Digital Wellness Programme

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

PRIMARY SCHOOL TEACHERS' MANUAL

Digital Wellness Programme

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

PRIMARY SCHOOL TEACHER'S 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

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

Digital Wellness Programme - PRIMARY SCHOOL TEACHER'S MANUAL

October 2015

ISBN: 978-1-928261-70-4

Editors
Beverley Malan
Coetzee Bester

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

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

TABLE OF CONTENTS

FOREWORD IV

OVERVIEW OF TEACHING AND LEARNING CONTENT 1

THEME 1: LEARNING THE LINGO 3

THEME 2: SAFETY FIRST 8

THEME 3: SHARING AND CARING 22

MCAFEE MATERIAL (8 PAGES) 31

BIBLIOGRAPHY 33

FOREWORD

All of us today have a parallel existence. This shows up as our online identity on social media sites, gaming portals, discussions forums, learning communities and even personal blogs and websites. In an ever-connected world, using the Internet every day has become a need rather than a choice. People use it not only for work purposes but also to download information, music, videos, movies, and games or to link up with people all over the world for all kinds of reasons.

For many children a world without mobile phones is unthinkable and unimaginable. Research conducted by the Kaiser Foundation[1] in the United States of America found that 85% of American children between 15 and 18 years of age, 69% of children between 11 and 13, and 31% of children between 8 and 10 own cell phones. The researchers also found that the children who were surveyed spent on average over half an hour talking on the phone but send more than 100 text messages *every day* – that is more than 3,000 per month.

Looking at these figures, which measured in terms of the speed at which technology changes, are **old** *(the research was conducted in 2010),* one has to wonder how many *What's Apps* (a feature not yet available at the time of the research) children in these age groups send and receive every day. The most disturbing finding of the Kaiser research was, however, that relatively few of the children surveyed have established rules around mobile phone use, suggesting that they may not be aware of the health, emotional and psychological risks associated with what can at best be called *cell phone addiction*.

The first aim of the Manual is to sensitize educators (parents and teachers) to the risks associated with the use of the Internet so that they can take

[1] Generation M2 Report, Kaiser Foundation, October 2010, cited by Microsoft in their tips for teaching kids Mobile Phone Safety.

the necessary steps to ensure the safety of the children in their care when they are on their smart phones or computers. Microsoft urges parents to control their children's access to and use of the Internet in ways that would make the children feel safe rather than alienated.

The advice Microsoft gives parents is simple and straightforward:

- Encourage your children to keep their pin codes and passwords safe and secret.

- Help your children use social networking safely and responsibly by communicating with them about their experiences, establishing Internet rules, ensuring that they abide by age limits and restrictions, and educating yourself about all this new technology.

- Be absolutely clear about what your children may and may not do on their phones and computers but give them the reasons for blocking them from certain sites and/or limiting their talk time on their phones or computers.

- Filter or block websites and content in terms of what is appropriate to your child's age and maturity.

- Use GPS cautiously – if you are using a family location service to monitor your children's whereabouts, make sure others cannot locate them. Otherwise consider disabling the location feature on your child's phone or, at least, turn it off on the phone's camera.

- Manage your child's Internet and phone contacts even if it means that you might have to block certain callers and/or restrict your child's calls to approved numbers only.

- Teach your children never to meet anyone in person that they have communicated with online only and warn them about expressing emotions and sharing secrets with strangers online.

- Be wary of providing identifiable information in your child's profile.

- If your children blog, make sure they do not reveal too much – establish rules for on line use, screen what your children plan to post before they post it, evaluate the blogging service, and save or review the web address of your child's blog.

- Listen to your children. Ask them to talk to you about their lives. Sit with younger children while they play and explore online. Regularly ask your children to show you around – what websites they visit, where they hang out, whom with and how they talk to each other. Only if you do this will you be able to detect whether or not your child is being bullied, harassed or stalked on the Internet so that you can stop it in its tracks.

- Watch for signs of online cruelty towards and by your children. If your children no longer wants to go to school or play on their computer there is a problem. Find out what it is and solve it with them.

- Make sure your children trust you and then live up to that trust.

- Teach your children about online bullying. Ask them to report bullying to you. Promise unconditional support. Reassure them that you won't curtail phone, gaming or computer privileges because they are being victimized."

The second, and equally important, aim of this manual is to ensure that primary school learners are alerted to the dangers and risks associated

with the unsafe use of cell phones and computers. To this purpose the Teacher's Manual covesr the knowledge, skills, attitudes and values that learners need to survive and thrive in the virtual world of technology – in other words how to safeguard themselves, their phones and their computers against cyberattacks, and what it means to be a responsible, ethical user of digital technology.

Lastly, please note that this programme also includes a workbook for primary school learners. That workbook includes (i) various practical activities that were designed by McAfee ® and Intel Digital Security® to assist young people in better understanding and awareness of digital safety, and (ii) notes and guidelines to parents of these learners. Please use every opportunity to involve the parents in growing with their children on this important journey of becoming knowledgeable on matters of digital safety. We trust that many of your learners' parents will already be very knowledgeable in this field. Please include them in the development of your material and if you develop new material please share it with us and as many others as possible.

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

OVERVIEW OF TEACHING AND LEARNING CONTENT

The content covered in the Teacher's Manual is divided into **three** themes, namely:

1. ***Learning the Lingo*** – The focus of this theme is to teach learners the key concepts and terms associated with the use of information communications technologies like mobile phones and computers.
2. ***Safety First*** – In this theme the focus is on two things, namely the risks/threats associated with the use of mobile phones and computers, and the steps learners and teachers could take to protect themselves, their phones and their computers against these.
3. ***Sharing and caring*** – Whereas the focus of Themes 2 and 3 is on potential threats against the users of mobile phones and computers, this theme focuses on the ways users should behave – what they should and should not do – to ensure that they do not cause harm to others.

Each theme is dealt with in more or less the same manner, starting with a short introduction to the theme – usually in the form of ***whole class teaching*** – and followed by one or ***more learning activities*** – some individual, some in pairs, some in small groups, and some in whole class discussions and/or debates. The length of these sessions is not stipulated because it will depend on the reading and comprehension levels of the learners concerned. Each teacher will therefore have to decide for him/herself how much time to allocate to each activity.

Given that the age range of children targeted for training is between 6 and 12, the emphasis is on both active and rote learning. Both types of learning can be facilitated by engaging children in activities which involve *association*, *sensory stimulation*, and *identification*. Put differently, activities for children in this age range tend to be more effective if what

they have to learn is presented and/or reinforced by means of ***pictures*** *(photos, drawings, cartoons and comic strips),* ***songs and/or rhymes*** *(rhythm, movement and sound),* ***stories*** *(character identification and role modeling),* and ***puzzles*** *(tactile & visual stimulation).* The use of color and competition in all of these also contribute to quicker and more lasting learning. Which games, drawings, songs, stories or cartoons are used is immaterial as long as they are purposeful, that is, as long as they contribute to the achievement of the learning outcomes specified in the manual.

The activities included in this manual should be regarded as examples only: the idea is that each teacher – primary teachers being very creative – will ultimately design their own teaching and learning activities. Until that time, though, use the ideas in this manual in conjunction with the activities games in the Activities Book for Primary School Learners which is in included in your Resource Pack. If you have access to the Internet, you could also download the Printable Activities developed by McAfee Security Centre.

On completion of the activities in this Primary School Teacher's Manual, learners should:

- Know and be able to correctly use basic Internet jargon
- Know what the Internet benefits *and* risks are
- Know what to do if and when problems occur
- Have developed good digital habits

In addition to this Manual, you would have received a *Concept Book*, which consists mostly of definitions and explanations of acronyms and terms used in the digital world. We trust that you will find both books useful and enjoyable and that they will stimulate your own creative urges.

THEME 1: LEARNING THE LINGO

The focus of this theme is on helping young learners acquire the language of the digital world. There are various ways of doing this but all of them would involve at least:

(a) Teaching them the terms and concepts critical to an understanding of thematic issues

(b) A whole class discussion of thematic issues

(c) The consolidation / internalization of content covered by means of active learning / learner activities.

The order in which these take place would depend on the theme to be addressed, the teaching – learning context / situation, and the teachers and learners concerned. Teachers could, for example, decide to:

- Start the lesson by talking to learners about the theme that is the focus of a particular lesson, then teaching them the terms and concepts critical to an understanding of the theme, and then engaging them in activities that will help consolidate their knowledge and understanding of the terms, concepts and issues relevant to the theme, or
- First teach the terms and concepts before they introduce thematic content, or
- Start with a learner activity that will serve as springboard to the introduction of the terms, concepts or thematic content, or
- Integrate the teaching of terms and thematic content into learner activities.

It is our contention that it is the prerogative of the teacher concerned to make these kinds of decisions. It is they, and only they, who know exactly what the reading and comprehension levels of the learners in their classrooms are, and what would work best for them.

Please note that, although this is a theme in its own right, it does not mean that the theme should be covered in isolation from other themes. We suggest that this theme should be part of each of the other themes in that learners learn the lingo of the theme at the start of or during the course of the theme concerned.

Key Terms and Concepts

The alphabetical list of terms and concepts appearing in Table 1, which follows, are terms that we regard as critical to an understanding of digital wellness *(i.e. the safe, responsible and ethical use of information and digital technology).* It is, however, up to teachers not only to decide which of these terms to teach but also which ones they would like to add. For definitions and explanations of the terms and concepts included in our list, please refer to Section 2 of the Concept *Book*.

Table 1: Key Concepts

A Access Accessibility App Appropriate **B** Blocking Behaviour	**C** Cracking Censorship Cyber bullying Cyber predators Cyber savvy Cyber stalking **D** Digital citizen Digital technology Digital world	**E** E-mail Ethics Ethical behaviour E-waste **F** Facebook Firewall **H** Hacking **I** Identity theft Information Information ethics Information network	**M** Malware **P** Password Pin code Phishing Plagiarism Pop-up Pornography Predator Privacy **R** Responsibility Respect	**S** Social media Spyware **T** Trojan horse **V** Value/s Value system **W** WhatsApp Worm/s

The complexity of terms to be learnt will be determined by the reading and comprehension levels of the age group concerned. Teachers will have to decide which terms and concepts are appropriate and critical to the

mastery of content associated with the respective themes being dealt with at any particular time.

- If learners are in the ***Foundation Phase*** (Grades 1 to 3), for example, it would probably suffice to teach them terminology associated with the safe use of and potential risks to their phones.

- If, however, learners are in the ***Intermediate Phase*** (Grades 4 to 6), teachers might gradually have to increase the range and complexity of the terms and concepts associated with cell phones and would also have to include computer-related jargon.

In both instances the use of games and/or competitions which involve movement, color and shape is an enjoyable way of learning. Ironically, it also yields the most immediate and lasting results.

The activities described below could serve as examples of what could be done to teach learners the lingo but they are by no means the only ways of doing so. Please add to or replace them with activities that are familiar to you and which you know work in the acquisition of new and unfamiliar vocabulary.

Word Games

The following games are suitable for learners in both the Foundation and Intermediate school phases (i.e. learners between the ages of 6 and 12) but the way in which they are played may not be exactly the same.

1. Mix and Match

In this game the *terms/concepts* to be learnt have to be matched either with *pictures* (for learners in the Foundation Phase), *definitions* and/or *examples* (in the Intermediate Phase).

a) The usual, straightforward way of playing the game would be to list the terms in the left hand column and the pictures, definitions or examples in the right hand one, but in a different order to the

terms in the left hand column. Learners then have to match what is in the right hand column with the correct terms in the left hand column. Teachers could let them indicate the matches in different ways *(by means of numbers, letters, lines or colors)* to keep the game new and interesting.

b) A different, more tactile method, involves writing/pasting the terms, definitions, pictures or examples on flash cards, mix them all up, issue groups of learners with envelopes containing the 'mix' and letting groups compete with one another in terms of who could sort out the mix in the shortest time.

c) An even more exciting way is to structure the game as a 'card game'. Design the game in the same way as in (b) but instead of flashcards, use cards the same size as those used in card games. Playing the game would involve a *'dealer'* shuffling and randomly distributing *'cards'* to all the 'players'. Each player in turn would then put a card face up in the centre of the table. Each time that the card that is put down corresponds *(either in picture or word form)* to the one put down by the previous player the one whose card it is, shouts ***SNAP***. S/he then takes all the cards in the centre as his/her winnings. The winner of the card game would be the one that eventually holds all the cards.

2. Word Magic

There are a number of games in which learners have to search for missing words. We suggest that teachers regularly alternate the form in which the game is presented to ensure that learners do not become bored searching for, completing or 'creating' words.

a) A ***word search*** game that is familiar to most teachers is the one consisting of a square block containing separate letters. Whoever plays the game must do a horizontal, vertical, and diagonal search

for the words hidden in the square. The words they must look for could be listed on the side of or below the square, or learners could simply be instructed to find words associated to a particular theme or object (computer features, cyber crime, human rights, cyber risks, etc.).

b) ***Word completion*** exercises could take different forms. Learners could, for example, be asked to:
   - Fill in the missing word / term in a sentence, e.g. *A phone with Internet access is called a ----- phone.*
   - Complete the word by filling in the missing consonants, e.g. *Never share your p- n code or p- ss w-rd with anyone, not even your b- st fr—nd.*
   - Complete a definition, e.g. *We call someone a **hacker** if he or she* ----------

c) Other ***word exercises*** include
   - Underlining the correct word in a sentence, e.g. *Using a key / <u>password</u> stops other people from gaining access to your computer.*
   - Scrambling letters in a word and asking learners to unscramble them to form the right word*, e.g.*

     ivurs = virus morw = worm eshitc = ethics
   - ***Crossword puzzles***, in which learners have to use their knowledge of terms and concepts to complete the crossword.

THEME 2: SAFETY FIRST

Deal with this theme by asking learners to imagine what it was like before people had mobile phones and computers, something that would be very difficult for them to imagine!!! Ask them whether or not they think the way smart phones and computers changed the way people live and interact with one another is a good or bad thing and why they think so.

(You might want to make a pictorial collage of the changes and use this as a stimulus or a frame of reference for the discussion and/or invite one or more grandparents to come and tell learners what it was like in the past – when letters, post card, telegrams were used to communicate with others and when telephone lines were shared between a whole lot of people.)

Use learner responses to the discussion or narratives of the elderly as basis for a discussion of the opportunities created by these technologies – access to the Internet, for example, which allows them to travel where-ever they want, to communicate with strangers on the other side of the world, and to have immediate access to the latest information on just about any topic they want at any time of the day – all of this without their even having to leave their rooms.

Having highlighted the benefits, shift the focus to the threats associated with Internet travel. The use of analogies between physical space – a house, for example – and virtual space – the digital world - is quite effective in getting the message across provided it is pitched at the reading and comprehension level of the learners concerned. Ask learners, for example, whether their houses are safe. If they say 'yes' ask them what it is that makes it safe. If they say no, ask them what it is that makes their houses unsafe. Some of the answers you might get are that houses are protected / safeguarded by means of burglar bars, alarms, and/or the use of security services (like Chubb or ADT), CCTV cameras) or community policing.

(Once again the use of pictures / drawings / photos of houses with different kinds of security features could serve as a stimulus for discussion.)

Gradually lead learners to the realization that, just as we take steps to protect our physical spaces we should be taking steps to protect the virtual spaces we inhabit or visit. You could, for example, relate whatever they said about the safety of their home – a physical space – to safety in cyber space. If they said they lock their doors to keep burglars out, ask them how they can 'lock' their phones and computers to keep cyber criminals out. If they say they build walls around their houses to keep strangers away, ask them what they can do to keep strangers away from their e-mail and/or favourite social media sites, et cetera.

Point out that there are also thieves, burglars and other types of criminals in cyber space and that we should therefore make the effort of protecting our mobile phones, our computers, and ourselves against them. Tell them that this is what the next couple of lessons will focus on:

- Internet risks to their mobile phones, computers and their person
- The steps they could take to protect these devices against harm
- Things they could do to prevent 'unwelcome' visitors from entering their digital places and spaces
- Which things they should and should not do while talking on their phones or using their computers.

Computers AND smart phones, which are essentially mini-computers, 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. Unfortunately they also create opportunities for bullying and the posting of suggestive photos or videos *(sexting)* and *geotagging,* a feature which allows not only parents but also cyber predators to keep track of children's whereabouts.

In alerting children to the dangers of the Internet you should be careful not to turn them into timid, frightened human beings who are too afraid to use their phones or computers and/or of what MIGHT happen to them. Do not, therefore, spend the bulk of the lesson on the bad things that could happen to them: rather focus on what they could do to prevent any harm coming to them.

Start by telling them how to keep their devices safe. Help them *understand* ***why***[2]:

- They should share their phone number only with family and close friends. They should NOT put it on a social network page, use it to enter contests, or give it to just anyone who asks for it. *(Ask learners why not.)*
- They should lock their phones with a PATTERN LOCK or a ***secret*** PIN CODE (they should even keep it secret from their best friends) - to prevent others from snooping or misusing it.
- Ask their parents to install security software on their children's phones and reputable anti-virus programs on their computers to safeguard them against malware attacks and even theft.
- They should not say, text or post anything that would hurt or embarrass someone else – bullying should be an absolute no-no!
- They should not make, send, or accept provocative texts, photos, or videos. Once they are shared, they can be forwarded to anyone, anytime, even years later when they are already grown up.
- They should never click on links in advertisements, contests, text messages offering free prizes - 'deals' or 'winnings' that sound too good to be true usually are - since these could contain malware (viruses) which could damage their phones or computers, or result

[2] Microsoft & LOOKBOTHWAYS, 2014. Teach Kids Mobile Safety.

in the selling information about them or even theft of their identity.

- They should not download apps without checking the reputation of the stores or sites hosting them. They could infect the device with malware or give someone access to information you do not want them to have.
- They should not use the free Wi-Fi in public places to shop or access e-mails since this could give hackers easy access to their devices.
- They should not keep *any* ***photos*** on their phone that they would not want others to see *(ask learners why not).*
- They should never post their ID, password, pin numbers, home address, contact details, or photos of yourself, your family or your home on the Internet or social networks.
- They should not place *any* pictures on their computers or phones that they would not want others to see.
- They should not make friends with strangers online - why they should include in their friends list only people you already know.
- They should 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!
- They should not open e-mails dropped into their SPAM folder – delete them immediately.
- They should not respond to any message that makes them 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. If you receive such messages on a "chat room", leave the "room" immediately.

- They should not let other persons use their mobile phones unless they or their parents have disabled their GPS for social networking applications.
- They should listen to their instincts – if they feel uncomfortable about something, they should ***not*** do it!.
- They should tell a trusted adult when they think something is wrong or someone is targeting or harassing them.
- They should limit the time they spend on the phone / computer – especially in playing games - there is still a real world with real people out there.

In short, teach learners not to rush when they are on the Internet. Instill in them a commitment to first consider:

a. The ***risks*** they might face if they were to respond to a message, access a particular site, or post something on the Net ***(i.e. to*** **STOP**);
b. The impact that their actions might have on their and others' safety **(i.e. to THINK)**, and
c. To connect only if the risks are minimal or non-existent (i.e. CONNECT)

Once you are sure that learners realize the importance of using their phones and computers responsibly, engage them in one or more fun activities aimed at consolidating and helping them internalize what they have learnt. Apart from the word games listed under Theme 1 other fun activities could include:

- Creating opportunities for learners to share, in pairs, groups or during whole class talk time, their own nasty experiences with mobile phones and/or computers.
- Teaching or letting learners compose a jingle, slogan or song which focuses on the STOP – THINK - CONNECT maxim.

- Letting learners play DETECTIVE – i.e. identifying people who are using their phones and/or computers responsibly/safely and/or irresponsibly or unsafely in a collage depicting some or other public place *(a shopping mall, a park, a taxi rank, etc).*
- Encouraging learners to create COLLAGES which visually depict either some of the Internet risks or the responsible and irresponsible use of mobile phones and computers
- Letting learners represent the STOP – THINK – CONNECT maxim symbolically as three separate **road signs** and post these on the wall of the classroom or computer laboratory.
- Telling or letting learners tell or write stories or dialogues related to computer or mobile phone incidents that could have been prevented or which illustrate safe/responsible or unsafe/irresponsible use of these devices.

More challenging activities, like the ones that follow, which require the application of knowledge and insights gained in the analysis of a situation or incident could be given to Intermediate phase learners with the requisite reading ability.

Activity 1

In this activity they will learn about some of the threats they might face in cyber space. Tell learners that the procedure they have to follow is set out in the steps below. Display, read and explain the instructions.

- First allocate a different reading to each of the members in your group.
- Each person then has to spend a few minutes reading about the threat allocated to him/her.
- When everybody has finished reading, the person who read about the threat has to tell the rest of the group what s/he has learnt from the reading.

- Listed below the readings are some of the most common online activities. When everybody has had a chance to share her/his understanding or the threat that s/he read about, the group as a whole has to discuss and answer the questions posed in the tables after the readings. The first table has been completed as an example of what you are expected to do.
- You have 30 to 40 minutes to complete this activity.

Provide these as handouts:

Reading 1

Cyber Bullying – Cyber bullying takes place when someone uses technology to harass or intimidate someone else by sending or posting means, threatening and intimidating messages to another person. Examples of cyber bullying include abusive e-mails, malicious posts on social networking sites, inappropriate image tagging, uploading of embarrassing photographs, creating fake profiles of web sites designed to hurt another person, and so on. Cyber bullying has serious emotional consequences and can leave the victims of bullying depressed and anxious, lower their self-esteem or even lead to suicidal thought.

Reading 2

Cyber Predators – Cyber predators are adults who exploit children and teenagers by using Internet communication tools such as mobile phones, chat rooms, social networking sites and even e-mail. Their main motive is sexual abuse. They use attention, affection, kindness and sympathy while interacting with young people in order to manipulate them into thinking the adult concerned cares about them. In this way they build a relationship of trust with the youngster concerned. Once trust is established and the youngster has taken the adult into his/her confidence, often sharing sensitive information, the adult arranges a personal meeting with the youngster. These meetings inevitably results in great emotional

and, sometimes, physical harm to the youngster with whom the adult has arranged the meeting.

Reading 3

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

Reading 4

Identity theft – Identity theft is a fast-growing cyber threat. What happens is that a person makes unauthorized use of someone else's name and personal information – passwords, usernames, banking or financial data, etc. – to commit theft or other crimes. It often occurs through a data breach, virus or phishing scam. Phishing scams are so called because phishers aim to 'fish' for personal information that will give them access to important data, money and other financial assets.

Reading 5

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

Display as Powerpoint or distribute as handouts.

Table 2: Internet Threats

Online Activity 1:

Posting personal information (name of school, phone number of physical address) on media sites		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?
People other than friends and family could find out where I live and study.	It could lead to criminal acts such as theft or burglary at my house.	I will not post personal information on social media sites.
***Online Activity 2**:* *Clicking on a link in your e-mail, or a Facebook post or smart phone message that announces a funny video of you.*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this.
***Online Activity 3**:* *Downloading songs and movies from popular file sharing sites*		
STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 4:
Researching various web sites on environment protection for a school project or assignment

STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 5:
Uploading revealing selfies on Twitter that you think make you look attractive

STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Online Activity 6:
Accepting friend requests from people you do not know

STOP	**THINK**	**CONNECT**
What are the risks?	How could this affect my safety or that of my family?	Should I go ahead and do this?

Activity 2

Present learners with a table like the one below using Powerpoint / flip chart or handouts, but with the following differences. Column 2 should be blank and the prevention strategies in Column 3 should be arranged in such a way that they do not correspond with the incident described in Column 1.

Learners have to:

- Identify and write down in Column 2 the risk or threat described in the scenario, and
- Match the scrambled prevention strategies in Column 3 with the scenario in Column 1 to which it relates

Table 3: Risk management

Description of cyber threat	***Name of threat***	***Prevention strategy***
Farouk created a web site, posted mean comments on it and uploaded embarrassing pictures of Anant on it after they had a big fight. The web site invites other learners to state why they do not like Anant.	Cyber bullying	Keep screenshots of content posted as evidence of harassment and report the incident to a parent or person of authority. Register and 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 for 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.

Activity 3

Learners have to read the scenarios that follow and, based on their knowledge and insight of internet communication, answer the questions following each scenario.

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 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 should she not? Give reasons for your answer.*
2. *Do you think it was responsible of Fiona's parents to allow her to open her own Skype account? Give reasons for your answer.*
3. *Why would the two girls want to connect via Skype? Could they not rather use another social media network? Give reasons for your answer.*

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.

THEME 3: SHARING AND CARING

Introduce the lesson / session by telling learners that the focus in this lesson / session is not on the bad things that other Internet users could do to them but on the harm that they could do to others if they do not behave the way they ought to.

Facilitate a discussion on the rules in learners' own homes regarding the way people should treat each other by asking questions like the following:

- Does your family eat together? If so, how often does this happen – every evening/morning, every Sunday, etc.?
- Do you think it is important for the family to eat together? Why / why not?
- Who washes the dishes after supper? Why?
- Do the children in your family have to do certain chores? If so, what are they and why are you expected to do them?
- Do your parents limit the time that you spend in front of the television/ computer/on the phone? If so, have they told you the reasons for doing so?
- Are there any rules in your home on how people should behave? If so, what are these rules?
- Do your parents punish you when you break these rules? If so, how do they punish you?

Use learners' responses to these and other questions as basis for a discussion on the need for rules and regulations in life and the values *(respect, caring, sharing, compassion, honesty, diligence, etc)* informing the rules.

You could perhaps ask learners to name people (pop stars, film stars, sport heroes, historical figures, etc.) whom they admire and to tell you why they admire them. Try to get them thinking about the person not only in terms of what s/he looks like but also in terms of how s/he behaves.

Follow this discussion by asking learners to think of people whom they thoroughly dislike or of whom they are afraid. Let them talk about their reasons for disliking / fearing the persons concerned but, once again guide them towards an assessment of the person's actions rather than of his/her appearance.

Also 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.

Use learner responses as basis for a discussion of moral/ethical and immoral/unethical behaviour. Guide them towards a realization that it is not obedience to rules that makes one moral but rather, adherence to a set of values. Point out that people who do the right thing because they fear punishment are not necessarily moral / ethical, whereas people who base their actions on what they believe – that is, on their values – are usually moral/ethical.

Point out that moral people usually treat other people as they themselves would like to be treated; that they treat other people with respect, care for them, and show compassion when there is a need for it. Moral people do not bully, harm or steal from others. Neither do they spread malicious gossip, tell lies or try to embarrass others.

An effective way of teaching learners moral lessons are by means of stories, preferably stories that are part of the cultural group to which they belong – African folk tales might, for example, have a greater impact on children from Africa than Grimm's fairy tales would. It is therefore up to the teacher to choose stories that will lend themselves to the teaching of good manners and moral values. The story must, as a rule, however, be followed by questions aimed at the teaching of values, attitudes and etiquette.

You could, for example, use the fable that follows or other fables involving animals as basis for a discussion of moral values and behaviour.

The Scorpion and the Frog

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

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

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

"Mr Frog," the scorpion shouted, "would you be so kind as to allow me on your back and take me to higher ground, because I fear I might drown in the flood. You know, we scorpions cannot swim.'

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

"Hey listen, Mr Frog. Why would I do that? You can see that I'm scared stiff of the flood and would not do a thing like that. I know that it would mean the end of both of us."

The frog thought for a moment. What the scorpion said made perfect sense. He looked at the water rising and at the scorpion

clinging to the rock. Hesitantly he moved closer and allowed the scorpion to get on his back.

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

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

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

Possible questions

1. Would you say the frog was kind and caring? Why do you think so?
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. Has anybody ever betrayed your trust? How did it make you feel?
5. Do you think the scorpion was honest or not? Why do you think so?
6. Have you ever behaved like the scorpion? When? Why? How did it make you feel?
7. Do you think that the scorpion would have stung the frog if there was a law against scorpions stinging frogs? Give reasons for your answer.
8. Who would you rather be in the story – the scorpion or the frog? Why?

Relate the story of the scorpion and the frog to Information Ethics, that is, to the way people should be using information and information communications technology. Emphasize the importance of:

- Verifying the accuracy of information before using it or passing it on to others
- Not posting or passing around inaccurate or false information

- Not using information to embarrass, deceive or intimidate others
- Not stealing information from others and pretending that it is one's own
- Not using information communications technology for criminal activities
- Not using information communications technology as a means of
- Basing choices about what to do with information (e.g. passing it on or not) on values rather than expediency

Explain the meaning and possible impact on others of each of these abuses of information and information communications technology. Choose one or more of these for a more detailed discussion. The choice would depend on the kind of information immorality – if one could call it that – most prevalent in your school or of particular importance at any point in time.

For example:

- If cyber-bullying is a problem in your school, spend a whole lesson on that (see Section 3 of the *Concept Book* for more information on cyber bullying)
- If gaming addiction is a problem, spend time on that (surf the Internet for more information on this problem)
- If you are giving learners an assignment or project to do, spend some time on plagiarism and copyright as information ethics issues.

Having sensitized learners to the impact *(positive and negative*) that the kind of information and the ways in which it is accessed and disseminated could have on themselves and other people let them do some or other activity which will demonstrate their understanding of and commitment to the responsible, safe and ethical use of information and information communications technology.

An important point to make if you think the learners in your class are emotionally ready for this is to alert them to the existence of information ethics dilemmas, or Catch 22 situations. Tell them that a person who is caught in a situation like this is forced to make a choice between two things that have an equally strong pull on him or her. S/he might have been told something in secret which could, if not revealed, cause someone great harm However, if s/he tells, s/he is breaking the confidence of the person who told her/him the secret. What should s/he do – tell or keep quiet?

We end this manual with a few of these information ethics dilemmas that school children might at some time find themselves in. if you feel that the learners in your classes are mature enough to make information ethics decisions, let them do the case studies that follow or write your own, based on media articles or actual incidents that caused dilemmas like these.

Activity 4

In this activity learners have to:

- Quietly read the information ethics scenarios that follow 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, share and discuss your answers in pairs or in groups.
- Once all the questions and responses have been discussed, answer the last question in writing.

Information ethics scenario 1

Farouk, who goes to a private school, receives an e-mail with a subject line that reads, “You have just won R10,000. All he needs to do is to open the e-mail, click on the link provided and enter the personal information requested. Knowing that his parents have made and are still making major sacrifices to keep him in this school because they want him to have a

better future, he is very tempted to open the e-mail but is frightened that it is a hoax.

Questions

1. *Between which two things does Farouk have to choose? In other words, what is the dilemma?*
2. *What makes the dilemma a 'moral' one?*
3. *What do you think will happen if Farouk opened the e-mail?*
4. *What do you think will happen if he did not open it?*
5. *What would you have done if you were in his shoes and why?*
6. *Did the group discussion change your perception of what Farouk should or could have done? If so, what changes would you like to make to your original answer. If not, what is it that makes you stick to your original answer?*

Information ethics scenario 2

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

Questions

1. *What is the dilemma? In other words between what and what does Sipho have to choose?*
2. *What makes the dilemma a 'moral' one?*
3. *What do you think the consequences would be if Sipho does what his friend asks?*
4. *What do you think the consequences would be if he decided to refuse his friend's offer?*
5. *What would you have done if you were in his shoes and why?*

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

Information ethics dilemma 3

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

Questions

1. *What is the dilemma? In other words, between what and what do Dick and Tracy have to choose?*
2. *What makes the dilemma a 'moral' one?*
3. *What do you think the consequences would be if Dick and Tracy decided to download the freebies?*
4. *What do you think the consequences would be if 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 basic knowledge of information ethics.

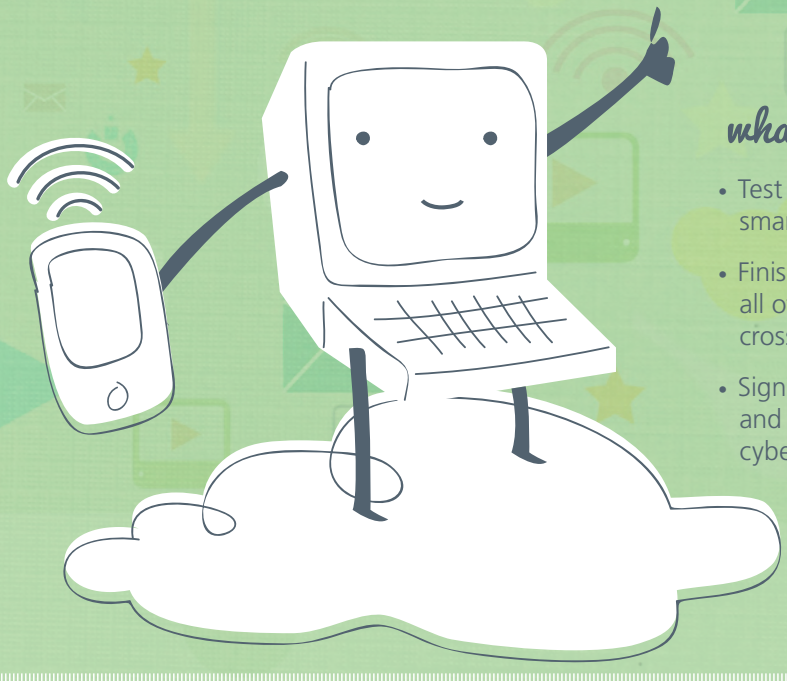
Some practical material to consider for use in the classroom

Copied in the next few pages we wish to present, with full recognition of the effort by McAfee® and Intel Digital Security®, fun activities and material that could assist in the classroom. You will notice that both McAfee® and Intel Digital Security® are involved in this and other programmes aimed at enhancing safety in our children's digital world.

ONLINE SAFETY

FOR KIDS

activity book

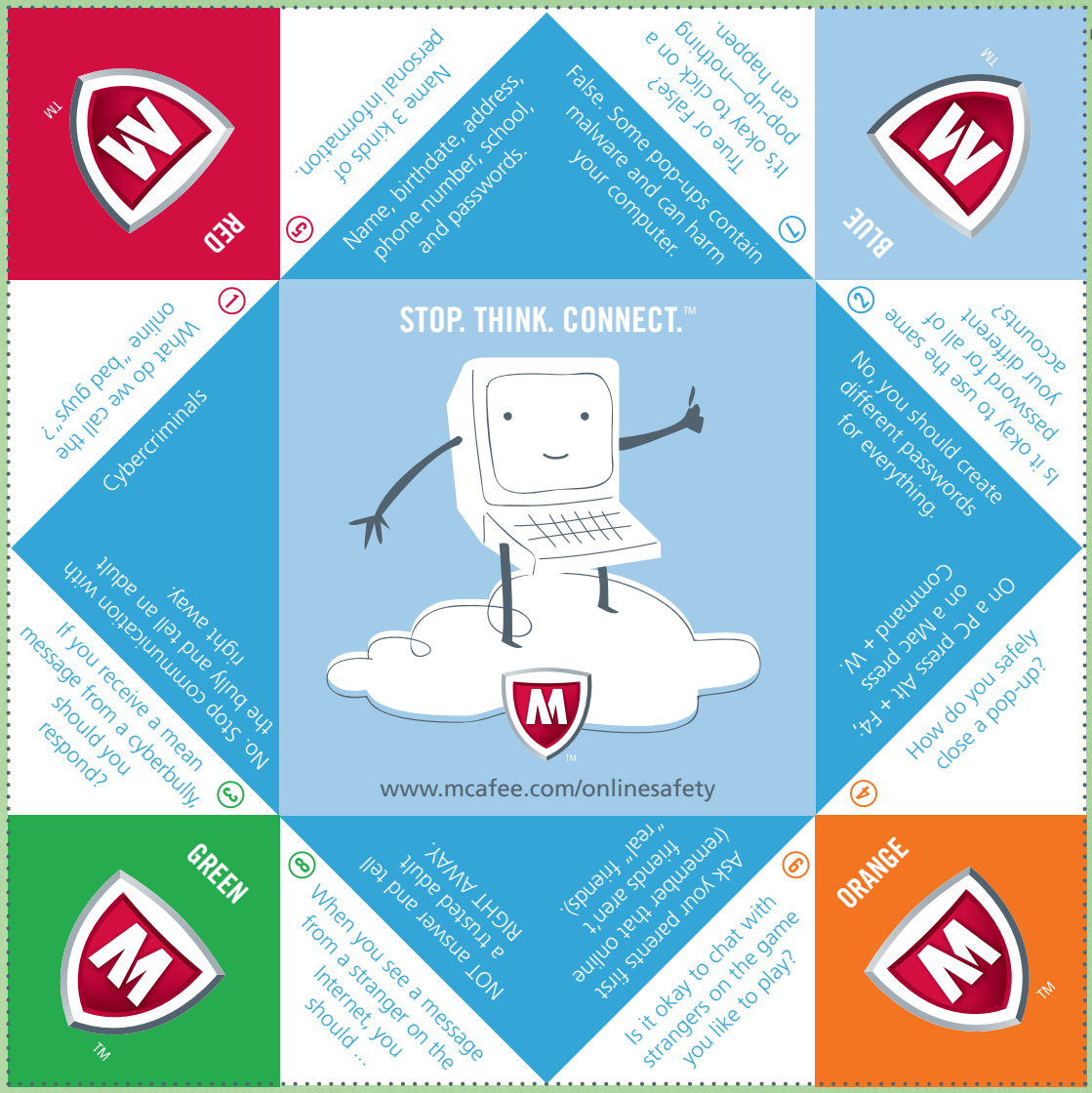


what's inside

- Test your Internet safety smarts with our origami quiz.
- Finish the word search to get all of the answers for our tricky crossword puzzle.
- Sign the Internet Safety Pledge and promise to be a responsible cyber citizen.

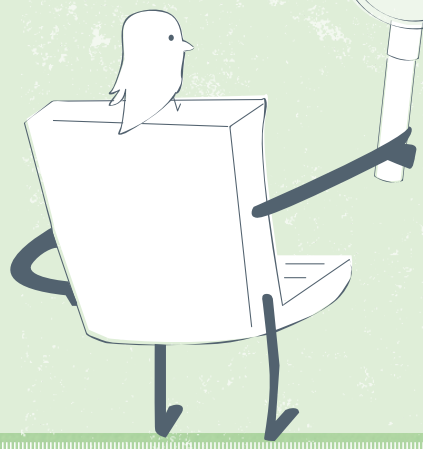
FORTUNE-TELLER QUIZ

1. Cut around outside of fortune-teller along the dotted lines.
2. Fold the top right corner over to reach the bottom left corner and crease. Open it back up.
3. Repeat the fold with the other two corners and crease. Open it back up.
4. With the wrong side up, fold all 4 corners towards the center so they meet evenly and then crease.
5. Turn it over and fold all four corners toward the center again (it's smaller now).
6. Slide your thumbs and index fingers inside the 4 flaps and pinch them together. Now take the quiz!



WORD SEARCH

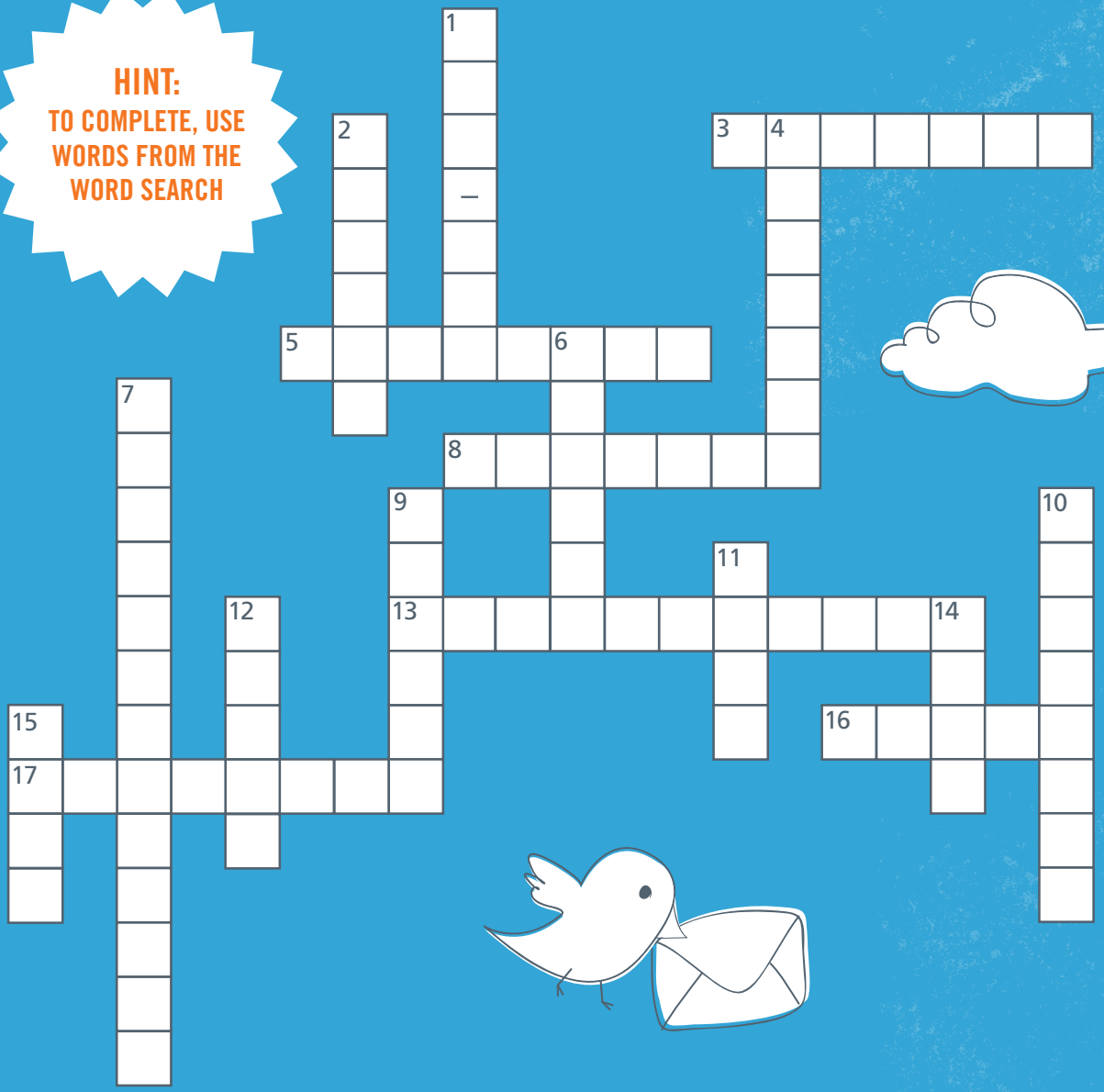
E R A W Y P S E P A Y J P Y G
N A Z Y O C E O T M A C S R N
E Z M P I F R V F A Q C S G I
F J U C V X A E E J V C G I Y
I P I H T O W K B M I I Q M L
S T S C P V L W P H V C R A L
C E L L U L A R T P I D K P U
Q I D W F G M E N A R X S S B
J D C O A G R O E S U N N H R
P D H T W E U M P S S N Y O E
W P O A B N A J P W Q X T R B
W E A Y C I L C K O N Z B N Y
G L C O L K H O A R T L D F C
O N L I N E E W A D Q S V N V
G M E C T K P R Q D Y Q X E O



CELLULAR
DOWNLOAD
HACKER
PASSWORD
SCAM
STOP
CYBERBULLYING
EMAIL
MALWARE
POP-UPS
SPAM
VIRUS
CYBERETHICS
GEOTAG
ONLINE
PRIVATE
SPYWARE

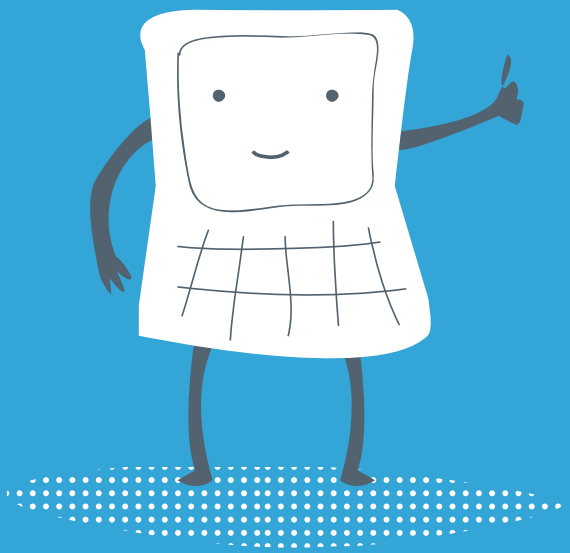
CROSSWORD PUZZLE

HINT:
TO COMPLETE, USE WORDS FROM THE WORD SEARCH



across

3. Software that is used to collect personal information without your permission
5. Don't share this with anyone other than your parents
8. Software designed to damage a computer or device
13. Treating others online the way you want to be treated
16. An electronic mail used for communicating with another person
17. Involving a cell phone



down

1. Don't be fooled into clicking on these (hyphenated word)
2. It allows others to know where you have taken a picture
4. Personal information should always be kept _____
6. Being connected to the Internet
7. The act of repeatedly harassing someone over the Internet
9. Someone who can gain unauthorized access to other computers or devices
10. Whenever you receive information from the Internet, you _____ it to your computer
11. _____ .THINK.CONNECT.
12. A program that can make your computer sick
14. Junk email
15. An online offer for a free Apple iPad is usually a _____

FUN MAZE

HELP CHIP GET HIS EMAIL

INTERNET HUNT

CIRCLE EVERYTHING YOU SEE THAT CONNECTS TO THE INTERNET, AND THEN COLOR FOR FUN.

McAfee
An Intel Company

INTERNET SAFETY PLEDGE

BECAUSE USING THE COMPUTER AND THE INTERNET IS A PRIVILEGE THAT I DON'T WANT TO LOSE...

I will not reveal my name, phone number, address, or passwords with online "friends".

I will never meet in person with people I met online.

I will always treat others online as I would like to be treated.

If an online situation makes me feel unsafe or uncomfortable, I promise to let a trusted adult know.

CHILD'S SIGNATURE

DATE

PARENT'S SIGNATURE

DATE

www.mcafee.com/onlinesafety

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

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