Digital Wellness Programme

A proposed toolkit to support the introduction of an Information Ethics curriculum in schools and communities in Africa

RESOURCE AND CONCEPTS BOOK

Digital Wellness Programme

A proposed toolkit to support the introduction of an Information Ethics curriculum in schools and communities in Africa

RESOURCE AND CONCEPTS BOOK

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 - RESOURCE AND CONCEPTS BOOK

2015

ISBN: 978-1-928261-65-0

Authors / Editors
Beverley Malan
Coetzee Bester

This work is licensed under a Creative Commons Attribution-Non-commercial-No Derivative Works 2.5 South African Licence. Please see http://creativecommons.org/licenses/by-nc-nd/2.5/za for details.

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

SECTION 1: ACRONYMS AND USEFUL LINKS 1

SECTION 2: KEY CONCEPTS 3

SECTION 3: CYBER BULLYING 32

SECTION 4: TEN FREQUENTLY ASKED QUESTIONS 38

BIBLIOGRAPHY 41

FOREWORD

Since the first African Conference on Information Ethics was held in February 2007, various academic institutions, government departments and private sector stakeholders have contributed to the expansion of the work and objectives set by the conference. These objectives not only included the growth of an awareness of Information Ethics in Africa but also a commitment to formally research the topic and to teach the new knowledge in formal courses at universities.

In support of the mentioned academic objectives, the Africa Network for Information Ethics (ANIE) and the Africa Centre of Excellence for Information Ethics (ACEIE) were created to further support UNESCO activities in WSIS on the African continent. The Memorandum of Agreement between the University of Pretoria and the Department of Communications (signed on the 15th of December 2011) formalized the existence of the ACEIE, whose main task is to be a hub for research and of networks between all parties passionate about and interested in Information Ethics in Africa. To this purpose the ACEIE coordinated numerous workshops in Africa and produced various books and articles aimed at ensuring that data on information ethics remain current, thought-provoking and development –oriented.

The need for a *Resource Book* originated during the course of workshops with academics, educators, and various other groups interested in learning more about cyber safety and information ethics. Workshop participants told us that, because they were not familiar with all the terms being used at workshops they sometimes had trouble following or participating in discussions. They suggested that a book with brief explanations of key concepts would be very useful. We heard what they said, and the Resource Book is the result.

Aimed at providing interested parties with a better understanding of Information Ethics terms as well as a platform for debate on Information Ethics issues, the Resource Book consists of **four** sections, each serving a very specific purpose.

- ***Section 1*** consists of a table with not only acronyms that are commonly used in discussions relating to digital safety, information communications technology and information ethics but also with links to web-sites that provide detailed information on various Information Ethics topics/themes.

- ***Section 2***, which is a response to workshop participants' request for a glossary of key concepts, consists of a list of Information Ethics terms/concepts, followed by

a brief definition and a somewhat more detailed explanation of the term/concept concerned.

- ***Section 3*** consists of a single text on ***cyber bullying.*** Given the constant increase in cyber bullying and the harmful effect it has on those who are being bullied we thought that the information in this text might assist parents, teachers and community leaders to help promote digital/cyber safety in their organizations and communities.

- ***Section 4*** provides answers to ***Ten Frequently Asked Questions*** on cyber safety and information ethics matters. The list is an abbreviated version of a list that first appeared as an appendix to the 2014 Intel Education Digital Wellness Curriculum.

We trust that you will find the Resource Book not only useful but also reader-friendly, and that it will help you in your efforts to promote digital/cyber safety and information ethics in your schools, classrooms and/ or communities.

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

SECTION 1: ACRONYMS AND USEFUL LINKS

.

Acronym	What it stands for	Link
ACEIE	African Centre of Excellence for Information Ethics	www.up.ac.za/aceie
AI	Artificial Intelligence	http://www.journals.elsevier.com/artificial-intelligence/
AISI	African Information Society Initiative	http://www.isn.ethz.ch/isn/Digital-Library/Organizations/Detail//?id=90672
ANIE	African Network for Information Ethics	http://www.africainfoethics.org
CGM	Consumer Generated Media	http://www.beaffinitive.com/case-studies/consumer-generated-media/
CMC	Computer Mediated Communication	http://jcmc.indiana.edu/
CSR	Corporate Social Responsibility	http://issues.tigweb.org/csr?gclid=CP6x5O2Iu7YCFRHMtAod5D4A3g
COMNET-IT	Commonwealth Network of Information Technology for Development	http://www.comnet-it.org/
ICIE	International Center for Information Ethics	http://icie.zkm.de
ICT	Information and Communication Technology	http://www.researchictafrica.net/home.php
IE	Information Ethics	http://www.unesco.org/new/?id=21230
IFLA	International Federation of Library Associations and Institutions	http://www.ifla.org
IK	Indigenous Knowledge	http://www.unesco.org/most/bpindi.htm
IMF	International Monetary Fund	http://www.imf.org
INSEIT	International Society for Ethics and Information Technology	http://inseit.net
IPRs	Intellectual Property Rights	http://stats.oecd.org/glossary/detail.asp?ID=3236
IRIE	International Review of Information Ethics	http://www.i-r-i-e.net
IS	Information Systems	http://www.journals.elsevier.com/information-systems/
IS	Information Security	http://www.sans.org/information_security.php
ITU	International Telecommunication Union	http://www.itu.int
MOOCs	Massive Open Online Courses	www.mooc-list.com/
NEPAD	New Partnership for Africa's Development	http://www.nepad.org
NGO	Non-Governmental Organisation	http://www.sangoco.org.za/
OECD	Organisation for Economic Co-operation and Development	http://www.oecd.org
PDA	Personal Digital Assistant	http://www.hp.com/hpinfo/newsroom/press/pdabrochure.html
PNC on ISAD	Presidential National Commission on Information Society and Development	http://www.pnc.gov.za
POPI (legislation)	Protection of Personal Information Bill	http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf
SADC	Southern African Development Community	www.sadc.int/
SNS	Social Networking Site	http://socialmediatoday.com/node/195917

UCC	User Created Content	http://www.oecd.org/sti/ieconomy/participativewebanduser-createdcontentweb20wikisandsocialnetworking.htm#
UGC	User Generated Content	http://www.webopedia.com/TERM/U/UGC.html
UN	United Nations	www.un.org/en
UNESCO	United Nations Educational, Scientific, and Cultural Organization	http://www.unesco.org
UN ICT	United Nations Information and Communication Technologies Task Force	http://www.unicttf.org
VR	Virtual Reality	http://www.vrs.org.uk/
WEF	World Economic Forum	http://www.weforum.org
WPIIS	OECD Working Party on Indicators for the Information Society	http://new.unctad.org/templates/Event____926.aspx
WSIF	Web Services Invocation Framework	http://ws.apache.org/wsif
WSIS	World Summit on the Information Society	http://www.itu.int/wsis/index.html
www	World Wide Web	

SECTION 2: KEY CONCEPTS

Note:

- Terms and concepts are alphabetically arranged, with each term being defined and/or briefly explained.
- While the primary purpose of this section is to define and explain terminology, workshop activities related to specific terms/concepts are sometimes included with a view to stimulating critical reflection and debate on information ethics matters.
- Open spaces following each concept are meant for notes and/or conclusions reached during such discussions.

Access to information **–** the human right to access information, the means of obtaining or providing information (a mobile or other computing device), and the processes (ID, library card or password) required to get into information systems and/or information communications technology.

On the one hand, access to information is promoted by the development of new ICTs that provide remote access to information. On the other hand, access to information is hindered by laws, censorship, and some archiving processes. A significant hindrance in the accessing of information is cost-related, with many would-be users not being able to afford the tools needed to access the information they need or want.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Accessibility - The ease or difficulty with which one can gain access to information.

Information is accessible when it is easy for anyone to find or gain access to it but inaccessible when it is difficult to do so. The more accessible information is, the more people can make use of it. An inaccessible website, for instance, can restrict or hinder access to information for a significant proportion of users. Accessibility in information systems is important to avoid discrimination. In some countries, for example, the Disability Discrimination Act makes it a legal requirement for websites to be usable regardless of disability.

Accountability - Both the ability and responsibility to give account to some other party for your actions, in other words to take responsibility for what you do. Everyone who is in a position of power or trust is accountable to the persons who give them that power or trust (through election or employment for example). In this way, citizens have the responsibility to hold Government accountable for what it does. Government has to answer for its actions towards the citizens it serves. The same goes for other public, private and voluntary organizations, where officials have to answer to someone for their actions and take responsibility for whatever they do or say.

_____

_____

_____

_____

_____

Awareness – Knowledge of the existence or presence of something or someone, e.g. that there are certain risks attached to the use of the Internet.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Censorship - Limiting the type and content of information made available to the public by removing what is deemed to be immoral or not in the best interest of the recipients of the information. When the information that is allowed to circulate in society is officially supervised, edited, restricted or selectively prohibited, thus essentially being controlled in some way, it is called censorship. As a rule censors are usually government officials/departments, religious bodies, private pressure groups and, sometimes, information producers themselves (like speakers, writers and artists).

Any information, whether it appears in books, periodicals, films, television, radio, news articles or reports, speech, and/or internet websites in whatever form (stories, songs, cartoons, paintings, etc.) can be censored. Reasons given for censoring include morality, social norms, ideological positions, political stability and/or State security, to name but a few. Parties opposed to censorship argue that it might undermine

society's ability to use its own discretion, obstruct/hinder political opposition, end up drawing more attention to the thing being censored instead of deflecting it and that censorship is a form of invasion, administration and a threat to freedom.

Copyright – If you look on the inside front cover of a book you will see that the organization that published the book tells the reader who holds copyright – that is, who has the right to copy what is written in the book. Usually this is the publisher or the author of the book. There is also copyright on music, plays, films etc. which means that no one but the copyright holder may make copies of, distribute or perform these without the permission of the copyright holder.

***Corporate Social Responsibility* -** The ethical responsibility that corporations have towards the society in which they are located.

The consequence of our actions is an important ethical concern, and to take it into consideration is a necessary part of being a good citizen. Although corporations are not persons, they are legal entities with legal rights and responsibilities. On these grounds it may be expected that corporations behave like good citizens, aligning their behaviour to societal norms, values, objectives and expectations. To this effect, corporations are sometimes expected to take responsibility for and solve social problems they cause or contribute to; allocate resources to broad social ends, like helping other major institutions (eg. governments and universities) to achieve social progress, and to see to it that production and distribution of their products contribute to overall socio-economic welfare. This point is important to consider alongside the issue of information poverty.

Consider the enormous social and economic impact that ICT corporations and platforms, like Microsoft, Apple, Google, Facebook, Blackberry, Twitter, Nokia, MTN, etc. have on the world on an international scale. Their products and services determine how we communicate, format, and disseminate the information we need to participate and function in the Information Society. If these ICT giants focus purely on profits without taking responsibility for their actions, decisions and products, serious harm could be done to the social order of the societies in which they operate.

Cracking – Gaining unauthorized access to a system, usually with malicious intent, e.g. the intent of damaging the system, thus making them *cyber criminals.*

Ideas for discussion

- Would you hire a cracker to gain personal information about someone else?
- What kind of penalty should be implemented for crackers?
- How do you feel knowing that there are skilled crackers 'out there'?
- What would you do if you find out someone you know is a cracker?
- What should be done to prevent people with hacking skills from becoming crackers?
- How would you feel if you find out that a cracker has gained access to your personal information, like your bank account?

Culture - The way things are done in a particular group, community or nation – which behaviours and/or beliefs are acceptable or not, which rituals are followed at weddings, births and death, et cetera

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Cyber bullying – Harassing, humiliating or threatening someone in cyber space[1] by sending them nasty e-mails, posting malicious information, fake profiles or embarrassing photographs or comments on social networking sites. Like children who are bullied at school, people of all ages who are victims of cyber bullying carry the emotional scars of the bullying with them for life unless they receive help after the event.

_____

_____

_____

_____

_____

_____

_____

[11] See Section 3 of the Resource Book for examples of cyber bullying and ways of dealing with cyber bullies

Cyber crime - The use of information communications technology for activities that are against the law – cracking, phishing and identity theft, for example.

Cyber pornography – The publishing / posting of obscene or sexually provocative content on the Internet, often relating to children.

Cyber predators – A predator is an animal *(like a hyena)* that stalks/tracks other animals in order to kill them. Cyber predators are usually adults who exploit children of all ages with the view to sexually abusing them. Their stalking techniques include showing false/insincere affection, sympathy, kindness, etc. to lure children into the trap of trusting them before they go over to the actual 'hunt', in which they do the children concerned all kinds of emotional and physical harm.

Cyber savvy – A person is cyber savvy when s/he knows and understands the risks and opportunities associated with the use of information communications technology and knows how to protect him/herself and his/her devices against the threats.

Cyber space – The Internet world, that is, web-sites and networks where one can obtain information, communicate with others, download music and movies, play games, et cetera.

Cyber stalking – Following and tracking a user's internet chats without the person's knowledge. Also see *cyber predator.*

Digital divide - The gap between those who have and those who do not have open and/or free access to ICT and electronic information systems either because they do not have the resources or the requisite skills to access information systems. The divide is not only between groups in a society, but between the 'developed and developing' nations of the world. The digital revolution will have economic, social and political implications – much of which will be guided by who takes the lead in Information and Communication Technologies.

E-learning and E-literacy – *E-learning* refers to the ability to use electronic communications technologies for educational purposes whereas e-*literacy* refers to the ability to use it for different purposes.

E-waste – electronic hardware and devices that are discarded due to age or decay.

Because of the rapid pace of the development of new ICTs, many electronic devices like mobile phones become outdated very quickly. This leads to a huge disposal problem – how do we get rid of all the devices, in other words, how can we handle e-waste? The so called 'developed world' does this by dumping their e-waste in developing countries, paying them for the allocation of dumping space. The problem is the that developing countries used in this way usually do not have the infrastructure to protect the environment and people living in the vicinity of the dumps.

Food for thought:
Some solutions are to recycle or reuse electronic components or hardware. Can you think of any other way in which one could get rid of the waste without endangering other people's health or living conditions?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

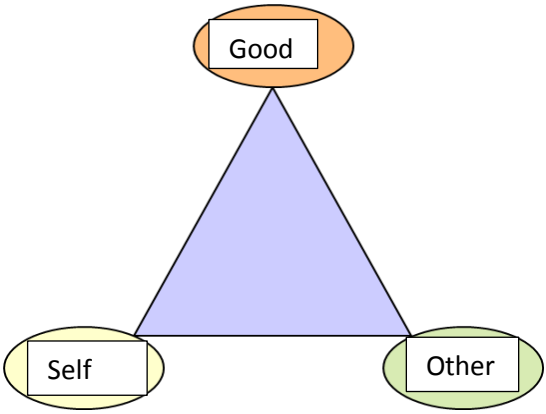
_____

_____

_____

_____

Ethic / ethical framework / code of ethics – A value system that governs one's behaviour and/or a field of study which focuses on moral or philosophical issues. The focus on ethics as a field of study is on the difference between right and wrong good (fair or just) and evil (unfair or unjust), with regard to oneself and the 'other' (Rossouw and Van Vuuren, 2004:3).



In terms of this definition, behaviour is ethical if it takes into consideration not only what is good for oneself, but also what is good for others. This 'good' could be determined by a group and formalized as a law or religious doctrine, for example. It could, however, also be very personal – a way of life or a code of conduct. The dilemma is that many a time what an individual regards as right/good or wrong/evil is in conflict with the norm in a particular society/group.

Discussion point

How could conflicts between personal and group ethics be resolved and/or which one of the two should be considered in determining what is, in fact, good or evil?

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firewall – An 'imaginary wall', created by another computer, as part of your anti-virus program, which first screens incoming information before allowing it through, thereby protecting your device against potential harm.

Fraud – A criminal activity in in which one party intentionally deceives another in order to gain an unfair advantage or financial benefit while causing a loss to the person being deceived.

Fraud occurs when information which should be made available is hidden or when false information is presented as the truth. Fraud increases the cost of running a business, undermines competitive business, and leads to corruption in public and private sectors. Like other crimes, fraud is said to have three dimensions, namely: motive, opportunity and rationalization.

Gaming addiction – Like any addiction – smoking, alcohol, gambling, drugs – which takes over and ruins a person's life, gaming addiction could make one physically ill (because of excessive hours spent in front of the computer), isolate one from one's friends, and impact negatively on one's education or career.

Hacking – Gaining access to an electronic device or system – for reasons of curiosity or interest rather than malicious intent - by using techniques or mechanisms that were not intended to provide access; a 'hacker' would, therefore be someone who "illegally gains access to and sometimes tampers with information in a computer system" (Merriam-Webster online dictionary)

Hashtag – A # sign before a word or phrase to identify messages on a specific topic.

Human rights - Rights that can legally be claimed by all human beings and are usually protected in terms of a country's Constitution. Some of these rights are the right to privacy, the right to life, the right to human dignity, and the right to information.

Identity theft – One's identity is stolen when someone else uses one's name or personal information (ID, e-mail address, account numbers, etc) to commit some or other crime. The most common causes of identity theft are viruses, data breaches or phishing scams. A person who does this is guilty of ***identity fraud***, which is a criminal offence. *(Also see **Ten Frequently Asked Questions** in Section 4)*

Impact - The effect or influence that one or more things or processes have on something else. The spreading of false information about a person could, for example, have a negative impact on the reputation, dignity, or self-esteem of the person concerned.

Information **-** Meaningfully organized or structured data: a piece of information is considered valueless if, after receiving it, things remain unchanged". Business Dictionary.com therefore defines information as data that is "(1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty. Information is valuable *because* it can affect behaviour [sic], a decision, or an outcome. For example, if a manager is told his/her company's net profit decreased in the past month, he/she may use this information as a reason to cut financial spending for the next month.

Information can be generated through research and experience; it can be shared, hidden, modified, analysed, synthesized, and manipulated. Information can also become outdated, and be bought and sold for different reasons or purposes.

Information Age **-** An age in which the generation, dissemination and use of information dominates the broad spectrum of human affairs *(also see Information and Knowledge Society).*

Information communications technology - Technologies that provide access to information via electronic devices and/or tele-communications media - it is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, satellite technology and other communication mediums.

Information Ethics - Accessing and using information and information communications technology in morally responsible ways. Information ethics is concerned with issues like information privacy, information poverty, moral agency, and problems arising from the life-cycle of information. It explores and evaluates the development of moral values, social contracts and the possibility of moral integration in the creation of new power structures and ethical conflicts. It also considers new forms of trust, marginalization, waste, inequality, security, accountability, censorship, governance, fraud, community and informational self-determination.

Information and Knowledge Society - A society in which physical, mental, social and economic survival depend on the generation, processing, and free flow of knowledge and information.

The term describes today's society, where our lives at home and at work are information intense (Balkin,2004). How we create, share, protect and manipulate information is one of the most important factors in our daily lives, as well as in economics, power structures, and global cultures. These devices change the way we work and communicate, since we can send information to each other instantly. Countries or economies that do not or cannot participate in the Information Society cannot be globally competitive. In other words, where people do not have the skills or equipment to access information, they become excluded from the Information

Society. Organizations like UNESCO aim to create a more inclusive environment through empowerment.

Information Life Cycle – The cyclical process required to transform raw data into reliable and usable information.

Information network - A network which is used for the generation, recording and sharing / dissemination of information.

Information Poverty – Insufficient information, minimal access to, or lack of the means required to access the information needed to improve one's living quality and/or effective functioning (Britz, 2004)

'Poverty' is relative to 'wealth', and as with money, information poverty leaves one in a disadvantaged position in society. Information poverty could be the result of a person's level of education, especially the skills needed to use ICT, fluency in English – since this is the dominant language of ICT programming - governmental policies, cultural and religious beliefs.

Information System – any "integrated set of components" designed to facilitate the collection, storage, and processing of information and/or data. Businesses and other organizations rely on information systems as basis for operational management, customer interaction, and competitive marketing *(Britannica Online Encyclopaedia).*

Integrity - Always behaving in accordance with one's own set of personal values and beliefs even when doing so could have negative consequences for the self.

Malware – Malicious software, e.g. viruses, worms, spyware and Trojan horses, which is installed on your device with the intention of stealing your password/s, deleting your files, or reformatting the hard disk of your computer or laptop. are examples of malware.

Phishing – Real-life fishermen, in order to catch a fish, use the kind of bait that the fish they want to catch will take. *Phishers* want to catch people: the bait they use could be an inheritance or big sum of money you supposedly won in a competition. Once you take the bait you are required either to provide your bank details, physical address, ID, password, etc so that the phisher can 'deposit' the money into your account or you are directed to a link or button that you have to click. Don't do this – unless you want to be a dead *phish*.

Plagiarism – Presenting someone else's work as if it was created by you, whether this piece of work is a poem, song, novel, play, quotation or information included in an assignment without acknowledging the source.

Privacy – This is one of the human rights accorded to all people and implies that a person may keep his/her information to him/herself without being subject to surveillance.

Research - Reading up on or collecting evidence on something - to test its validity, reliability or truth, or to find answers/solutions to important questions.

Respect – A human quality in which a person behaves in such a way that s/he does not insult or harm someone else and/or in any way undermine this person's human rights.

Responsibility – Doing what one is supposed to be doing in a way that shows one is willing to accept the consequences of one's actions.

Spyware – Pop-up ads *(see **Ten frequently Asked Questions**, in Section 4)* and web browsing monitors that infect computers for commercial gain.

Trojan horse – A program that you download without knowing that it includes a 'back door' that allows attackers to gain access to your device.

Value - Something that one holds dear and which determines one's decisions or actions.

Value system - A set of values that governs the behaviour of the group or groups of people who developed it and/or agreed to accept it as their own

Virus – A computer program file that attaches itself to disks or other files and then replicates itself repeatedly without your knowledge or permission *(see **Ten frequently asked questions** in Section 4).*

Worm – Like a virus but it does not infect your files. What it does is send copies of your files to other computers via a network.

SECTION 3: CYBER BULLYING

Note:

The text which follows reflects a mix of views expressed by education researchers, psychologists, and information technology experts. References to various Microsoft websites which deal with issues like these are also indicated in the text.

Because young people grow up online we should not be surprised that, as is the case on school premises and playgrounds, bullying is becoming a major problem. In order to address this problem we first need to know what bullying is, why certain children are inclined to bullying others and how they choose their victims.

First, what is bullying?

Simply put, bullying occurs when one or more persons deliberately and repeatedly tease, demean, intimidate, harass or physically hurt another person or persons. With the exception of physical bullying, all other kinds of bullying could take place on line. In this kind of bullying, known as online or ***cyber bullying,*** the bullies could hurt their victims in a number of ways, some of which are briefly described below.

- Bullies could send hurtful or threatening messages to their victims' cell-phones, spread unfounded rumours, or distribute embarrassing or altered photos or videos of the victim on social media. These kinds of rumours would be very harmful to the victim's self-esteem and could in the long run result in a number of psychological disturbances, like depression, bulimia, agoraphobia, et cetera.

- Bullies could choose to disclose secrets or private information about their victim by, for example, forwarding a confidential text message to others. The victim would then become afraid of ever sharing secrets or confidential information with everyone, resulting in extreme loneliness. Such loneliness could eventually lead to depression, bulimia or even suicide.

- Bullies would take steps to deliberately exclude their victims/s from a group in a game, virtual worlds or social media sites without giving any explanation for doing so. The victim might then start believing that s/he is ugly, stupid, or not acceptable to other people.

- Bullies could break into someone's phone or social media account with a view to impersonating this person. They would then impersonate the target and then 'share' hateful comments or malicious gossip about the victim's friends as if it came from the person they impersonated. The victims, thinking that the messages came from the person being impersonated, would then quarrel with the victim and/or refuse to be friends with him/her any longer. The victim is then isolated from his/her social network and could feel very lonely.

- Bullies would pretend to befriend someone, gain his/her trust, and then do something to deliberately betray the trust. The victim then becomes afraid of ever again trusting someone else. In the end, not having someone with whom they can share their deepest thoughts and feelings the victim could either become so over-burdened that s/he considers 'ending it all' or so angry at society that s/he decides to take revenge, as is often the case in unexpected school shootings and/or attacks on teachers, parents or other learners.

Second, why bully?

There are many reasons why children start bullying. Perhaps these children are being bullied at home – by their older brothers, sisters, or parents. Perhaps they feel 'invisible' because they do not get enough attention at home or at school. Perhaps nobody wants to be 'their' friend and, by bullying, they are not only expressing their frustration and anger but are simultaneously attracting the attention and/or admiration of other children who feel like them, hence they no longer feel alone, hurt, or deprived of attention.

Another reason why people become bullies could be that they choose the wrong role models. If they themselves feel weak or vulnerable they might look up to someone who appears to be strong and powerful – a bigger brother or sister, a father or mother, an uncle or aunt, a movie star, or a political figure. If the person they admire solves his/her problems by attacking others – verbally or physically – and seems always to be victorious, the child who feels weak or vulnerable might start imitating his/her role model's behaviour by bullying those of whom s/he is most afraid. And if it works, the bullying escalates to other areas of this child's life.

Bullying is not always intentional, though. Sometimes the 'bullies' are simply bored, or trying to be funny and, as others respond to their 'jokes', embarrassing photos, or untrue bits of gossip on a social media site, the whole thing escalates until they are

no longer in control of what is being said and, because they started it, it is extremely difficult for them to 'escape' from the situation they created in the first place.

What we have not explored is why certain people are targeted as victims by the bullies, so let's look at that for a moment.

Third, why submit to bullying?

Just as there are many reasons why someone becomes a bully, so there are many reasons why someone is targeted as a potential bullying victim. Some of the reasons that have emerged from research on bullying are listed below.

The most obvious person targeted as a potential victim by bullies is the person who is 'different' from the bullies themselves in terms of image, language, ability, size, dress, behaviour, et cetera. Think, for example, of the typical 'nerd' who prefers to spend his/her time in a library or in front of a computer rather than taking part in competitive or physical activities like sport. This child is an obvious target for the more 'butch' sector of school society and, unless his/her self-esteem is particularly good, and/or s/he knows how to defend him/herself chances are that s/he will be targeted for bullying.

Other people who might stand out from the group are those who are academically inclined in a school which places a high value on sport, those who speak with a different accent, those who belong to a different religion than the majority of school children, or those who, in a poor school, comes to school with their own lunch or lunch money, thus signalling that they are 'richer' than the others and must therefore be deprived of their riches – the lunch or the lunch money.

Physically small or weak children are also targeted by bullies who might make them 'pay' for 'protection' or who might simply use them as a metaphorical 'punch bag' on which they can rid themselves of their own anger or frustration.

While these reasons are more applicable to physical bullying, a child's online image or profile might create the impression that s/he is weak, vulnerable or 'different', hence s/he could be a potential victim of online bullying. It is, of course, also possible that, because the bullies do not have the opportunity of harming them in the actual world – at school or on the playground - because there are adults around, they resort to doing so on line.

Fourth, how does one identify bullies and their victims?

Identifying bullies and/or the victims of bullying is not as easy as it sounds, especially if bullying happens on line. There are, however, a few general guidelines that could assist adults – parents and teachers in particular – in picking up signs that a child is involved in online bullying, either as the perpetrator or as the victim. Some of these signs, or signals, are briefly described below but there might be other warning signs particular to specific contexts, situations and adult-child relationships. Watch out for these and, if you suspect bullying, take the necessary steps to stop it in its tracks.

i. ***Establish a relationship of trust*** between you, the adult, and the child or children for whom you are responsible. This is possible if you listen - ***really listen*** - to the kids. Ask them to talk about themselves, their interests, their dreams, their fears, their lives and/or life situations. Do not judge, do not preach, and do not give advice on what to do – unless specifically asked to. Even then it is better to *lead* the child towards finding his/her own solution rather than to *give* it to him/her on a platter.

ii. ***Get them to invite you into their world*** – the virtual, cyber sites where they feel comfortable. You could, for example, ask older kids to 'take you on a tour' of the websites they visit and/or the chat rooms where they 'hang out'. You could even ask them to allow you to play a cyber game with them or explore different sites with them. This will be easy if you have already established a relationship of trust with them but impossible if you have not done so. Be very careful not to breach this trust – by secretly or furtively going onto their sites or the chat rooms they visit when they are not around because you want to find out 'what they are up to'. If you do, they will never trust you again.

iii. ***Watch for signs of online cruelty*** – on the sites or in the chat rooms to which you are invited but also in the behaviour of the kids themselves. Do they look upset while texting or playing a game? Are they suddenly reluctant to go to school, to play or work with other kids in their class or neighbourhood? Have they suddenly 'lost interest' in using their mobile phone or computer? Any or all of these could be signs that the child or children concerned are being bullied online.

iv. ***Ask kids to report bullying to you or to another trusted adult*** - Promise unconditional support. Reassure them that you will not put restrictions on

their phone, gaming or use of the computer because they are being victimized. Also assure them that their identities or the exact nature of bullying will at no stage be divulged to the bully or bullies concerned. Then keep your word. Perhaps ask if you could pretend to be the person victimized in order to 'talk' the online bully out of bullying you, the supposed victim, in future, Allow the victim to sit with you while you do so and do not post anything that makes the victim uncomfortable or fearful. This too, will only be possible if the child already trusts you implicitly. Otherwise, do not even ask!!!

Fifth, how does one deal with bullying?

There is no single answer to this question: the appropriate answer will be determined by context, situation and the adult-child relationship concerned. However, the general guidelines that follow could serve as basis for the development of an anti-bullying plan of action – at home, at school, or in the community.

i. First of all, ***get the full story*** – that is, the *what*, *how*, *when*, *where* and *why* of the situation, from ***both*** the bully and the one/s being bullied. Listen carefully, take it seriously and, if you feel that this is necessary, take notes for future reference.

ii. ***Work out a plan of action*** - not on your own, but with the cooperation of both parties - the bully and the bullied.

- ***Don't blame*** either party for the incident. Rather try to understand the reasons *(not excuses)* and/or source of the bullying behaviour.

- ***Be supportive*** – that is, do not give the impression that you reject, condemn or disapprove of the child: focus on the behaviour instead.

- **Ask** the parties concerned how *they* think the conflict could be resolved so that neither party gets hurt. You could, for example talk about how the bully could make amends, how the victim could protect him/herself from being bullied again, etc.

- ***Report*** the bullying incident/s to the website or company where it occurred, without divulging the children's names. Microsoft could, for example, be contacted on *www.microsoft.com/reportabuse*.

- If necessary, ***contact counsellors*** or other experts who have been trained in dealing with bullies and their victims and ask them for advice or help in resolving situations like these.

- Having dealt with a specific situation, ***shift your focus***: from individuals to groups, and from reaction to prevention. You could, for example, prepare a lesson, run a workshop, or write a feature for your school or local newspaper on the ethical dimensions of online behaviour *(refer to the unit in your Workbook that deals with* ***information ethics*** *for ideas in this regard).*

- Convince you community – school, church, local – of the need for ***empathy training***. Training could focus, for example, on social and emotional issues – self-esteem, social responsibility, healthy/strong relationships, emotional intelligence, personal and social boundaries, etc. *(for a list of well-tested programmes, go to* ***aka.ms/EffectivePrograms****)*

- Run a ***kindness campaign*** in your community – school, church, local – in which people are encouraged to do one kind thing for someone else each day. The recipient of this 'kindness' could be a friend, a family member, a teacher, or even a stranger. Involve your local newspaper or radio station, have a march, organize a 'Be kind' competition. Be creative - do whatever will work in your particular community or context – and or surf the net for ideas (*schoolclimate.or/bullybust/resources/key_resources*, for example).

SECTION 4: TEN FREQUENTLY ASKED QUESTIONS

Note:

The ten questions listed here could be used for different purposes – as basis for a quiz, a questionnaire, a class test, for group or plenary discussions.

Q1 How do I create a safe, secure password?

A1 There are four things you have to look at when creating a password, namely length, complexity, variation, and variety.

i. *Length*: Create a password that consists of 8 or more characters
ii. *Complexity*: Include letters, numbers, punctuation, and symbols in your password
iii. *Variation:* Change your passwords regularly (every 3 months at least)
iv. *Variety:* Use different passwords for different accounts

Q2 What is a computer virus?

A2 It is a program file that can attach itself to other files, replicating itself over and over without the user knowing that it is happening. The virus can spread from one computer to another, sometimes by using an e-mail program, instant messenger or by disguising itself as an attachment. Not all viruses are harmful but some can destroy files and/or entirely erase a computer's hard drive.

Q3 How can I make sure viruses don't attack my electronic devices?

A3 There are *four* things you MUST do.

i. The first step is to install antivirus, anti-spyware and anti-malware programs on your computer and to set them to run automatic scans.
ii. Make sure you use an e-mail provider that scans all e-mails before you are allowed to open them.
iii. Avoid suspicious websites and, if your anti-virus program gives you a warning, do NOT go back to this site.

iv. Be careful of downloads – only download from sites that are reliable and trustworthy.

Q4 ***What are pop-ups, and what should one do when a pop-up appears?***

A4 A pop-up is a form of on-line advertising on the World Wide Web (www) which is intended to attract web traffic or obtain e-mail addresses. It usually appears when a user is linking up to a new website. Online users find pop-ups quite annoying because they interrupt what the user is doing but they can be blocked by means of pop-up blockers if one wishes to do so.

Q5 ***What is pirating?***

A5 It is the unauthorized copying of music, software, movies and other shared media files. Doing so is illegal because (a) most programs are only licensed for use on a single computer, (b) the user is not the owner of the software, and (c) you are, in fact, stealing someone else's intellectual property.

Q6 ***How should internet users respond to chain e-mails?***

A6 Chain letters and hoax messages are another type of Internet fraud. By persuading recipients to pass on the e-mail to other mail addresses, the sender clogs up in-boxes and slows down the server. In a sense, chain mails which play on your emotions or fears – telling you that something bad will happen to you if you do not pass it on – is a form of bullying / intimidation. Do not pass them on – delete them immediately.

Q7 ***Can one permanently remove posts from a Facebook Wall?***

A7 One can remove posts from one's OWN wall but whatever you have posted on someone else's wall can only be removed by that person and, if s/he has already forwarded it to other people removing it is well-nigh impossible.

Q8 **What should I do if my Facebook account is hacked?**

A8 There are FOUR things you should do, viz.:

i. Visit the Facebook Help Center and attempt to reclaim your account.
ii. Make sure that you change the password to your e-mail address immediately and, if it is the same password for other accounts change theirs too.
iii. Scan your system for viruses and, if there are any get rid of them.

iv. Notify your friends and family that your account has been hacked so that the hacker cannot send them malicious e-mail from 'you' or use your connections to phish from their accounts.

Q9 How can I change my privacy settings on Facebook?

A9 Click the account menu in the top right hand corner of any Facebook page and choose Privacy Settings. This page contains a group of general controls for your Facebook account, such as who can send you friend requests and messages. Your controls are right next to each thing you share. From this page you can then personalize your privacy settings for Contact Information Applications, Websites and Search.

Q10 Why would someone try to steal my identity?

A10 identity thieves take your personal information and use it to do things like renting an apartment, obtaining a credit card, or opening an account in your name. You may not find out about the theft until you review your credit record or statements and notice charges you did not make, or until you are contacted by a debt collector. This is why you should NEVER share personal information with strangers.

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 261698

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