace with activities in the *Recource Book*, in order to still cover all the *themes*. The effectiveness of the workshop will therefore depend largely on the manner in which workshop facilitators use available resources, manage time, monitor and support participant learning. Put differently, workshop facilitators should *manage* and *lead participants* towards the achievement of the workshop *outcomes*. How to do this is briefly explained in the description of the roles that workshop facilitators might have to perform prior to, during and after a workshop.

Workshop facilitators would each have received three documents – a Facilitator's Guide, A Recource Book, and a Participant's Workbook.

- The ***Facilitator's Guide*** spells out the issues that should be addressed, suggests ways of dealing with these issues in a workshop context, and indicates approximately how much time should be spent on each activity. The Facilitator's Guide is meant to assist workshop facilitators in the performance of the roles they have to adopt while workshopping a diverse pool of adults who are interested in becoming facilitators themselves. The activities, case studies and scenarios included in the workshop are adult-oriented and generic in nature. It might, therefore, be necessary to adapt or replace some of the activities and cases studies in workshops catering for specific sectors of society and/or for different age groups. If the potential facilitators are school teachers they are advised to also consult the Manuals for Secondary/Primary School Teachers and Secondary School Learners which contain activities and case studies more appropriate to school learners

Please note that, while the Facilitator's Guide includes *brief descriptions* of the nature and purpose of each activity, it does not include the activities as such. These appear only in the Participant's Activity Book. Facilitators would, therefore, have to refer to the Participant's Activity Book and/or the Recource Book for detailed explanations of different workshop activities.

- The ***Participant's Activity Book*** is a workbook containing short readings on digital and information-related issues, followed by one or more activities that create the opportunity for participants to engage with the issues raised in the reading.
- The ***Concept Book*** is essentially a mini-dictionary of terms used in discussions on digital/cyber safety and information ethics issues. It consists of a list of frequently used acronyms, an alphabetical list of key concepts, a reading on Cyber Bullying and a list of Ten Frequently Asked Questions with proposed answers.

Every workshop facilitator has to perform a number of rules during the course of an IE workshop

a. The role of the workshop facilitator

The term, *facilitator*, is derived from the French word*, facile,* which means *to make easy or possible. A* facilitator is therefore a person who has the duty to *"make a task – 'learning' in this case - easy/possible".* In order to do so, facilitators must do everything in their power to help participants acquire the knowledge, skills and attitudes reflected in the workshop outcomes. They also have to use *all the means* at their disposal - teaching, demonstration, role play, plenary and group discussions, audio-visual aids – to make learning easy/possible. To ensure that this happens, good facilitators therefore tend to work out some or other workshop procedure or protocol. See the text box which follows, prior to conducting the workshop.

Step 1 - Set the tone of the workshop. Do this by welcoming participants, introducing yourself, telling them what the workshop is about, and giving them the opportunity of sharing their *expectations* of the workshop with you and the rest of the participants.

Step 2 - Negotiate the rules of the workshop – what you expect of participants and what they expect of you and each other. Record these and display them somewhere prominent to ensure that they are not forgotten or ignored.

Step 3 - Explain the way in which the workshop and/or workshop sessions are ***structured.*** Allow comments and questions of clarification from participants to avoid potential conflicts from happening later on.

Step 4 – Break the ice with an activity that will simultaneously relax participants and give them a sense of what the workshop is all about.

Step 5 – First introduce and ***then facilitate a plenary discussion*** on the theme or issue to be addressed in the session concerned.

Step 6 - Engage participants in an activity that requires the application of acquired knowledge and understanding.

Step 7: Create opportunities for ***participant feedback*** on the outcomes and their experience of the activity.

Step 8: Wrap up the session by pulling the loose ends together and telling participants what the focus of the next session will be.

b. The role of the workshop manager

A ***manager*** is somebody who makes decisions, designs plans, organizes activities to ensure that the plans are carried out, creates structures, monitors the execution of the plans, and evaluates the effectiveness and efficiency of the plan against pre-specified criteria / results.

A workshop manager would therefore have to make decisions on workshop content, readings, activities, resources and time allocations to ensure the achievement of workshop outcomes.

Once these decisions have been made the workshop facilitator / manager has to prepare for the workshop by:

- *Working through* the Facilitator's Guide, the Recource Book and the Participant's Activity Book.
- *Studying* the *introduction* to each unit carefully to help him / her decide on the most appropriate facilitation method/s, teaching aids, learning activities and time allocations.
- *Surfing the internet* for more information on the topics covered to boost his / her own confidence in his / her ability to field questions from workshop participants.
- *Considering* the compilation of his / her own *Workshop*/*Resource Portfolios,* which could include readings, case studies/scenarios, pictures and/or cartoons from the Internet, newspapers or magazines.
- *Preparing* any teaching/learning aids he / she would like to use in addition to or instead of the ones with which he / she has been provided with.
- *Checking whether* any apparatus that is going to be used during facilitation is in working order and that the venue is suitable for the kind of activities planned.

During the actual workshop the facilitator, performing a managerial role, has to *ensure* that participants are on time, finish activities within the specified time allocations, follow workshop protocol, etc. And all the time, from the beginning of the workshop to the end, the facilitator has to *evaluate* the effectiveness of the learning taking place, immediately addressing whatever might be hindering learning.

c. The role of the workshop leader

Leaders lead, courageously *breaking new ground* and *inspiring others to follow them.* Instead of quitting when things get difficult they think of *new strategies and/or techniques* to realize their vision or reach their destination. In an IE workshop it would mean that facilitators should share their vision of a digital world with participants, convince them of the *value* that digital citizenship could add to their lives, warn them of the imminent *dangers* of a digital lifestyle, and help them acquire the competence necessary for digital survival and the reaping of the benefits associated with being a literate and responsible digital citizen.

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

INTRODUCTION AND ORIENTATION

 30 minutes

Start the workshop by welcoming participants. Then introduce yourself and give them a brief overview of the topic, purpose, themes and structure of the workshop *(refer to the **Foreword** and the Introduction in the Participant's Activity Book for information on these).* Also explain that, because this is a facilitator's workshop, aimed at adults who might have to conduct workshops on digital matters in different sectors of society, the activities, case studies and scenarios included in the workshop are not context-specific. Should participants plan to eventually facilitate workshops for school children, classroom teachers and school principals the participants might have to replace or supplement this Guide with the manuals for secondary or primary school teachers and learners.

Wrap up the introduction and welcome with the ***Ice-breaker*** described below *(Activity 1 in the Participant's Activity Book).*

Activity 1: Ice-breaker

In this activity participants are required to ***match*** terms and their definitions with each other. The activity serves three ***purposes***, namely:

I. To get participants talking to each other about information communications technology (ICT)
II. To familiarize them with key concepts that will be used in Themes 1 and 2
III. To demonstrate to participants the value of using the *Recource Book* in their search for information on ICT and IE matters / issues

The ***facilitator's responsibility*** in this activity is to:

I. Sensitize participants to the risks involved in digital/cyber space activities
II. Prepare and issue the strips of paper required for these activities
III. Ensure that participants understand what they have to do
IV. See to it that participants carry out the instructions as set out in their Activity Books in the time allocated to this activity.

One way of approaching this activity is for you, as facilitator, to follow the steps described hereafter. Please feel free, though, in this and subsequent activities, to adopt alternative approaches that better suit your facilitation style and/or the learning styles and needs of different target groups.

Step 1

Divide participants into ***two groups*** that would naturally compete with each other – males against females, teachers /district officials against school principals, employed and unemployed, etc. – to create a spirit of healthy competition and the active participation of all participants.

Step 2

Issue two envelopes containing *strips of paper* to each group, one envelope containing strips on which you have written different ***terms/ concepts*** and the other containing strips with ***definitions*** of the terms *(use your Recource Book as a source in the preparation of these strips).*

Note: You could either give both groups the same terms and definitions or give each group a different set of terms and definitions.

Step 3

Tell participants that each group has to ***match*** the *terms* in one envelope with the *definitions* in the other and that the winning group will qualify as champions of the first round of competitions.

Step 4

Walk around, checking that participants are on the right track but do not be tempted to help anyone with the matching exercise as such. If you do, the group will be disqualified.

Step 5

When all the groups have completed the exercise, ***display*** the correct matching on a ***Power Point Slide*** (PPS) or simply read the answers out.

Note

This activity could also be used to facilitate workshops for adults across different sectors and, with minor adjustments/replacements also for workshops aimed at educators and learners in the senior phase of secondary schools. However, if the target group is primary school children, the Ice-breaker activity in the Manual for Primary School Teachers would be more appropriate.

UNIT 1: DIGITAL CITIZENSHIP

SESSION 1  60 minutes

Introduce this unit with a discussion of *citizenship* as a concept. You could, for example, ask participants to share with you their understanding of what a society, citizenship, and culture are, what the relationship between the three should be and why. Talk, for example, about the origin and function of societal values, the responsibilities of citizens, and the purpose served by government regulations.

Follow the introduction with a discussion of *digital citizenship (see Recource Book for a definition of the term),* highlighting the similarities and differences between ordinary and digital citizenship. Ask participants to indicate what they think the similarities and differences between the real world and the digital world are, whether the same values and rules that govern real societies should also apply to digital societies or not, and, if so, why?

Wrap up the discussion by first reading with participants the *Introduction* to *Session 1* in their Activity Books. This done, tell them that, in order for the workshop to be effective you, as the facilitator, must know how cyber savvy the group is and that the next activity is aimed at getting them to help you determine this. Then refer them to Activity 2 in their Activity Books.

Activity 2: Cyber Savvy Research

In this activity participants are required to adopt the role of ***researchers.*** Their task is to collect information on fellow participants' knowledge of digital threats and appropriate digital behaviour by interviewing ***one*** of the

workshop participants, using the ***questionnaire*** that appears in their Activity Books.

The ***primary purpose*** of the activity is to help the facilitator determine the average level of expertise of the target group so that s/he can allocate more time to aspects with which the target group does not seem familiar.

A ***secondary purpose*** is to introduce participants to the process of information gathering and interpretation, something that is critical in determining the accuracy and objectivity of information posted on the Internet.

The ***responsibility*** of the facilitator in this activity is to operate as the ***guide on the side***, ensuring that participants understand the interview protocol, and assisting them in the analysis and interpretation of collected data.

i. First, tell participants that this is a *pair activity*. Ask them to pair up with a person whom they do ***not*** know or with whom they would ***not*** normally associate.

ii. Once the pairs have been formed*, read the introduction* to *the activity to the participants,* making sure that they know exactly what they have to do.

iii. Go through the interview protocol with them, answering clarification questions if and when these arise.

iv. When you are sure that everybody understands what is required, offer some suggestions on time management to help them complete the activity in the allocated time and let them start.

Debriefing

When you are sure that everybody has completed Activity 2, initiate a debriefing session.

1. Tell participants that the questions in the questionnaire refer to one of three features of digital citizenship that will be addressed during the course of the workshop, namely *cyber security, cyber safety* and *information ethics*.
2. Graphically illustrate *(using either a Power Point slide or a Flip Chart*) the difference between the three terms *(see Figure 2 for a graphic illustration).*

Figure 1: Workshop themes[1]

3. Using the graphic illustration as frame of reference *work through* the questionnaire with participants, asking them to (a) indicate which questions relates to which feature, and (b) to highlight each feature in a different colour - *e.g. all the questions relating to cyber security in*

[1] Derived and slightly adjusted from INTEL Corporation, 2014.

yellow, those relating to cyber safety in green, and those relating to cyber ethics in blue.

Note: Cyber crime is not explicitly addressed in the Questionnaire so ignore this feature for the moment. It will be dealt with later.

4. Focusing on *one feature (all the questions highlighted in the same colour) at a time*, ask participant "researchers" to indicate by a show of hands whether the people they interviewed answered ***Yes*** or ***No*** to each question.
5. Use this feedback *(on the responses recorded in Column 2 of the questionnaire only)* to *construct* (on a flip chart or Power Point slide), ***three graphs*** *(pie chart, line or bar graph)* - one graph per highlighted feature - indicating the number of people who responded *yes* and *no*.
6. As soon as the graph relating to a specific aspect has been completed, ask participants to ***identify*** from the graph the areas in which the group as a whole seems most savvy and most vulnerable, and to speculate on the possible **reasons** for the strengths and vulnerabilities.
7. Do ***not*** discuss the *third column* of the interview questionnaire yet. This will be done during the course of the workshop.
8. Wrap up the session by telling participants that each of the subsequent sessions will deal with a different digital citizenship feature and that they will periodically be coming back to the graph to further evaluate the cyber savviness of their interviewee.

Note

This activity could also be used to facilitate workshops for educators and learners in the senior phase of secondary schools but for younger learners the ice-breaker activities in the manuals for primary and secondary school teachers and learners would be more appropriate.

UNIT 2: DIGITAL/CYBER SECURITY

SESSION 1  30 minutes

Building on the analogy of the digital world as a parallel to the real / physical world in which we all live, remind participants that to be a citizen of any world – physical or virtual - implies that one has to accept the responsibilities associated with citizenship. One of these responsibilities is to learn the language of the country where one is a citizen - in the case of digital citizenship that would be the jargon dealt with in the previous session. Another responsibility is to obey the rules/laws of the country concerned to ensure that everything runs smoothly – that there are no security risks - and that citizens feel safe.

Tell participants that the focus of this session is on *digital/cyber* security. Ask them what it is that gives them a sense of security in their homes, workplace, community, or country. Use their responses as basis for a comparison or analogy of steps ordinary and digital citizens respectively could take to make their habitats/worlds more secure and/or read and discuss the *Introduction* to Session 2 in the Participant's Activity Book as an example of such an analogy.

Having sensitized participants to the importance of cyber security, refer them to Activity 3 in the Participant's Activity Book.

Activity 3: Risk Management

The aim of the first activity of this session is to sensitize participants to the risks/threats associated with digital travel – in cyber space - and to share with them the advice of experts on what they could do to minimize the risks.

The role of the facilitator is, firstly, to guide participants through the activity, and, secondly to ensure that, by the end of the session, all participants have filled in the appropriate risk management strategies in the last column of the table. Facilitators could do this by either following the steps outlined below or by using other methods deemed more appropriate to the context and target group concerned.

Step 1

Read the introduction to the activity out loud, taking care to explain anything that you think might not be clear to the participants. Allow comments and questions from participants if there are indications that they want to do this.

Step 2

Divide participants into 2 equally-sized groups and allocate a table to each group.

NB!!!

I. *The activity should ideally be a group activity but if you are running out of time, you could change it to a **plenary discussion**. In this case you need not divide participants into groups. Instead, display (on a PP slide or a flip chart) the completed tables – as they appear in the **Facilitator's Guide** – and let participants fill in the missing information as you talk them through the table content.*

II. *The last column of the tables in the Participant's' Activity Book is blank; only the tables in the Facilitator's Guide have the answers already filled in.*

Step 3

Tell participants to carefully read the instructions and the notes following the table allocated to their group and encourage them to ask for clarification if they are unsure about anything.

Step 4

Refer them to the safety tips following the table allocated to their group if they struggle to complete the empty column.

Step 5

Tell them how much time they have to complete this activity.

Table 1: Mobile Protection[2]

Risk	***Risk management***	***Risk management questions***	***Risk management answers***
Malware infection and attacks	Install reputable security software as protection	*How do I do this?*	Download anything from secure websites, e.g. McAfee Mobile Security, which also has an anti-theft option. Download from *https://www.mcafeemobilesecurity.com*
	Avoid downloading apps from untested sites.	*How would you know whether or not an app store is reputable?*	Review the terms and conditions of use. When installing apps to determine if you are giving access to information you don't want to share.
Un-desirable access to your private or personal informa-tion	Explore and customize settings on your phone.	*How would you do this?*	Select strict options in settings for location reporting, app installation, tracking online behaviour and Wi-Fi networking.
	Lock your phone with a pin code or pattern lock.	*Why should one do this?*	This ensures that even if your phone is stolen, the thief cannot immediately access information on it. You can then use security software to *remotely* 'wipe off' or delete information from your phone.

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

Access to your hone	Do not use public Wi-Fi to shop or access e-mails. Rather use you network provider connection.	*Why not?*	Public Wi-Fi hot spots can give hackers easy access to your phone and, by implication, to your accounts and emails.

Table 2: Computer Protection[3]

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?	Opt for automatic updating.
	Install legitimate anti-virus & anti-spyware programmes & never turn off your firewall	Where do I get these?	Buy from a store or download from reputable web-site.
	Use flash drives / memory sticks cautiously	Why?	They could carry viruses to your computer – scan them before opening
Restricting access to your computer	Create different, strong passwords for different sites and keep them secret.	What does a strong password look like?	Mix letters, symbols and numbers

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

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?	Avoid pop-ups of any kind – they are dangerous. Press CTRL + F4 or, if that doesn't work, Alt + F4 to remove them.
			Confirm authenticity with sender and/or look for sites preceded by http(s) or a padlock beside the address

Note

This activity is too difficult for school children and should be replaced by an activity that is more appropriate to the age and cognitive level of the children concerned. See relevant learner and/or teacher manual for examples of appropriate activities. Also adjust the debriefing session in terms of the activity chosen.

Debriefing

If you opted for the group activity ask participants whether they found it difficult or easy and let them share their frustrations if any. Then display your tables, with the answers and ask participants to compare your answers with theirs, to make adjustments if they feel these are needed, and/or to share additional strategies that have worked for them in the past.

SESSION 2

 25 minutes

Display the case study that follows on a Power Point (PP) slide and ask participants to use the insights they acquired from completing and discussing the tables to indicate which crime was committed, to suggest ways in which the victim could have protected herself from hackers before this incident happened, and to recommend ways in which she could prevent this from happening again.

Accept any contributions that indicate participants' understanding of digital/cyber security and ask for comments on any responses that seem uninformed.

Cyber Security Case Study

Lorenza Bacino, a newspaper journalist, discovered that her e-mail was hacked when it started sending spam to all her contacts. Realizing that her password was laughably easy she decided to change it.

A week later she found that she was locked out of her e-mail account altogether. She had to contact her provider to get back into her own account. She then changed the passwords on all her accounts thinking that was the end of it.

A few weeks later she received a clothing catalogue with a letter saying that about R10 000 would be deducted from her credit card in the next seven days following her successful purchases. She quickly called the company, which agreed to cancel the order.

A few months later a phone company contacted her, saying that someone had tried to set up an account in her name. The company had smelled a rat when the address that was provided didn't match up with some of the credit card details.

Lorenza is now constantly on guard because she doesn't know what might happen next!

Note

This case study is not appropriate for school children. Having discussed various threats to digital devices with the children, consider using the case study overleaf, or consult the relevant Teacher or Learner Manual for more appropriate case studies.

Cyber security case study for school children

Grace celebrated her 13th birthday two days ago. She was delighted to find that someone had sent her a birthday card. Although she did not know who sent the card she downloaded it anyway. Since then she has been unable to find some files that she had stored on her computer. She knows that she did not delete them.

Questions

1. What do you think happened to Grace's files?
2. What should she not have done? Why not?
3. What can she do to fix the problem?
4. What could she do to prevent the same thing from happening again in future?

On completion of the case study discussion ask participants to turn back to the *Cyber Savvy Questionnaire,* to read the answers their interviewee gave to the sections dealing with cyber security, and then, on the basis of what they now know about this aspect, to answer Questions 1 and 2 in the spaces provided below the questionnaire.

End the session by telling participants that the next session will focus on ***Digital/Cyber Safety.*** Explain that the term refers to Internet activities aimed at doing harm to ICT users rather than to their devices, as well as the steps users could take to protect themselves against these risks.

UNIT 3: DIGITAL/CYBER SAFETY

SESSION 1  30 minutes

In this unit the facilitator has to awaken participants' critical awareness of the risks they face when they engage with others on social networks. It is a good idea, therefore, to address the knowledge issues during a plenary session with a view to ensuring that participants will be equipped with the knowledge and understanding they would need to analyze the case studies that appear later on in the session.

It might be a good idea to start the plenary session with a discussion of the increased use of social media sites and apps *(applications)* to communicate with friends, join groups based on common interests, share articles, photos and other personal information, buy or sell something, et cetera.

Allow participants to briefly talk about their favourite social media site/s, the reasons for their preference/s and the purpose/s for which they use these sites in particular – as part of the plenary session or in participant groups. Wrap up the discussion by asking participants to quietly read the *Introduction* to Session 3 in their Activity Books.

Once everybody has finished reading the Introduction, ask participants:

- For their comments on the reading content
- Whether they can think of any other reasons why social media users would resort to this kind of verbal "warfare"
- To indicate, by a show of hands, how many of them have ever had a particularly "pleasant" or "unpleasant" encounter with someone on a social media site. If unpleasant, how did they handle it?
- Give one or two participants the opportunity of sharing this with the target group as a whole. Do not comment on what they say,

and do not encourage a discussion of the experience. Just tell them that such encounters will be discussed in a subsequent session.

SESSION 2  20 minutes

Following the plenary discussion, refer participants to *Table 3* in their Activity Books. Point out that the focus of the previous unit - on ways of protecting one's ICT *devices* against threats – has shifted in this unit to ways in which ICT users could, and should, protect *themselves* from being harmed by those they encounter on social media sites.

Talk participants through the table, dealing with each risk in turn by, for example, clarifying terms which may be unfamiliar *(use the Recource Book as a teaching aid but explain terms in ways that are appropriate to the target group concerned).*

Explain and, *where appropriate*, use your laptop to demonstrate and project on a screen ***(show and tell, in other words)*** how the risk management activities described in Column 4 of the Table could be executed.

Table 3: Self-protection

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

SESSION 3

35 minutes

Follow the presentation of the table with a discussion of a ***Prohibitions List*** *(Appendix 1 in participants' Activity Books).* This list reflects the views of cyber security experts on cyber activities/actions that should be avoided at all cost if one wants to stay safe.

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 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 stop this, is to ignore their messages, "block" the contact or to change 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 have 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.

In working through this list ask participants to indicate ***what harm*** they think could come to them if they **did** the things prohibited in this list. If participants know of people who have come to harm because they did some of the things prohibited in the list, give them the opportunity of sharing these, but keep it short.

Having ensured that they are fully aware of the risks posed by social media sites and have a sense of the steps they could take to protect themselves against these, let participants do ***Activity 4*** in their Activity Books.

SESSION 4  20 minutes

Activity 4: Playing it safe!

In this activity participants are given the opportunity of applying their knowledge of digital/cyber safety to a number of imaginary situations *(see Table 4)* - where someone's safety might have been at risk.

Participants have 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)

Tell participants that they can decide whether they want to do this activity in groups, in pairs, or on their own. All these options are allowed provided that they finish the activity in the time allocated to it.

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 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 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 will 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 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.	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 Facilitator's Guide only.*

Debriefing

Either display, with the correct "matches", the table on a power point slide or simply share them orally with participants once they have completed their own matching process. Give them time to adjust their responses before referring them to Activity 5 in their Activity Books.

Conclude this session by telling participants that the next session is devoted to the reading of imaginary scenarios similar to ones they might face in the real world. Ask them to use the insights they have gained thus far in deciding how they would have reacted to the threats described in the scenarios. Then refer them to Activity 5 in their Activity Books.

SESSION 5  30 minutes

Activity 5: Cyber safety case studies

Divide participants into 6 (six) groups.

Allocate the first scenario to Groups 1 and 2, the second scenario to Groups 3 and 4, and the third scenario to Groups 5 and 6.

Tell them that the purpose of this activity is to see whether they can apply what they have learnt about the safe and responsible use of social media in the analysis of a case study. Briefly explain how they should go about "analyzing" a case – read, discuss/debate with reference to what they learnt, decide on the most appropriate response, and then write it down.

Tell them how much time they have to complete the activity and let them start.

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?*
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 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 should she 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 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 started to win many of his role-playing bouts. After a while he became so emotionally attached to his gaming avatar and to his ever increasing scores that he spent longer and longer hours hooked to the screen.

After a while he started joining online gaming groups. Their admiration when he told them about his high scores 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 Peter so that they could work out a solution. Because Thomas now feels very alone – Peter being the only "friend" he has left – he is tempted to do as Peter asks but something somewhere in 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 rules in the ***Prohibitions List*** did Thomas ignore?
2. Which signs were there that his gaming was having a negative effect on his personality?
3. Why, do you think, was he particularly 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 adults use in protecting children against gaming and other cyber addictions?

Answer

There are no correct of incorrect answers here. What you want is for participants 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 classrooms.

Ask participants what steps they think they, as parents, school principals and classroom teachers, could take to prevent the children for whom they are responsible against this kind of addiction.

Debriefing

Ask the different groups responsible to share their responses to the scenarios allocated to them during a plenary session. If the responses of two groups dealing with the same topic differ radically ask participants to (a) reflect on the possible reasons for the differences and (b) to reach a consensus about the most appropriate response. If responses are completely off track, share with them the responses provided in your Facilitator's Guide, otherwise commend them for sharing their insights with all present.

Then spend some time talking about ***cyber addiction*** – what it is, what effect it could have not only on the person concerned but also on those close to him/her, and what it has to do with cyber safety. You might have to surf the Internet for information on this prior to the workshop.

Do the same with cyber bullying (*see Recource Book for information and/or surf the Internet for articles dealing with this problem).*

Alternatively, and if there is time, you could give one group of participants the opportunity of surfing the Net for information on cyberbullying and another group to surf the Net for information on cyber addiction.

Wrap up the session by asking participants to return to their ***Cyber Savvy Questionnaire***, read Column 3 of the questions dealing with Digital/Cyber Safety, and answer in writing, Questions 3 and 4 following the questionnaire.

UNIT 4: DIGITAL / CYBER CRIME

The purpose of this unit is to create in participants an awareness of the legal consequences of information-related crimes, especially those perpetrated by means of electronic media. The facilitator's role is to sensitize participants to the existence and danger of internet activities that are regarded as criminal, to give them a basic knowledge of legislation related to information-related crimes, and to develop in them a commitment not to engage in such activities themselves.

SESSION 1  30 minutes

The focus of this session is to introduce participants to the notion of cyber legislation. The steps described below might provide you, the facilitator, with some ideas of how to do this.

Step 1

Start the session by asking participants how they would explain to someone else what they mean when they use the word, ***crime,*** or the phrase, ***criminal activity***. Ask them to illustrate their explanations with an *example* of some or other crime.

Step 2

Using participants' responses in Step 1, facilitate a plenary discussion on ***cyber crime*** – which activities they think would qualify, why, what the

impact of these 'crimes' are on those at the receiving end, what, if any, legal consequences there should be.

Step 3

Give participants some idea of existing legislation on cyber crimes in other countries *(surf the Internet for information)* and ask them about such legislation, or the need for it, in their own countries.

Step 4

Refer participants to Table 5, which gives 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: Cyber crime and its legal consequences

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 1 takh fine

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

Step 5

If workshop participants are based in South Africa, give them a sense of the status quo here with regard to cyber crime by naming and indicating the purpose of each of the following pieces of legislation. You could even briefly summarize each of these pieces of legislation if you think that this would be useful.

- The ***Protection of Information Bill***
- The ***Act on Electronic Communication and Transactions***
- 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).***

(If you do not know what these Acts says you would have to look them up on the Internet.)

Display a summary of the ***Protection of Harassment Act*** (see the text box that follows), indicating its significance in relation to cyber safety issues discussed in the preceding session. Emphasize the key features of this Act, namely its *definition* of harassment, its potential to *protect* teenagers against cyber bullying, and the fact that it provides victims of cyber bullying with an inexpensive *civil recourse* aimed at stopping most forms of harassment, also e-harassment. Ask participants to relate what is in this Act to the cyber safety readings and scenarios discussed in the previous session.

Wrap up the discussion by indicating that, notwithstanding the existence of these Acts, there is currently no South African law dealing specifically with *social media transgressions*. Because of this, legal action taken against transgressors is informed by the South African Constitution and the common laws principles stipulated in the *Employment Act, the Consumer*

Act, as well as those of the *Intellectual Property Act,* and the *Protection of Harassment Act (2013)* mentioned earlier.

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

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

According to the same Act:

- A person or persons to whom these messages are sent should immediately apply for a protection order from a clerk of court.
- The clerk of court will then issue a restriction order on 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.

Note

i. The discussion of this particular Act would have to be replaced by a discussion of Acts particular to other countries if workshops on this topic are conducted there.

ii. The discussion as it is here could take place with secondary school learners as well. If used for primary school learners, the information in the text box might have to be simplified to a level appropriate to learners' language and/or reading ability.

SESSION 2  90 minutes

Tell participants that the links between *Constitutional values* and *Common Law principles* in the RSA are illustrated in five information-related cases (brought to the CCMA in the RSA), which they are now going to discuss in smaller groups.

Activity 6: Crime or not?

Divide participants into ***4 groups*** and then refer them to *Activity 6* in their Activity Books.

Allocate one of the four case studies in their Activity Books *(see below*) to each group, ask them to carefully read and follow the instructions, and give them the time allocation for this activity.

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 policy in your school or place of work? Give reasons for your answer.*

Case Study Answers

The CCMA supported the dismissal, arguing that Facebook *privacy settings allowed anybody who wanted to post comments to do so unless they were deliberately blocked. Moreover, employers were entitled to intercept posts in terms of RICA (Regulation of Interception of Communication and provision of Communication-related Information (Act 70 of 2002).*

The answers to Questions 2, 3 and 4 will have to be debated by participants during the plenary session.

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.

The employee appealed to the CCMA, claiming that he simply exercised his constitutional right to freedom of speech.

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 policy in your school or place of work? Give reasons for your answer.*

Case Study Answers

The CCMA found that the employee was fairly dismissed for two reasons: first, the allegations were unfounded because he did not and could not provide any evidence of his claims and, secondly, there were no internal deliberations regarding these claims prior to the face-book posting.

The answers to Questions 2, 3 and 4 will have to be debated by participants during the plenary session.

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

Case Study Answers

The CCMA found that the employer's access to the employee's account had initially been gained accidentally but that subsequent access was intentional. The dismissal was regarded as procedurally and substantially unfair and had to be overturned.

The answers to Questions 2, 3 and 4 will have to be debated by participants during the plenary session.

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 policy in your school or place of work? Give reasons for your answer.*

Case Study Answers

According to a cyber specialist the group could be prosecuted in the RSA in terms of the Act on Electronic Communication and Transactions but because the entertainer concerned had not lost any money as a result of the attack and his web-site had not been damaged, there is little chance that his law suit will succeed.

The answers to Questions 2 to 5 will have to be debated by participants during the plenary session.

Debriefing

Give the rapporteur of each group the opportunity of presenting his/her group's case study to the gathering during the plenary session, indicating how the group responded to each question, and allowing the rest of the gathering to comment, or add to these responses.

After each presentation share the conclusions/judgments passed by the CCMA with participants, inviting comments on these if they seem keen to comment.

Note

i. The actual judgments appear in the Facilitator's Guide only and therefore have to be shared with participants.

ii. These cases are specific to South Africa. If these workshops are facilitated in other countries it would be necessary for facilitators to replace them with cases relevant to the country concerned or to follow the discussion of one or more of these cases with a discussion of cases known to workshop participants in the countries concerned.

UNIT 5: INFORMATION ETHICS

Introduce the theme by telling participants that, whereas the preceding sessions focused on ways in which one could protect oneself against *cyber risks created by other internet users,* the focus of the sessions that follow is on the way all Internet users should behave and why.

Spend some time to facilitate a discussion on *etiquette (manners) in general,* then ask participants for their views on the need for, and nature of, cyber manners, or *Netiquette.*

Link good manners and behaviour to good / sound values / morals. Tell participants that the purpose of this unit is to sensitize them to values and morals assosiated with internet behaviour, develop an awareness of and a commitment to information ethics. Key to achieving this purpose is to reach consensus on the meaning attached to *information ethics* as a concept, hence concept clarification is the focus of the first session of this unit.

SESSION 1

30 minutes

Use participant's views on Netiquette (i.e. Internet etiquette) as basis for a plenary brainstorming session which focuses alternately on the meaning of the concepts, "information", "ethics", and "information ethics" *(see or read and discuss the Introduction to the Participant's Activity Book, and/or use the definitions of these terms in the Concept Book as examples*). Take note of all contributions but do not accept any definitions as definitive. Instead, tell participants that you are going to ask them to write their own definitions of these terms after they have had the opportunity to discuss various aspects of information ethics.

SESSION 2  45 minutes

On completion of the plenary discussion, refer participants to the fable *(The Frog and the Scorpion)* in their Activity Books, read it out - as dramatically as you can - asking them to follow your reading.

Once you have read it, either facilitate a discussion on or allow groups to discuss values as the foundation of ethical behaviour, making it a point to let participants reflect on the function/s served by values, differences in African and other value systems, and the impact they think electronic technology, especially information *communications* technology, has had on people's traditional values.

You could, for example, ask some or all of the questions following the fable as basis for either a plenary or group discussion.

Wrap up the discussion by asking participants – or groups of participants - for a general indication of the insights they gained about the influence that values and laws play in controlling or modifying people's behaviour. Guide them to the realization that the fable raises questions about values, morality, ethical conduct, power and control, and the influence of our behaviour on others; that the lesson in the fable is that we should be aware of the impact that our behaviour has on ourselves and others. Sometimes the consequences are good; sometimes, as in the fable, they are bad. This is true in real life situations as well as in the virtual, cyber world. The fable also seems to suggest that fear – even of death – is not always enough to stop people from doing harm to others, and to themselves. What does this imply about the power of the law in changing people's behaviour?

SESSION 3  30 minutes

Using the preceding discussion as basis, ask participants to reflect on the implications that the lessons of the fable have for real life situations. Do these lessons suggest that laws – which are aimed at the external control of people's behaviour – are not in themselves enough to keep a nation or community in line? Suggest to them that something else might be required, something that drives people internally to behave in ways that take cognizance of other people's needs, vulnerabilities and living spaces. That "something" is called a moral/ethical code.

Indicate that, while laws are imposed from the outside, a moral/ethical code is usually much more personal, a set of values that evolves from the inside out, over time, something that serves as basis and/or frame of reference for personal or organizational behaviour and decision-making. An ethical person / organization, for example, is one that consistently behaves in accordance with his/her/its *internal* code, even if doing so is risky or contrary to what is popular and/or regarded as the "norm".

If participants are South Africans, highlight the fact that, although the RSA Constitution is the supreme law of the country, it is also in a sense a social contract or code of ethics. Illustrate/substantiate your comment by displaying a PP slide of the founding values of the Constitution, indicating that all these values indicate the need for *"respect".*

Follow this slide with one which lists all the human rights in the Constitution that relate to the use of information and/or information communications technology. With this slide as frame of reference, facilitate a discussion on the values underpinning each right and what it is that should be *"respected"* in terms of the right concerned. Emphasize the notion that the protection of one person's right is another person's responsibility. In other words, *if I do not respect your rights, I cannot*

expect other people to respect mine. To emphasize this point, read, and invite comment on, the extract in the text box below.

> ***Yes, but why me?***
>
> *First they came for the Jews*
> *And I did not speak out –*
> *Because I was not a Jew*
> *Then they came for the communists*
> *And I did not speak out -*
> *Because I was not a communist*
> *Then they came for the trade unionists*
> *And I did not speak out –*
> *Because I was not a trade unionist*
> *Then they came for me – and there was no one left to speak out for me*

Conclude the discussion by asking participants to think of the implications that each of the rights mentioned has for the way in which information is created, accessed, and disseminated. Record the implications on a flip chart and post it on the wall for reference during the activity that follows.

Note:

For workshops in other countries their Constitutions or social contracts would have to serve as basis for the ensuing discussion.

SESSION 4  45 minutes

Refer participants to Activity 7 in their Activity Books, indicating that its purpose is to give them the opportunity of combining their knowledge and understanding of cyber legislation and information ethics into a policy or code of conduct for their community, place of work, classroom or school.

Activity 7: Information ethics codes

Divide participants into groups consisting of people who do similar work, live in the same community, teach at the same school, or visit the same Internet Café, for example.

Tell participants that each group has to:

1. Start the activity by discussing the values they think should inform the use of the Internet *(or e-learning at schools)* and the human rights that should be actively protected in these situations.

2. Secondly, based on the outcome of the group discussion, each group should perform the task applicable to its group, namely:

    i. *Groups consisting of classroom teachers only should, as a group, draw up a code of conduct for the use of information and ICT in their classrooms. The rules included in the code should reflect a commitment to values as well as respect for other ICT users' human rights.*

    ii. *School principal groups should, as a group, draw up a code of conduct for the use of information and ICT as a means of school management. The rules included in the code should*

reflect a commitment to values as well as respect for other users' human rights.

iii. Internet users could draw up a code of conduct for the use of the NET cafés

3. On completion of its ***Information Ethics Code of Conduct*** each group should post it on the wall, for 'public scrutiny'.

4. Once all the posters are up, give the different groups the opportunity of doing a *gallery walk* - moving from one poster to the next - assessing each code in terms of the extent to which they think it would promote the responsible and ethical use of information and information communications technology in classrooms and/or schools, internet cafes or places of work, whichever one is relevant. Indicate that they are allowed to write comments on these posters, provided that the comments are constructive and/or contribute to the improvement of the poster concerned.

Note

This activity was originally designed for educators. It may, therefore, not be applicable in generic workshops where participants represent different sectors of society. Facilitators conducting these workshops would have to adjust the educator activity to the needs and contexts of the participants attending their workshops.

Debriefing

Give participants the opportunity of commenting on the value of this exercise for their particular context and sharing what they, as individuals, learnt from drawing up and assessing different codes of conduct.

SESSION 5  90 minutes

Start this session by asking participants how they would now define ethics considering the activities they have done so far in this session. Do not comment on any views – just listen. Then, read with them what philosophers have to say about the nature and value of ethics *(see Reading/Text in Participant's Activity Book).*

Ask participants whether they think conflicts could be erased if the moral code of a nation and the legislation written to govern the people are perfectly aligned? Allow some opinions, then indicate that, while this should be the case, it seldom is. Substantiate your claim with reference to the disjuncture that exists between the RSA Constitution[4] (which prohibits discrimination against others – on the basis of race, gender, disability, language, religion) – and the increasing number of newspaper reports on people discriminating against one another. Ask them why they think this is the case. Are there groups in this country whose moral or religious code tells them that discrimination is OK?

Refer to the fact that the Constitution also stipulates that all humans have the "right to life". By implication, no one may take another's life, not even if the person committed a murder or some other horrendous crime. Not even the courts may impose a death sentence. Yet the media are full of murder, rape and hijacking reports influencing ordinary people to call for a return of capital punishment. What does all of this say about the morality / ethos of our nation?

Ask participants whether it is possible that the values enshrined in the Constitution do not reflect the values that the citizens of the country hold

[4] Once again, the reference to the RSA Constitution is context-specific and will have to be changed if workshops are conducted in other countries.

dear? If this is the case, a person who transgresses the law could, for example, be doing so because the values informing a particular law is the direct opposite of his/her moral code.

Suggest that, by remaining true to his/her own code/ethic regardless of the legal consequences, this person retains his/her integrity because s/he has stayed true to his/her own internal compass. A person who finds himself in this kind of Catch 22 situation experiences a moral dilemma because s/he is caught in a situation which requires her/him make a choice between two things – one that is either legally/morally right and one that seems to be circumstantial (that is, dictated by the circumstances in which the person finds her/himself).

Refer to some of the many examples of moral dilemmas in the history of the world.

- Think of Thomas More, a British scholar and confidant of King Henry IV, who refused to accept the king's decision to divorce his wife. More argued that divorce was against the doctrine of the Catholic Church even though the king's wife could not give him an heir. Because More refused to change his opinion he lost all his property and was publically beheaded.
- Think of the French Resistance Movement during World War II in which ordinary French citizens risked their lives to smuggle Jews out of Germany through underground tunnels and dark forests to prevent them from dying in gas chambers or being buried in mass graves.
- Think of Nelson Mandela, who refused to submit to apartheid laws even though it meant that he would spend most of his life an exile in Robben Island prison.
- Think of the UCT professor who 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.

Tell participants that examples of moral dilemmas also occur in the sphere of Information and Information Communications Technology. The most famous of these is the one in which an American citizen who 'cracked' the FBI network and 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.

Ask participants whether they know his name and/or can 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? Give reasons for your answer.

Display *(on a Power Point slide),* and/or read aloud, the following moral dilemma scenario.

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 does, however, perform abortions. Susan knew this but was not worried because the abortions would be done by doctors, not by nurses.

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 such an 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.

Ask participants what they think will happen to Susan because she refused? In other words, what would the consequences of her action be?

Then ask them how they 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?

Finally, ask participants what they would have done if they were in Susan's position and why they would do so.

Now tell them that the next activity will present them with possible moral dilemmas in the sphere of information ethics.

Activity 8: Information ethics dilemmas

Divide the class into groups, ensuring that persons who might have the same value orientations or agendas are in the same group *(e.g. classroom teachers and school principals separate, or community leaders and community members separate) because their perspectives and power positions are different.*

Refer participants to Activity 8, remind them again what an information ethics dilemma is, and then allocate a specific dilemma to each group.

Read through the instructions with participants before they commence with the activity, emphasizing that the first part of the activity is *individual* – this is very important since it gives each person the chance of first reflecting on his/her personal values and then using these as basis for determining how they fit in or are in conflict with the values of other group members.

Debriefing

When all the groups have completed the activity, give each of the rapporteurs the opportunity of presenting their group dilemma, questions and responses in a plenary session.

When they have all had a chance to present refer participants back to the ***Cyber Savvy Questionnaire***. Ask them to read what is written in Column 3 on information ethics matters, and then to answer the remaining questions following the questionnaire in writing.

Thank participants for their participation in the workshop and wish them luck in their attempts to use e-learning as a means of improving learner understanding, academic performance and ethical behaviour.

Conclude the session and the workshop by asking participants to complete a workshop evaluation form prepared in advance. Alternatively to critically reflect on the workshop in terms of its having added value to their knowledge and understanding of the themes covered and/or better equipped them to deal with possible e-learning issues in their classes and schools.

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 261667

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

Universiteit van Pretoria
University of Pretoria
Yunibesithi ya Pretoria

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie

basic education
Department:
Basic Education
REPUBLIC OF SOUTH AFRICA

intel® Education

African Centre of Excellence for Information Ethics