Digital Wellness Programme

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

RESOURCE AND CONCEPTS BOOK

Digital Wellness Programme

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

RESOURCE AND CONCEPTS BOOK

The *Digital Wellness Toolkit* is dedicated as a tribute to the work in the field of Information Ethics by our Brother, colleague and friend

Chief Michael Anyiam-Osigwe

14 April 1959 - 29 November 2014

telecommunications
& postal services

Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

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

Digital Wellness Programme - RESOURCE AND CONCEPTS BOOK

October 2015

ISBN: 978-1-928261-65-0

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

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 the achievement of the objectives set by the conference. These objectives not only included an increased awareness of Information Ethics in Africa but also a commitment to formally research the topic and to teach the new knowledge generated by research in formal courses at universities.

In support of these 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 to facilitate the networking of all those who are 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 and Concepts 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 and Concepts Book* is the result.

Aimed at providing interested parties with a better understanding of Information Ethics terminology as well as at establishing a platform for debate on Information Ethics issues, the *Resource and Concept Book* consists of **five** 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.

- ***Section 5*** provides interested parties with a set of – E-safety Guidelines developed for schools by the Department of Basic Education in South Africa.

We trust that you will find the *Resource and Concepts 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
October 2015

SECTION 1: ACRONYMS AND USEFUL LINKS

.Acronym	What it stands for	Link
ACEIE	Africa Centre of Excellence for Information Ethics	www.up.ac.za/aceie
AI	Artificial Intelligence	http://www.journals.elsevier.com/artificial-intelligence/
AISI	Africa 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 Telecommunications 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. 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 easier it is for people to 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,theDisability 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 another 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). Citizens have the right to hold their governments accountable for what they do. By implication governments have to answer for their actions to the citizens they serve. 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) we call it 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 the form of 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 censorship undermines 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. Hence the accusation that censorship is a form of invasive administration that poses 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 which they caused or to which they contributed; to allocate resources to broad social ends, like helping other major institutions (eg. governments and universities) to achieve social progress, and tosee to it that the 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 an Information and Knowledge 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 the 'crackers' *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 found 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 found 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 – a term used interchangeably with ‘digital’ (both referring to things technological and related to the vIrtual world of the Internet)

____

____

____

____

Cyber bullying – Harassing, humiliating or threatening other people 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.

____

____

____

____

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

____

____

____

____

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

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 intent of 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/or 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 these.

____

____

____

____

____

Cyber space – The Internet world, that is, web-sites and networks where one can obtain and share 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, 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 has economic, social and political implications for those who control it as well as for those who don't. What these implications are will be determined by the values and intent of those who take the lead in Information and Communication Technologies.

____

____

____

____

____

____

____

E-learning and E-literacy – *E-learning* refers to the use of electronic communications technologies for educational purposes; e-*literacy* refers to a person's ability to use these technologies 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. The question is how 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 that the developing countries being 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?

____

____

____

____

____

____

____

____

____

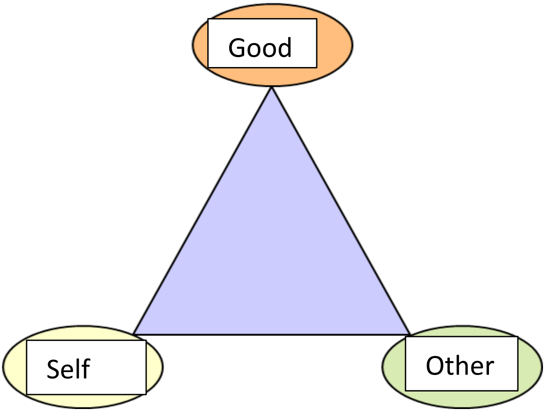
____

____

____

____

Ethic / ethical framework / code of ethics **–** A value system that governs one's behaviour and/or a field of study which focuses on moral and other 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 an anti-virus program. The ‘wall’ screens incoming information before allowing it through, thereby protecting the 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 a crime. 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 a 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 has decreased in the past month, he/she may use this information as a reason to cut financial spending for the coming month.

Information can be generated through research and experience; it can be shared, hidden, modified, analysed, synthesized, and manipulated. Information can also become outdated, or 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 are seldom globally competitive. In other words, people who do not have the skills or equipment to access information are essentially excluded from the Information Society. Organizations like UNESCO aim to create a more inclusive environment through empowerment.

____

____

____

____

____

____

Information Life Cycle – The cyclicalprocess 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 a device with the intention of stealing the user's password/s, deleting files, or reformatting the hard disk of the 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 to either 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. Don't click on these – 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 him / her as 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 another person’s human rights.

____

____

____

____

____

Responsibility – Doing what one is supposed to be doing and to show that be willing to accept the consequences of one’s actions.

____

____

____

____

____

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

____

____

____

____

____

____

Trojan horse – A program that you download without knowing that it includes a ‘back door’ which gives potential attackers access to a device

____

____

____

____

____

____

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

____

____

____

____

____

____

Value system - A set of values or unwritten rules that govern 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 the user's knowledge or permission *(see **Ten frequently asked questions** in Section 4).*

Worm – Like a virus but it does not infect the files. What it does is send copies of files from a computer 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 also a major Internet problem. In order to address this problem we need to know (a) what bullying is, (b) why certain children are inclined to bullying others, and (c) 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. Rumours like these would be very harmful to the victim's self-esteem and could in the long run. It could, for example, cause 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 anyone, 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 world or social media site 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 'share' hateful comments or malicious gossip about the victim's friends as if it came from the person they impersonated. The victim's friends, thinking that the messages came from him/her, would then either quarrel with him/her or refuse to be friends with him/her any longer. The victim is then isolated from his/her social network and could become very lonely.

- Bullies would pretend to befriend someone, gain his/her trust, and then do something to deliberately betray the trust. The person being bullied then becomes afraid of ever again trusting another person again. In the end, not having someone with whom they can share their deepest thoughts and feelings victims of bullying could either become so over-burdened that they consider 'ending it all' or so angry at society that they decide to take revenge. This 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.* By bullying others 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. Because of this 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.* When 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.

Third, why submit to bullying?

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.

Just as there are many reasons why someone becomes a bully, so there are many reasons why someone is targeted as a potential victim to bullying. 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 isweak, 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 online. 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 -***reallylisten*** - 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 them advice on what to do – unless you are 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 roomswhere 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 watch 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 to 'protect' them. 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 him/her uncomfortable, exposed 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: involve both parties - the bully and the bullied in deciding on a plan.

- ***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 nobody 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, ***contactcounsellors*** 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. (*go to* ***aka.ms/EffectivePrograms*** for *a list of well-tested programmes,)*

- Run a ***kindness campaign*** in your community – school, church, or street – in which people are encouraged to do one kind thing for someone else each day. The recipient of the '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 one of the reasons why you should NEVER share personal information with strangers.

SECTION 5: POLICY ON E-SAFETY IN SCHOOLS

We insert, with the compliments of the Department of Basic Education, for your convenience and consideration, a draft document towards the development of policy on *E- SAFETY GUIDELINES FOR SCHOOLS.*

Guidelines on e-Safety in Schools: Educating towards responsible, accountable and ethical use of ICT in education

basic education

Department:
Basic Education
REPUBLIC OF SOUTH AFRICA

Table of Contents

Introduction

An ever-increasing use of technology in society, both globally and locally, has allowed easier, faster and cheaper access to Information and Communication Technologies (ICT) like never before. This has resulted in digital 'citizens' of all ages having to acquire a new skills-set not taught using traditional methods and media. The pervasiveness of technology is often negatively publicised and the education system is responding positively by equipping all role players (teachers, learners and parents/guardians) with guidelines around the ability to recognise potential dangers and be discerning enough to avoid them.

The advantages of using ICT's for education far outweigh the disadvantages however; the latter need to be managed thoughtfully and responsibly in order to ensure the protection of our children. It is essential that schools are aware of how to manage the technology environment so that their learners have positive and safe experiences when using it and the learners, in turn, need to understand the implications of irresponsible use and need to be accountable for their behaviour. This can be done through proper Information Security (IS) education and awareness within schools.

It is essential that IS education is not confined to awareness of the risks and dangers of ICT's, but also includes an understanding of the benefits. The Safe School Committee[2] (comprising of all relevant stakeholders including school management), prescribed by South African Schools Act [3] should consider that while there are real dangers, too many limitations and controls can significantly decrease the positive aspects of access to technology. It is also essential that parents and guardians also need to share the responsibility as access to technology is not confined to the school walls, or solely to the time spent in the school environment.

The focus of the White Paper on e-Education[4] published in 2004 recognises the role that ICT can play in education, and by extension in lifelong learning and the development process. The larger society benefits

[2] Department of Basic Education Draft School Safety Policy 2010

[3] South African Schools Act No 84 of 1996

[4] White Paper e-Education 1994

from electronic education (e-Education) include learning-for-life, the communication and exchange that are essential to democratic living, and globally competitive human resources.

As South Africa improves access through affordable hardware, software and connectivity, so must guidelines be in place for proper implementation and management thereof.

1. Purpose

The e-Safety Guidelines seek to identify the different ICT's currently used by school communities in particular, teachers and learners and to recommend strategies around managing ICT's in order for the appropriate and optimum use in, and for, education. This can be done by identifying all role players involved and their role and responsibility toward electronic safety (e-safety).

2. Background

Media and technology are evolving at a rapid pace, bringing opportunities, challenges and risks that are new to this generation. We are living in a world of rapid change, economically, politically, socially and technologically. The advent of improved connectivity and thus access to ICT's (for example the Internet and cell-phones) highlights the necessity for strategies to be in place in order that school communities have a positive, safe and fruitful experience of utilising technology.

Cell-phones in particular, are endemic in this country having a far-reaching footprint, even in the most rural of areas, so education needs to be a step ahead in ensuring that learners are equipped to manage both the risks and the benefits.

The Internet is a largely un-policed environment; anybody can upload information either authentic or not, unlike a traditional library whereby books go through an editorial process thus ensuring quality of information. We therefore recognise the need to teach our learners information literacy skills and these include digital literacy. Finding, selecting and using information effectively and appropriately are essential in the information age. Teaching our learners to use the most appropriate communication tools for productive and wholesome interactions, as well as the development of their critical thinking skills, is a responsibility of teachers and parents/ guardians.

Equally, social network platforms provide unprecedented opportunity for building contacts and staying in touch with current events, developing an online identity for socialising, but the environment needs to be managed so that it does not predominate in the life of a learner.

It is essential that the value of the various platforms, devices and mediums is embraced in schools but it is equally important that education around the use thereof is intensive and thorough. Information literacy, and thus digital literacy, is about knowing what is available technologically speaking and selecting the most appropriate tools to find and communicate information in the most efficient, effective, responsible, safe and appropriate way possible. These are the skills required of the 21st century learner and global digital citizen.

Finally ethical use of information and communication platforms is a key aspect of education. The principles inherent in the Constitution and cited in the Bill of Responsibilities for the Youth of South Africa[5] are applicable in the online environment as anywhere else. Building the culture of responsibility, accountability and humanity in our schools also has application in the information age. Learners are, on the whole, proficient users of technology but are not necessarily worldly wise, it is for this reason guidelines are necessary.

3. Scope

The guidelines for e-safety in schools apply to all learners, teachers and school management, including School Governing Bodies (SGB's), within the context of schools in South Africa. These guidelines should also assist parent/guardians to ensure that their children are e-safe. Provincial Department of Education officials and District officials should also be familiar with the document, and support the implementation of it in schools.

4. How to best use these guidelines

The Department of Basic Education (DBE) acknowledges that while it is important to formulate guidelines on safety in schools, this document

[5] A Bill of Responsibilities for the Youth of South Africa 2008

cannot be a comprehensive document to address all matters of safety in schools.

The DBE like to acknowledge other contributions by Educationalists, other Government departments and private sector to fully research, comprehend and address the challenges related to e-safety in schools.

The DBE thus would like to see this document to form part of, and enhance other projects with the same objectives. In practice this implies that the DBE would like to refer the readers of this document to also take note of the Digital Wellness Toolkit that was developed by the ACEIE, University of Pretoria and Intel. This toolkit complements the guidelines as set out in the e-Safety guide for schools, by providing practical ideas of implementation.

5. Acronyms

AUP	Acceptable Use Policy
CSRT	Cyber Security Policy (CSRT).
DALRO	Dramatic, Artistic and Literary Rights Organisation
DBE	Department of Basic Education
DVD	Digital Video Disk
FAQ	Frequently Asked Questions
FET	Further Education and Training
FPB	Film and Publications Board
GET	General Education and Training
ICT	Information and Communication Technology
IS	Information Security
IT	Information Technology
SAMRO	Southern African Music Rights Organisation
SAPS	South African Police Services
SGB	School Governing Body
SMS	Short Message Service
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
URL	Uniform Resource Locator

6. Glossary and Definitions

- Asynchronistic: occurs at different times e.g. e-mail conversations
- Blogs: Weblogs (blogs) are online journals created by individuals or groups and stored on the Internet. They are usually text based, but

also include other media such as images, video and sound content. Blogs are an ideal space to write about personal ideas and opinions

- Browsers: tools to access the Internet
- Cloud computing: term used to describe delivering hosted services such as infrastructure, platform and software services to other devices on demand. It lessens the work the local machine
- Communities of Practice (CoPs): a group of people who have a common interest or profession and who communicate and share information.
- Cyber bullying: Harassing, humiliating or threatening someone in cyber space, by sending them nasty e-mails, posting malicious information, fake profiles or embarrassing photographs or comments on social networking sites.
- Cybercrime: computer crime or cybercrime is a form of crime where the Internet or computers are used as a medium to commit crime
- Cyberspace: the global network of interconnected computers and communication systems
- Cybersecurity: computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users
- Cyberstalking: individuals who keep track of user's activities and information
- Creative Commons licences: these licenses allow creators to communicate which rights they reserve, and which rights they waive for the benefit of sharing
- Dark Web: 'is World Wide Web content that exists on dark nets, networks which overlay the public Internet and require specific software, configurations or authorization to access and are often used for illegal or criminal activity. The Dark Web forms part of the Deep Web, the part of the Web not indexed by search engines. Wikipedia [Accessed August 2015]
- Digital image: an image created by digital technology such as a digital camera, or imaging editing software
- Digital Literacy: the ability to find, discern, select and use online information appropriately.

- Digital footprint: the collection of data, which includes images, videos and text, posted by an individual online
- e-Education: consists of e-Learning, e-Teaching, e-Awareness and all the administrative responsibilities connected to these actions
- e-Learning: a broad term that generally refers to any kind of learning that is done with a computer and Internet connection or CD-ROM. It is widely used by individuals, educational institutions and businesses. e-Learning includes m-Learning.
- e-Mail: electronic mail, most commonly abbreviated email and e-mail, is a method of exchanging digital messages
- Filtering: a process to deny access to certain websites or resources as defined in the filter
- Firewall: part of a computer system or network that is designed to block unauthorised access while permitting authorised communications
- Flaming: hostile and insulting interaction between Internet users
- Internet: a worldwide network that connects smaller networks together
- Information literacy: the ability to recognise the need for information; to find, organise and evaluate such information for effective decision making or problem -solving, to generate new knowledge and to apply these skills for effective life-long learning
- Information skills: the skills which underpin a learner’s ability to define the purpose of an information task, locate resources of data, select, interpret and use information to complete a task
- IT (Information Technology): defined as the “study, designs, expansion, execution, preservation or supervision of computer based information systems, specifically on computer hardware and software functions
- ICTs (Information and Communication Technologies): defined as forms of technologies that are used to create, store, share or transmit, exchange information; radio, television, video, DVD, telephone (both fixed line and mobile phones), satellite systems, computer and network hardware and software; as well as the equipment and services associated with these technologies, such as videoconferencing and electronic mail (UNESCO 2002)
- Inter-operability: the degree to which different types of software and hardware can interact effectively with each other

- Malware: a malicious or intentionally or unintentionally damaging software programme
- Media: message and images that we consume and create, as well as the technology used to consume and create these messages. These include television, movies, video games, books, magazines, the Internet, cell-phones and more
- m-Learning: a broad term that generally refers to any kind of learning that is done with a cell-phone, supplied directly on the cell-phone, as an application, game or similar content – or accessed via the Internet. It is widely used by individuals, educational institutions and businesses
- Multimedia: media that combine media of communication (text and graphics and sound etc.)
- Netiquette: Netiquette is a set of social conventions that facilitate interaction over networks, ranging from mailing lists to blogs and forums
- Phishing scams: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- Plagiarism: "the wrongful appropriation, close imitation, or purloining and publication, of another author's language, thoughts, ideas, or expressions, and the representation of them as one's own original work”, Wikipedia [Accessed August 2010]
- Social Media: user-created communication and content that may take the form of video, audio, text or multimedia that are published and shared in a social environment, such as a blog, wiki or video hosting site
- Social Networking: online platforms that provide means of personal communications between participants such as FaceBook, LinkedIn, Twitter, Buzz and many others
- Spam: is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately
- Spoofing: Spoofing, or decoying, is the practice of inundating online networks with bogus or incomplete files of the same name in an effort to frustrate traders and reduce unlawful downloading
- Synchronistic: things occur at the same time e.g. online chat

- URL (Uniform Resource Locator): address that identifies a specific website e.g. http://www.education.gov.za
- Viral branding: refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness or to achieve other marketing objectives (such as product sales) through self-replicating viral processes
- White-list: An approved list; often used with regard to Internet content filtering, a whitelist only includes addresses (such as URLs or e-mail) that have been specifically vetted in advance

7. Acknowledgements

External advisors

Child Welfare SA

Cyanre

Department of Telecommunications and Postal Services(DTPS)

Department of Justice and Constitutional Development

Department of Social Development

Film and Publications Board (FPB)

Department of Home Affairs

Meraka Institute

Africa Centre for Excellence in Information Ethics (ACEIE) University of Pretoria

Microsoft

MTN SA (Pty) Ltd

MXit

Oracle

SA Law Reform Commission

SchoolNet

South African Police Service (SAPS)

Vodacom

Intel

Department of Basic Education

Directorate: Curriculum Innovation
Directorate: FET Schools
Directorate: Gender Equity
Directorate: School Safety and Enrichment Programmes

Critical Readers

Ms J Batchelor	Head IT Integration Cornwall Hill College
Ms M du Toit	Independent
Dr E Kritzinger	Senior Lecturer: School of Computing UNISA
D Nicholson	Copyright Services librarian: University of the Witwatersrand, Johannesburg
Dr P Miller	Pinelands High School
Dr H Vermeulen	University of Cape Town
Ms M Verster	Educational Technologist
Mr S Vosloo	Shuttleworth Foundation

8. Regulatory Framework

Legislation

Act No. 11 of 1967	Performers' Protection Act
Act No. 42 of 1993	Animal Matters Amendment Act
Act No. 108 of 1996	Constitution of the Republic of South Africa
Act No. 65 of 1996	Films and Publications Act
Act No. 84 of 1996	South African Schools Act
Act No.13 of 2000	Independent Communications Authority of South Africa Act
Act No. 70 of 2002	Regulation of Interception of Communications and Provision of Communication-Related Information Act
Act No. 36 of 2005	Electronic Communications and Transactions Act
Act No. 38 of 2005	Children's Act
Act No. 31 of 2007	Education Laws Amendment Act
Act No. 32 of 2007	Criminal Law (Sexual Offences and Related Matters) Amendment Act
2008	A Bill of Responsibilities for the Youth of South Africa
B9 – 2009	Protection of Personal Information Bill

Policies
2010 Cyber Security Draft Policy: Department of Communications
2010 School Safety Draft Policy: Department of Basic Education

9. Advantages of ICT access in schools

In the South African context, the concept of e-Education revolves around the use of ICT to accelerate the achievement of national education goals. e-Education is further about connecting learners to other learners, teachers and related professional support services. e-Education connects learners and teachers to more information, ideas and one another via effective combinations of pedagogy and technology. The challenge is to transcend mere exchange of information and to transform it into a range of learning activities that meet educational objectives. e-Education is more than developing computer literacy and the skills necessary to operate various ICT's.

It is the ability to apply ICT skills to access, manage, integrate, evaluate, and create content in order to enhance teaching and learning and to function in a knowledge society. ICT capable learners are able to access information in the digital era, manage information effectively, interpret and integrate the results of research, evaluate the quality of these results, and create new content by adapting, applying, designing, inventing, or authoring information.

Success in the infusion of ICT into teaching and learning will ensure that every learner will be equipped for full participation in the knowledge society before they leave school. These learners will use ICTs to enhance interaction between citizens, governmental organisations and public and elected officials. These learners will invent new ways of using ICTs to realise the Department of Basic Education's vision of developing a lifelong learner who is a critical and an active digital citizen and who embodies the fundamental values of the constitution.

10. Issues of concern regarding ICT access in schools

The Byron Review[6] has classified the risks of ICT use as relating to **content**, **contact** and **conduct**. The risk is often determined by **behaviours** rather than the technologies themselves.

	Commercial	**Aggressiv e**	**Sexual**	**Values**
Content (child as recipient)	Adverts Spam Sponsorship Personal information	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting Personal information	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal: Downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

10.1. Online harassment and cyber bullying

Some aspects of digital communication can give rise to unfortunate behaviour. These include;

- The ability to communicate anonymously and so to escape responsibility for one's actions.
- The ability to communicate remotely thus not having to deal with a "face to face" confrontation where the normal rules of politeness might inhibit unpleasant behaviour.
- The public nature of social media and social networks, which makes it easy to publically humiliate an individual with little or no consequence.

[6] Byron Review, 2008: Available at http://www.dcsf.gov.uk/byronreview

- An invasion of privacy if messages sent to/from an individual are released into the public domain

Cyber bullying can include the repeated sending of unwanted communication; “cyber stalking” as well as the posting of offensive statements about other learners or about teachers using any of the digital mediums that can make learners, and teachers, feel embarrassed, upset, depressed, or afraid. Groups and cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member, can quickly escalate into something much more serious. It should be made clear to all that bullying using digital means is still regarded as bullying and carries serious consequences according to the Acceptable Use Policy of the school.

It must be noted that bullying of any kind is a social problem and is thus a whole school responsibility. Normal courtesy and good manners apply as much in the cyber world as the real world.

10.2. Inappropriate or illegal online behaviours

Young people may get involved in other inappropriate, anti-social or illegal behaviour while using new technologies. The teaching of appropriate behaviours and critical thinking skills to enable learners to remain both safe and legal when using the Internet and related technologies is essential. Young learners who have been engaging in risky or illegal behaviours online may benefit from professional support or counselling to redress the balance of their online and offline life. Some children may become involved in much more serious activities. Possible risks include;

- Involvement in identity theft;
- Participation in hate or cult websites;
- Buying and selling of stolen goods and drugs;
- Divulging personal information online; and
- Publishing compromising information which may harm an individual’s reputation

Learners should be aware of the consequences of leaving “online tracks” often called a Digital Footprint i.e. information about themselves that may damage their reputations and employment opportunities.

It is also essential for learners to take charge of protecting their own privacy, and avoid posting any information which can be used by identity thieves. Identity theft is a very real risk that has significant personal and financial cost. Learners should be made aware of safety and privacy measures that exist on social networking sites; these can include a “Report Abuse” button, safety tips, age restrictions, built in privacy controls etc.

10.3. Physical danger and sexual abuse

A criminal minority make use of the Internet and related services such as “chat-rooms” to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity and exploitation. Cyber stalking is where individuals keep track of the activities of certain people through their participation on social networking sites. This can result in physical stalking if their whereabouts are revealed online. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online friendship. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to a meeting in person or even persuading a young person to forward explicit photographic images of him/herself or another young person, or even just to participate in communication of a sexual nature. These techniques are examples of criminal conduct and adult persons who commit such acts can be convicted of the “sexual grooming” of children.

A young person needs to understand that it is unwise to supply personal information, pictures of an explicit nature or arrange to meet people they have met online, thereby posing a risk to their safety or that of their family or friends. Furthermore the online world offers a degree of anonymity and the online persona of a person, under these circumstances, is far removed from reality, hence learners need to understand this.

10.4. Exposure to unsuitable materials

Exposure to inappropriate materials poses a risk when using the Internet. This may include, but is not limited to, material that is pornographic, hateful or violent in nature, activities that are dangerous or illegal, or material that is just age-inappropriate or biased. One of the key benefits of the Internet is that it is open to all, but unfortunately this also means that those with extreme views are able to share their ideas without restriction or consideration of other views. In the case of pornography the Internet plays host to a large amount of material. Curiosity about sexuality issues is a normal part of sexual development, but young people may be shocked by some of the overtly explicit material online. The ease of access to adult sites such online gambling, making and sale of weapons, and sites providing recipes for drug or bomb making are also of great concern. This space is often referred to as the “Dark Web”

Through mobile devices such as cell-phones and tablets, young people may themselves become perpetrators in the creation of inappropriate content by the making and distribution of indecent images, videos and derogatory lists. They also might not actually create the content but may view and thus be exposed to unsuitable material or be the victim of such abuse of technology.

10.5. Plagiarism and copyright infringement

Copyright law applies on the Internet, but is ignored by many young people who download and swap music files, “cut and paste” homework assignments from other’s work, purchase whole assignments from online “cheat sites” and are doing so without realising the implications and consequences. The school needs to ensure that assignments are given in such a way as to not invite a “cut and paste” response but have activities within that require primary research, problem-solving and other higher-order thinking skills as opposed to merely superficially ‘grazing’ for information. Learners must be taught that credit must always be given to the source of information and pirating music, images, videos or software is not only unethical but is dishonest and illegal. Available referencing and citation programmes can help instil correct research methodology as must teachers critically evaluate what is expected from the learner.

Social networking platforms have created an environment whereby information is shared without necessarily giving credit to the source. The democratisation of information i.e. everybody has an equal voice, is one of the most valued aspects of recent technologies. It has however, blurred the edges of respect for intellectual capital and anybody who ventures into the environment needs to understand that their opinions might not necessarily be given credit to them.

10.6. Obsessive use of the Internet [7]

Habitual use or addictive behaviour in the online world creates the potential for learners to become obsessed with the Internet or cell-phone chat services and related technologies. Factors such as spending a significant amount of time online, deterioration of the quality of schoolwork, diminished sleep time, or negative impacts upon family relationships, may all be indicative that the online world is taking too high a priority in a young person's life and can intrude excessively if not managed properly.

Another aspect of misuse of the technology is the circulating of band-width intensive e-mail (large file attachments) which are unrelated to the school working environment, chain letters etc. Beyond compromising the speed of connectivity, the time taken on managing inappropriate and personal activities during school working hours can be costly to the performance of both the learner and teacher.

11. Responsibilities

Although these guidelines have been written specifically with schools in mind it is also essential that Provincial and District officials take cognisance of the content and apply it in their own situation where relevant. Ethical and accountable use of technology applies at district level as well as in the schools. They should also support the school in implementation of the guidelines.

[7] Safer Children in a Digital World: the report of the Byron Review - Children and New Technology 2008

11.1. The Responsibility of the School

Technology, as per its broadest meaning, has an imperative role in today's classrooms. The use of that technology, however, must be carefully and strategically implemented in order to be of highest value to both teachers and learners. Technology use has a place in formal and informal learning; it does not only happen in the classroom but outside of the school environments. Traditional controls no longer exist and schools need to embrace the potential of technology for learning through using appropriate measures.

Recognising that the use of technology will increase exponentially in all our lives, the responsibility of the school is to not only incorporate technology as a valuable learning tool, but to also equip the learners to be discerning, responsible and ethical participants in the information age.

Through the Safe School Committee schools must develop their own Acceptable Use Policy (AUP), as it must be recognised that children will bring an increasingly sophisticated range of handheld devices into school giving them separate access to content that is not necessarily appropriate. The AUP should be linked to, and the penalties defined by, the existing Code of Conduct[8] that must be adopted by every public school.

The AUP should clearly define the penalties imposed for violation of the agreement and this should be read and signed by every learner and responsible parent or guardian. The school must keep the copies signed by the learner and the parent/guardian and all signatories should have access to a copy via the school Intranet or otherwise. A simplified version of the AUP should be posted in the staffroom and also on the screen of all the computers. In order to create a sense of personal responsibility it is important that wording is values-based as opposed to rules-based.

As misuse of technology is not necessarily confined to learners, schools can elect to have a similar policy for teachers. The AUP policy of a school will have to be revisited once the Protection of Personal Information Bill, 2009, is enacted. The Bill aims to regulate the processing of personal information by public and private institutions and will, among others, regulate unsolicited electronic communications such as "spam". An

[8] South African Schools Act (Act No 84 of 1996 amended 2007)

Information Regulator will be appointed to oversee the implementation of the legislation. AUP policies may, therefore, in future, have to be adapted with the assistance of the DBE and Information Protection Regulator to ensure that they are brought in line with the legislation concerned, where necessary.

11.2. The Responsibility of the Teacher

Teachers have a specific responsibility in terms of the use of ICT in schools. Partnership for 21st Century Skills.[9] specifically refers to information literacy as well as ICT literacy. Learners are increasingly using their cell-phones to communicate, share and find information and teachers need to understand the concept of the 21st century learner, especially to ensure that their teaching strategy is in line with the devices their learners use. Teaching and learning can be greatly enhanced with increased access to communication and information and this potential needs to be maximised by teachers. Integrating technology appropriately into teaching practice is important; a 'just-in-time' approach within a contextualised learning environment versus "just-in-case" i.e. learning computer skills in case they may be needed in the future. An additional responsibility of the teacher is to make sure that they themselves are digitally literate and can educate around the technology with confidence.

Teachers can direct learners to age appropriate content and web browsers; they can also create White Lists of carefully selected websites appropriate to the topic and the age group. Telling learners to "Google" a topic i.e. use a single search engine to find information, is the equivalent of exposing them to a massive library with no information retrieval skills, furthermore the most benign topic can elicit inappropriate material.

It is further suggested that teachers may need to provide guidance, counselling and advice to learners who may be dealing with harassment, stalking, cyber bullying etc.

A further aspect of the responsibility of the teacher is to not abuse access to technology for personal matters, doing time consuming non-work related activities, circulating bandwidth intensive files and images which do not benefit the learners or the school, using school printers for personal use

[9] Partnership for 21st Century Skills http://www.p21.org/

etc. Leading by example in the ethical use of technology goes a long way in educating learners.

11.3. The Responsibility of the Learner

Learners today are navigating social networking websites, downloading music, uploading photos and videos, e-mailing, blogging, building personal websites, and playing online games with people from around the world. Online and user-generated media, whether it is television, cell-phone, online games or videos is especially challenging because there are few barriers to what can be posted and made available, and that can make for offensive content.

Learners are however, at different levels of sophistication and this can negate a positive global experience. The nature of technology, especially interactions predominantly in a second language for the majority of our learners, can give rise to misinterpretation and misunderstandings.

Learning to take responsibility for one's behaviour is an important element in the education path and this includes the use of technology. The ease of access can invite an inappropriate, spontaneous reaction and it is important that learners understand the need to select the most suitable communication tool to resolve issues and not create them. An aspect of taking responsibility in the environment is to report any inappropriate behaviour especially if offensive acts are negatively affecting a fellow learner.

11.4. The Responsibility of the Parent/Guardian

Parent and guardians have a responsibility to monitor the use of technology both in the home and outside of it. This is difficult to do, especially with cell-phones, but if children and young adults are educated around the use of technology and the education is values-based versus rules-based then this can go a long way to ensuring the healthy and balanced use of the devices.

It is possible to set up age appropriate content filters on Internet browsers and it is also possible to check the cache (browsing history) on a computer if it is felt necessary to do so. The technology enables parents/guardians to password protect either a computer or online facilities like "chat rooms" even through cell-phone access. This prohibits children of a sensitive age from accessing these areas.

There is filtering/monitoring software that can be downloaded but children and young adults need to be informed that their activity is being checked upon. It is important that the school is supported by the parent/guardian in respect of any sanctions imposed if the school AUP has been breached.

Parents/guardians are encouraged to disallow children from using or accessing the Internet in isolation or behind closed doors. A suitable family area should be set up for such usage and this includes access to television. Furthermore parents/guardians should discourage their children from publicly divulging personal information such as contact details and whereabouts.

12. Strategies for managing ICT access in schools

It is very important that a school sets up a team within the Safe School Committee to manage e-Safety and this team should consist of at least;

- School Management
- Network administrator
- IT teacher
- Teacher-Librarian/Counsellor/Life Skills teacher
- School Governing Body representative
- A member of the local police service
- Learner representative
- Other appropriate specialists

The function of the team is to develop, implement and enforce an Acceptable Use Policy/ies (AUP) for the school with attendant penalties for breach of such a policy.

12.1. Acceptable Use Policies (AUP's)

It is strongly advised that each school, as part of the function of the Safe School Committee, develops an Acceptable Use Policy and all learners should be required to sign it, indicating that they accept the policy and related sanctions. Alternatively, two separate policies can be developed, learner specific and teacher specific. It is further advised that the Acceptable Use Policy/s should include a clear statement of the actions, which the school will take if the policy is breached. This will considerably strengthen the school's position should this situation arise.

The policy/s should be endorsed by a credible legal service to ensure that it is implementable in terms of the legislation and also that Child Protection procedures are followed. South African Police Services (SAPS) has guidelines in this regard.

All role players must be made aware of the content and consequences of the policy. Parents/guardians should take all reasonable steps to ensure that their children comply with the requirements.

There are basically three levels of issues surrounding the use of technology. First, there are the problems associated with nuisance in classes and disruption of learning and teaching. Second, there is the type of incident, which has potentially criminal implications. Third, there are incidents with specifically child protection dimensions. An Acceptable Use Policy must therefore address all three levels.

The suggestion is offered that the policy might explicitly cover the following:

- The school's responsibility and rights towards ICT use;
- The learner's responsibilities and rights towards ICT use;
- The parent/guardians responsibility and rights towards ICT use; and
- The consequences if the policy is not adhered to.

It is stressed that in cases, which are disciplinary in level, school disciplinary procedures (including exclusions when required) should be used proportionally and appropriately. In other cases, it is best for schools to work constructively with parents/guardians. In connection with these issues, the normal rules and protocols apply with regard to the rights of schools to take action over behaviour, which is school-related but which actually occurs out of school.

12.1.1. School Software Security

There are several ways that a school can manage online security and it is important that a strategy is in place. The two main elements are to ensure that school computers are protected from viruses and malware and also that online behaviour on the part of learners and teachers is managed.

12.1.2. Antivirus Software

Antivirus software should be installed on the school server/individual computers and not only the software definitions updated online on a regular basis but the computers regularly scanned. Furthermore peripherals such as memory sticks/flash drives, external hard drives etc should also be scanned as this is a common way for viruses to be introduced into a system.

Proprietary antivirus software normally entails the payment on an annual licence fee and this range from a single-user licence to multiple-user licence.

There are free antivirus software programmes available on the Internet. Furthermore there are online detection programmes which scan computers whilst linked on the Internet.

It is vital that antivirus software is current and regularly updated, checked and computers are scanned. There is no use in having antivirus software if it is not properly managed.

12.1.3. Monitoring software

This can be installed on computers so that online activity can be monitored. There are many commercial programmes available as well as Open Source classroom management programmes.

A programme should be selected on the basis of controlling online behaviour through documenting and recording for the purpose of pastoral intervention versus punishment and/or banning. Users (learners and teachers) must be informed at the outset that their online activity is being monitored. The purpose is to provide a sage online environment which educates users how to manage their access.

In addition to informing users (learners and teachers) of the fact that monitoring is taking place, they should also be informed, within the AUP, of the following:

- Exactly what data is captured by the monitoring software?
- How long is this data kept
- Who has access to this data

- How the data will be kept safe so that unauthorised users cannot access it
- What mechanisms there are to ensure the data is accurate
- How this data can be used.

The issues discussed above must be set out and explained in the AUP.

12.1.4. Document Security

In keeping with the points in 12.2.2, included in the AUP should be a reference to document security and the confidentiality of school documentation. It is known that businesses have been compromised through the deletion or inappropriate copying or forwarding of information and this has to be a consideration for schools. A system for password access for different user groups needs to be created and certain documents need to be secured, either password protected or using software such as Adobe Acrobat. Information security requires that information on learners stored on the school network is secure.

Computer hacking by mischievous learners is another element of school ICT security and it is for this reason that the identity of all users is kept. It must be impressed on learners that their password is confidential and that they must log off before leaving a computer.

It is also advisable that an on-site and off-site backup of all the school data is kept and is regularly updated. Hardware failure happens as does theft and fire. The backup also needs to be tested on a regular basis.

13. Conclusion

Through the development and implementation of these guidelines it is hoped that schools are equipped to manage ICT in a positive and productive way. ICT's are part of the lives of the 21st century learner and will increasingly impinge on society. There is no choice but to embrace the attributes of technology and use them to enhance the education, communication and knowledge acquiring process. Education wants to develop global digital citizens who are confident users who collaborate and participate but who know the boundaries and respect decent behaviour.

14. References

Byron, T. 2008 *Safer Children in a Digital World: the report of the Byron Review - Children and New Technology* [Online]. Available: http://www.dfes.gov.uk/byronreview/ [22 August 2010]

Palfrey, J. et al 2008 *Enhancing Child Safety and Online Technologies: final report of the Internet Safety Technical Task force* (Berkman Centre for Internet & Society at Harvard University) [Online]. Available: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf[26 November 2010]

Prensky, M. 2001. *Digital Natives, Digital Immigrants*. From: *On the Horizon* (MCB University Press, Vol. 9 No. 50).

Trilling, B and Fadel C. 2009, *Partnership for 21st Century Skills: Learning for Life in Our Times.* Jossey-Bass. New York. (http://www.p21.org/)

White Paper on e-Education. 2004. National Gazette No. 26734, 26 August 2004.

Digital Wellness Toolkit. 2015. ACEIE [Online]. Available: http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics/article/2109737/digital-wellness-toolkit

Some Internet sites

Ask About Games	http://askaboutgames.com/
Becta e-Safety	http://www.becta.org.uk
Bloxx Web Filtering and Content	http://www.bloxx.com
Byron Review	http://www.dcsf.gov.uk/byronreview/
Child Exploitation and Online Protection Centre	http://www.ceop.police.uk/
Child Exploitation and Online Protection Centre	http: www.thinkuknow.org
Childnet International	http://www.childnet-int.org/
Classwatch	http://www.classwatch.co.uk
Forensic Software	http://www.forensicsoftware.co.uk
I am Learning	http://www.iamlearning.co.uk/home.php
Impero Classroom Management	http://www.imperosoftware.com/
Information Security Awareness Portal	http://www.securityportal.co.za
Internet Watch	http://www.iwf.org.uk
Italc: Open Source Classroom management system	http://italc.sourceforge.net/home.php
Learning Curve Education	http://www.learningcurve.info/
MXit Safety Guidelines for Learners and Parents	http://www.mxit.com
Plagiarism Advice	http://www.plagiarismadvice.org

South West Grid for Learning Trust	http://www.swgfl.org.uk/staying-safe
Wikipedia list of antivirus software	http://en.wikipedia.org/wiki/List_of_antivirus_software
Wits Plagiarism Portal	http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Plagiarism+Portal.htm
Wits Copyright Information	http://web.wits.ac.za/Library/Services/COPYRIGHT.htm
Wits Copyright Portal	http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Copyright+and+Related+Issues.htm

15. ANNEXURES

15.1. Examples of Acceptable Use Policies

15.2. Information sheets

ANNEXURE A: The Acceptable Use Policy (AUP) for ICT in a School

1. Developing an Acceptable Use Policy (AUP) for ICT in a school

The Acceptable Use Policy (AUP) for Internet use is one of the most important documents a school will produce. Creating a workable AUP requires thoughtful research and planning.

With the current push for computer technology in the classroom, many educators and parents fear dangers that the uncensored access to technology might hold for children: inappropriate or obscene words and images; violence; and people who pose an online threat.

One strategy that many schools use to defuse such dangers is an Acceptable Use Policy, or AUP, for the school.

WHAT IS AN AUP?

The Department of Basic Education suggests that an effective AUP contains the following six key elements:

- a preamble,
- a definition section,
- a policy statement,
- an acceptable uses section,
- an unacceptable uses section, and
- a violations/sanctions section.

The **preamble** explains why the policy is needed, its goals, and the process of developing the policy. This section should say that the school's overall code of conduct also applies to learner online activity.

The **definition section** defines key words used in the policy. Words and terms such as Internet, computer network, education purpose, and other possibly ambiguous terms need to be defined and explained to ensure learner and parent comprehension.

A **policy statement** must tell what computer services are covered by the AUP and the circumstances under which learners can use computer services. Schools may, for example, base learner access to computer services on the completion of a "computer responsibility" class that will enhance learner understanding of the AUP guidelines.

The **acceptable uses section** must define appropriate learner use of the computer network. It may, for example, limit learner use of the network to "educational purposes," which then must be defined.

In the **unacceptable uses section**, the AUP should give clear, specific examples of what constitutes unacceptable learner use. In determining what is unacceptable, the committee charged with drafting the AUP must consider:

- what kind of computer network sites, if any, should be off limits to learners;
- what kind of learner sending, forwarding, or posting of information, if any, should be prohibited,
- what kind of learner behaviour will be destructive to the computer network services and should, therefore, be restricted.
- ensure that learners understand and apply the feelings, rights, values and intellectual property of others in their use of technology in school and at home;
- understand what action should be undertaken if they feel threatened, worried, uncomfortable, vulnerable or at risk whilst using technology

Among the sites that might be off limits to learners are chat rooms and examination paper vendors. In addition, AUPs often prohibit learners from sending, forwarding, or posting sexually explicit messages, profanity, and harassing or violent messages.

The **violations/sanctions section** should tell learners how to report violations of the policy or whom to question about its application. The AUP should provide that violations will be handled in accordance with the school's general learner code of conduct.

A typical AUP has a section where learners and parents sign the document, in acknowledgement that they are aware of learner’s restrictions to network access and releasing the school of the responsibility for learners who choose to break those restrictions.

In a free and democratic society, access to information is a fundamental right of citizenship, and therefore independent learner use of telecommunications and electronic information resources will be permitted upon submission of permission forms and agreement forms by parents of minor learners (under 18 years of age) and by learners themselves. The message should thus be that learners have intellectual freedom based on their taking responsibility for accepting limits to that freedom.

SAFETY FIRST

AUPs should make learners aware of basic information and communication technology safety rules before they are allowed access independently. The rules should be considered to guide independent use by learners, such as:

- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I 'meet' online without first checking with my parent/guardian. If my parent/guardian agrees to the meeting, I will make sure it is in a public place and I will bring my parent/guardian.
- I will never send a person my picture or anything else without first checking with my parents.

It must be remembered that an AUP cannot be developed in a vacuum. A vital, workable Acceptable Use Policy must be based on a philosophy that balances freedom and responsibility. It should be a values-based document as well as that aimed at protecting the individual.

Schools must be prepared to:

- develop an 'acceptable use policy,' (AUP);
- provide examples of AUPs from schools and libraries;
- respond to inaccurate perceptions of inappropriate material;
- promote positive examples of use;
- understand software to block inappropriate sites and related safety/censorship issues;

- contact organisations committed to electronic freedom of information; and
- ensure there are appropriate pre-screened resources available to learners.

Example 1: A PRIMARY SCHOOL INTERNET ACCEPTABLE USE POLICY

Name of School :

Section A: Expectations

Whilst the Information Technology (IT) department has many stringent checks and controls in place, the Internet is a vast and continuously growing arena and as such there are some sites and images that may escape the schools scrutiny and it is in this area that the children need to be responsible and educated in their responses.

Learners are responsible for their own behaviour on the Internet just as they are in a classroom, on the sports field or on the playground. Communications and interaction on the internet are often public in nature and general school rules for behaviour and communications will apply. This includes their interaction with other learners on social networking sites such as Facebook, MXit, Twitter etc. even if accessed from home, as they are still learners of name of school and are expected to uphold the ethos of the school.

The use of the Internet is a privilege, not a right, and may be revoked if abused.

Learners are personally responsible for their actions when accessing and using the school computer resources. Learners are advised never to access, keep or send anything that they would not want their parents / teachers or anyone else to see. It is expected that the learners will follow and comply with rules set out below.

Acceptable uses

As internet facilities are a limited resource and one for which the school pays, users are expected to use them primarily for:

1. Direct educational purposes
2. Accessing information for private interests or hobbies which are school related
3. Constructive communication with other Internet users and email recipients

Section B: Unacceptable uses

Users are not to:

1. Take part in the sending or resending of chain letters.
2. Use bad, offensive or derogatory language, or participate in any activities which discredit another child, in any communications over the internet.
3. Attempt to access or send attachments of any pornographic or socially unacceptable content. This includes racist, violent, harmful and bullying content.
4. Use any other user's Email account or logon.
5. Attempt to spread viruses or download programmes or games or malware of any kind.

In addition, when using the school's network, internet and email facilities, learners must understand their responsibility and behave in the following manner:

1. All users are entitled to the privacy of their work and therefore it is an offence to use or attempt to use another user's account or password.
2. Should a site, email message or image manage to bypass the safety controls it is the learner's responsibility to close the item and report it immediately to a staff member, to enable the blocking of the material.
3. Storage capacity is at a premium and learners are encouraged to conserve space by deleting unnecessary emails or saved pictures and documents that take up space on the server.
4. Learners must in no way attempt to "hack into" or interfere with the normal running of any other computers or networks.
5. Learners have full responsibility for their user accounts and must not share their passwords with anyone other than their parents. If they do and their account is used for breaking any of the acceptable use policy and it is traced to their username they will be solely responsible as the owners of the account.
6. Learners must be aware that excessive usage and their internet activities are logged and can be traced.

7. Printing is costly and learners must be aware that they have the privilege of a printing account and should they exceed this by printing private matter they will have to purchase a “recharge” voucher.
8. The computer staff, general staff, management and the Principal reserve the right to investigate any child’s email or Internet usage who, in their opinion may be transgressing any of the rules in this policy.

We have read this document, discussed and understood its contents and agree to abide by them:

Learner’s name: ______________________
Date:_________________

Learner’s signature: ______________________
Date:_________________

Parent’s/ guardian’s name: __________________
Date:_________________

Parent’s/ guardian’s signature: __________________
Date:_________________

Example 2: MODEL OF AN ACCEPTABLE USE POLICY FOR ICT IN A SCHOOL

The school's information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

Learners must:

- Respect and protect the privacy of others.
- Use only assigned accounts.
- Not view, use, or copy passwords, data, or networks to which they are not authorized.
- Not distribute private information about others or themselves.
- Respect and protect the integrity, availability, and security of all electronic resources.
- Observe all network security practices, as posted.
- Report security risks or violations to a teacher or network administrator.
- Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
- Conserve, protect, and share these resources with other learners and Internet users.
- Respect and protect the intellectual property of others.
- Not infringe copyright (not making illegal copies of music, games, or movies!).
- Not plagiarise.
- Respect and practice the principles of community.
- Communicate only in ways that are kind and respectful.
- Report threatening or discomforting materials to a teacher.
- Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).

- Not use the resources to further other acts that are criminal or violate the school's code of conduct.
- Not send spam, chain letters, or other mass unsolicited mailings.
- Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Learners may, if in accord with the policy above

- Design and post web pages and other material from school resources.
- Use direct communications such as IRC, online chat, or instant messaging with a teacher's permission.
- Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher.
- Use the resources for any educational purpose.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a learner's privileges to use the school's information technology resources.

Supervision and Monitoring

School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any learner or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:

______________________________ ________________________

Learner Date

______________________________ ________________________

Parent/Guardian Date

Parents please discuss these rules with your child to ensure he or she understands them.

These rules also provide a good framework for your child's use of computers at home, at libraries, or anywhere.

ANNEXURE B

The following are guidelines on different media platforms, tools and content including Copyright issues.

Television Programmes

***Description**:* **Television (TV) is a medium for transmitting and receiving moving images, usually in colour and accompanied by sound.**

Uses: Television programmes can be used for education as well as entertainment. Documentaries, films and reality programmes can be used as a resource in the classroom as well as specially designed programmes aired to support the curriculum. At present there are existing education channels specifically to support education in South Africa.

Advantages: Television programmes can have a far reaching impact on learning. Well made, informative programmes can be an invaluable tool in ensuring an enriching and relevant learning environment. Locally developed programmes can be in the vernacular and contextualised for the local cultural and geographical environment.

Considerations:

- Access to television, especially subscription television is not always available to all learners and teachers.
- Advertisements can be intrusive and disruptive. They can also be inappropriate to the age of the learner.
- Licences for multiple viewers can be expensive.
- Programmes made in other countries do not always support local culture, language and traditions.
- Making television programmes is a time intensive and expensive venture which means that the majority of programmes are imported.
- Not all programmes on television have been classified according to the appropriate age group etc.

Recommendations:

- Although access to television is mostly in the home, schools can invest in making television available.
- Television is a passive medium with no interaction and should be used appropriately and selectively.
- Programmes can be valuable especially those aired specifically for learners. Recordings can be made of these and broadcast at school however; copyright rules should be adhered to.
- Programmes shown to learners should be properly classified by the Film and Publication Board.
- The school must comply with the Film and Publication Board classification as learners should not be exposed to inappropriate material.
- Schools must comply with the licence conditions of the SABC with the number of licences matching the number of television sets.
- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations and have steps in place to ensure compliance.

Digital imagery e.g. film, video/DVD and photographs

Description: The term "digital image" both moving and still, refers to an image created with digital technology such as digital camera, digital video camera, scanners or image editing software.

Uses: Every aspect of education can be enhanced through the use of digital images – either still images such as photographs or moving images such as video or animations.

Advantages:

- Images in education convey a powerful message especially and are especially useful for second language learners.
- Images are further enhanced when combined with sound and movement.
- Many cell-phones can be used to create digital still images and video, which makes it easy to create and share.

Considerations:

- Sharing images may be a cause for concern when these images are of a violent or personal nature or in any other way inappropriate.
- The taking and sharing of such images could be an invasion of privacy of an individual as well as potentially harmful to the viewer, especially if not used within the context of learning.
- Schools can hire/buy/record/copy videos/DVD's and inadvertently be in breach of copyright, especially if the group is large and the material used is only for purposes of entertainment.
- Images can be downloaded from the Internet and this could also breach copyright.
- Video streaming and downloading of large images can be a large drain on network resources.

Recommendations:

- Programmes shown to learners should be properly classified through the Film and Publication Board and these should be complied with.
- There are limitations on the size of the group of viewers, the purpose of the viewing and also whether learners can be charged. The school needs to be familiar with these rules.
- If photographs or video clips are uploaded to the Internet, learners and teachers need to be aware of the need to protect the identity of the people portrayed, as well as the identity of the authors of the material. If any of these are minors, it may be appropriate to take measures such as using only first names, or removing any information which could be used to track these individuals.
- Cognisance should be taken that some cultures do not permit images to be taken of people.
- Any image, whether still or video, may only be re-used with permission from the original copyright holder, or according to the terms of the Creative Commons licence if there is one.
- Teachers and learners should take cognisance of what images may be downloaded without breaching copyright.
- Credit should be given to the source of any digital material used for education purposes. Learners and teachers equally, should respect copyright.

- Schools should be aware that many brands are capitalising on the medium to promote their products and learners should be made aware of this.
- Permission from the parent/guardian can be included in the school's Acceptable Use Policy (AUP) if images of learners are to be used on the Internet.
- The school's Acceptable Use Policy (AUP) must specify where, when and what type of digital imagery can be used in a school.
- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations regarding group broadcasts (e.g. video hire) and have steps in place to ensure compliance.

Books, newspapers and magazines

Description: Print (paper-based) material can take a number of forms but the most commonly used in a school are books, newspapers and magazines.

Uses:

- Print materials should be made available in schools because the curriculum is resource-based. Access to print material is essential if we are to create a literate society.
- Information literate learners can only be developed if they have access to a range of resources, both digital and non-digital (paper based).
- One of the aims of education is to create discerning knowledge users who are ethical life-long users of information able to use a variety of resources.

Advantages:

- The advantage of print material is that it does not depend on electricity to be accessible nor expensive computer hardware which has to be maintained.
- Books go through an editorial and selection process so the information is, on the whole, trustworthy.
- Magazines can be used in a variety of teaching situations and the availability of paper-based material will encourage the reading habit as well as the fundamentals of information retrieval.
- Newspapers ensure currency of information and can also be used in a variety of ways for teaching e.g. debate topics.
- A range of resources encourages higher order thinking skills embedded in the research cycle e.g. comparison and evaluation.

Considerations:

- Print material needs to be managed, circulated and maintained.
- Theft, including vandalism is a key challenge to the provision of print material as well as the limitations of the size of the stock itself.
- If there is no budget or single person responsible for the collection, then this resource can be easily depleted or damaged.
- Books, newspapers and magazines date and thus require a budget to keep the collection current.

Recommendations:

- There should be a budget for paper-based material and the school should nominate an individual, in the absence of a school library/librarian to monitor and promote the use of the collection.
- Each school should ensure that key reference material that is current and relevant is available e.g. encyclopaedias, atlases and dictionaries.
- Credit should be given to the source of any information used for education purposes. Learners and teachers equally should respect copyright.
- Modifying work without permission can affect the reputation of the author. Permission should be sought.
- Photocopying of printed material should be limited to what is allowed in terms of the Copyright law.

- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations regarding copyright and have steps in place to ensure compliance.
- Photocopying of printed material should be limited to what is allowed, and copyright respected

Online Computers and Mobile devices

Description: An online computer in this context is a fixed machine that receives and outputs data in a meaningful way and is connected to the Internet. It can be a standalone device or linked to other computers through a server but is designed to stay in one place. Mobile devices include any type of technology that is designed to be taken and used on the move. The term 'mobile technologies' often refers to Tablets and cell-phones. It also applies to laptops and notebooks, media players and e-book readers.

The following is specific to mobile devices:

Uses:

Supporting learning in and outside the classroom through enhancing communications and access to information. There is an immediacy to the use of mobile devices i.e. 'anytime, anywhere learning' versus fixed technologies which are, at times, inaccessible.

Advantages:

- Parents/guardians can contact the learners during school hours and vice versa.
- The school can sms the parents/guardians school information e.g. change of sport practice.
- Sharing information with others, such as showing class projects to parents or sending missed assignments to classmates that are absent.
- Use of cell-phones can contribute to securing a learner's own safety.
- There are many ways mobile devices, such as cell-phones, can support learning across various aspects of the curriculum. For example: in Visual Arts, learners can compare the quality and

resolution of images taken on different devices in Life Orientation, learners can video and upload personal messages of support for safety campaigns, in Geography, they can investigate how topography affects mobile phone reception and plot data to GPS information systems.

- Giving learners flexible access to information, resources and tools; curriculum support e.g. social networking platforms, making learning a personal experience
- Recording and sharing experiences; and carrying out joint activities with learners from different schools or countries.
- Many cell-phones are equipped with calculators - plenty of new math curricula encourage the use of a calculator when problem-solving. A learner should become accustomed to having a calculator handy for both homework and real life maths applications.
- Many cell-phones are equipped with calendars – learners can be encouraged to load school events or project deadlines to their cell-phone calendars.
- Many cell-phones are equipped with a camera. These can be used for content creation, documentation and communication.
- If a learner is slow to copy notes from the board, pictures can be taken of the missed notes and accessed later. This also applies to sending notes to absent classmates.
- Sound recordings can be made of educational material.
- Interviews can be recorded with sound or video inserted into presentations and movies.
- As learners are using social networking platforms, teachers should be encouraged to add the contact names of his/her class to communication with the class collectively or individually on school related issues.

Considerations:

- Mobile devices have to be managed in an educationally sound manner as, by the very nature of their mobility, they can be very intrusive.
- Learners who carry mobile devices can be a target for thieves. Safety of learners on their way to and from school is a major consideration.

- Mobile devices can be used to cheat in exams by sending test questions to friends.
- The ability of mobile devices to make recordings, whether sound, picture or video, can be abused. For example:
  - Recording individuals without their knowledge. Consent to being filmed or photographed should be specified in the school's Acceptable Use Policy (AUP).
  - Recording illegal or inappropriate behaviour such as the abuse of people or animals, bullying or taunting messages.
  - Recording and sharing sexual behaviour – a practice called "sexting".
- Learners should never use mobile devices for illegal offences such as committing a crime, arranging a drug deal etc. and the penalties for such should be clearly specified in the school's Acceptable Use Policy (AUP).
- Mobile devices can blur the distinction between what happens at school, and outside of school. This can result in misunderstandings and confusion. For example – if a learner uses mobile devices to commit a crime at school this is taken by the Safe School Committee and, if outside school, it is a matter for the parents/guardian and SAPS.

Recommendations:

- Outright banning of the use of mobile devices in a school can be self-defeating and educationally unsound. Furthermore the mobile device environment is becoming more and endemic and schools have a responsibility to manage it and educate around it.
- An Acceptable Use Policy (AUP) in a school should specify when and for what purpose the use of mobile devices is acceptable in a school and have steps in place to ensure compliance. This includes sending and receiving calls to/from parents/guardians.

The following is specific to computers and mobile devices:

e-Mail:

Description: e-Mail, or electronic mail, is a method of exchanging digital messages across the Internet or other computer networks. This can be on a one-to-one basis or within a group, either open or closed.

Uses: e-Mail provides a quick and effective means of communication locally and internationally. It also allows for the attachment of documents and images which otherwise would have to be posted (snail mail) or faxed.

Advantages:

- e-Mail provides for a quick and simple response.
- It provides a useful record of communications leaving a ‘mail trail’ of evidence especially if “sent” items are never deleted.
- e-Mail gives time for a studied response to a discussion as opposed to the immediacy of a telephonic conversation or online synchronistic (when things occur at the same time) communication e.g. chat room. Asynchronistic (when things occur at unrelated times) communications allows for a period of time between responses.
- Unless e-mail is web-based, one need not be online to communicate; messages can be answered offline and only sent when connected.
- e-Mail is a useful way of sending attachments of text, images, sound or video.
- e-Mail can be sent to individuals or many, alternatively group mailing lists of recipients.

Considerations:

- e-Mail is subject to interception (violation of confidentiality, blocked delivery or replay), unauthorised modification of content or denial of message received. In other words, e-mail is exposed while in transit on the Internet.
- e-Mail fatigue is when there is an information overload and a user ignores a large number of e-mail messages after falling behind and failing to answer them.

- Sorting, sifting, filing and replying to e-mail can be time consuming with little benefit, especially if a user belongs to a number of mailing lists.
- Spam (group advertisements), flaming (insults) ‘fun’ mails (not work related), bogus virus warnings and untrimmed e-mails can all create problems for bandwidth, work concentration and time on task.
- Phishing and spoofing are bogus e-mails and websites which encourage people to divulge sensitive information like PIN numbers. Victims can fall prey to this and be defrauded.
- Attachments can spread viruses and can also use up bandwidth unnecessarily.
- e-Mails can accidentally be sent to the wrong person or group or forwarded to a person who is not the intended recipient. They can also be copied either visibly or ‘blindly’ to an unintended recipient.
- To secure e-mail, one needs to ensure confidentiality of the message, message integrity (what the receiver sees is exactly what was sent), non-repudiation (the sender cannot deny that the message was sent) and authenticity of the sender (the sender is who the sender claims to be).

Recommendations:

- Users must be made aware that they will be held responsible for the content of any e-mail message they transmit.
- e-Mail should not contain messages using language or content that is inappropriate or unacceptable.
- Users should be made aware of basic rules of Netiquette e.g. the use of capitalised words is considered shouting.
- The immediacy of the medium must be managed; users should avoid a hasty reaction to an e-mail if emotionally charged.
- Users should be taught the importance of not divulging passwords and also logging off after use.
- Teachers and learners should understand what is spam including hoaxes, and not forward such messages, contributing to unnecessary use of bandwidth. Users should be educated on what type of e-mail to ignore or delete.

- e-Mail users should take note of the size of attachments and reduce the file size where possible e.g. converting images to .jpg format or zipping files.
- All e-mail should have relevant subject lines and follow a thread of discussion.
- To mitigate the risks associated with the use of e-mail, users should be educated about security and personal risks associated with the use thereof.
- An Acceptable Use Policy (AUP) in a school should specify when and what purpose the use of e-mail is acceptable and have steps in place to ensure compliance.

Internet sites (World Wide Web)

Description: The Internet, in particular the World Wide Web, is a global set of interconnected computer networks using a protocol which allows them to connect to each other. It provides a platform for a massive library of current, relevant and pertinent information in a variety of formats e.g. video clips, images, presentations, text, spreadsheets also communication tools such as e-Mail, chat rooms, forums, blogs etc.

Uses: The main goal of Internet access in education is to enrich and extend learning through access to information, also enhance communications and sharing. Collaboration in the online environment allows both teachers and learners to be global citizens through being able to quickly and easily communicate across the world as well as developing their skills for the 21st century.

Advantages:

- Access to a range of resources in the education environment as well as generally.
- Access to current information and the ability to keep track of rapidly changing situations – an advantage over print material which can be slow and expensive to update (excluding newspapers).
- The ability to communicate with others in online forums and other social networks. Such communication is not limited to the purely

social, but can be used to support professional development as well as lifelong learning.

- The opportunity to broadcast opinions and information in the form of articles published on blogs and other websites.
- Sharing of teacher developed resources that have been peer reviewed, or with websites that have been evaluated by the education community,
- The opportunity to build lifelong research skills.
- The ability to interact with people from all over the world and be exposed to new points of view, alternative perspectives and other cultures (Communities of Practice – COP's).

Considerations:

- Anybody can create a website and upload information either true or not, unlike a traditional library whereby books go through an editorial and selection process thus ensuring a measure of quality control.
- Inappropriate material can be accessed online very easily, both deliberately as well as inadvertently. Users need to be aware that their use can be monitored and they can be identified for inappropriate use. Users of the Internet create a digital trail which cannot be erased.
- Creating White lists, or pre-screened lists of Internet sites, is appropriate in some instances but it must be remembered that learners must be educated to manage the Internet even when away from the protected environment of a school.
- Digital literacy, i.e. the ability to find, discern, select and use online information appropriately is a skill that needs to be taught. If learners do not understand that much of the information on the Internet is opinion not fact they will be the victims of misinformation.
- Modifying work without permission can affect the reputation of the author. Permission should be sought.
- The erroneous assumption that digital resources carry more credibility.
- Misuse of access to the Internet can cost the school both bandwidth as well as working time on the part of both learners and teachers.

Recommendations:

- All schools should have an information literacy plan in place whereby learners and teachers are taught how to find, evaluate and use the range of information resources available.
- All methods which limit access – whether lists of suitable sites, lists of blocked sites, or lists of unsuitable words, should be developed with the input of teachers who will be affected.
- Careful thought should be given to the process whereby these lists and limitations are managed and adjusted so that they do not adversely affect the ability of teachers to teach.
- The content of web pages or web searches can be filtered for unsuitable words using forensic software or firewalls, but care should be taken these do not impact on legitimate use. For example, blocking the word "breast" would make it impossible for anyone to find information on "breast cancer".
- White lists or pre-screened internet sites can be uploaded onto a school server.
- Shortcuts to useful, interesting and popular sites that are appropriate to the learner's age can be placed on the desktop of each computer.
- Browsers come with built-in safety parental control features; parents/guardians can protect the computers in the home through using these.
- Having computer screens in public place minimises the temptation to misuse access.
- Software can be installed so that all computers are "set to default" each morning. This will delete unauthorised material from the computers.
- Applying rating settings on browsers, checking the cache (visited sites) in the browser and password protecting computers are all measures which can be taken.
- Checking the history of sites visited can be a useful tool in managing user access and misuse.
- Making sure that learners know that their use is monitored and that they have to take responsibility for how they use the Internet.
- Phishing and spoof sites. To avoid these dangers, users are advised to:

- Log off after using a site especially on a public computer as found in an Internet Café or school computer room,
    - Avoid clicking a URL link in an email
    - Check for a padlock in the address bar of the browser if it is a financial site,
    - Look for the https in the site address, this versus http which is insecure
    - Change passwords and PIN numbers regularly.
- An Acceptable Use Policy (AUP) needs to be in place and have steps in place to ensure compliance in order that users accept their responsibility for their use of the Internet

Social Media and Social Networking

Description: Social Media: refers to the platforms that make it possible for users to actively participate online by creating their own online presence, and communicating with others. User-created communication and content that may take the form of video, audio, text or multimedia that is published and shared in a social environment, such as a blog, wiki, forum, podcast, social bookmarking or video hosting site. Access can be either on using an online computer or using mobile devices such as cell-phones.

Social Networking: online platforms that provide means of personal communications between participants such as FaceBook, LinkedIn, Twitter, Whatsup, Buzz and many others

Uses:

- Participating in online communities that share an interest – to gain or share knowledge.
- When used positively the social media platforms allow people to share music, art, video, opinion, collaborate on work or have discussions and learn from one another.
- Socialising: keeping in touch with existing friends and finding new friends. A channel for the promotion of a cause or product.
- Social media platforms allow users to link up with each other quickly and effectively. This can be particularly effective in the professional environment.

- Individuals can use social media to further their personal or professional goals e.g.
    - Creating and managing their online presence to form an impressive online CV
    - Communicating their opinions, values, and experiences
- Sharing information, pictures, activities, resources and websites can assist lifelong learning and create Communities of Practice (CoP's).
-

Advantages:

- There can be opportunity for substantial professional growth as members of the group are kept abreast of the latest developments and the views of thought leaders.
- Users can create an impressive online presence to further their professional goals – for example, writing a blog in the area you specialise in to prove your expertise.
- A way of connecting and reconnecting with people.
- Users of these social media platforms have the ability to create their own material and post whatever they like in the platform of their choice e.g. films, magazines or text.
- When used positively the social media platforms allow people to share music, art, video, opinion, collaborate on work or have discussions and learn from one another.

Considerations:

- As with all online communication tools the social media environment has to be managed so that it does not become all consuming.
- Cognisance must be given to Copyright law when sharing these media.
- Modifying work without permission can affect the reputation of the author. Permission should be sought
- Like e-mail etc, issues of privacy and circumspection apply as any communication can be forwarded and very often credit is not given to the source.
- Social media networks are often visible to people from the user's professional as well as personal life. This blurring of social and professional lines can result in embarrassing or otherwise

inappropriate revelations. For example – if a teacher "friends" learners on Facebook, they should be aware of what aspects of their profile are visible to the learners.

- Online stalking, harassment and bullying can occur, with resulting emotional stress.
- Naive users may fall prey to hackers, phishers and other online scams.
- Users should take care to familiarise themselves with the privacy settings, and avoid sharing any information that they don't wish to be publically available.
- Users should take care not to share compromising images or inappropriate messages that may damage their reputations later in life (creating a digital footprint).
- Users should be aware that behaviour on sites may or may not be moderated, and content is usually uncensored.
- Social networking platforms can be bandwidth intensive.

Recommendations:

- Activity is advised for professional purposes in the education environment.
- Learners should be taught critical thinking skills and digital literacy to enable them to navigate safely through this online world.
- It offers a variety of privacy settings and again, circumspect use of the site is advised.
- Learners should be sensitised to the appropriate etiquette for each online environment, and be made aware of the consequences of misbehaviour.
- Learners should be made aware of the consequences of their use of social media, and encouraged to act responsibly.
- An Acceptable Use Policy (AUP) in a school should specify when and for what purposes the use of social media platforms are acceptable in a school.

Online gaming

Description:

An online game is a game played over some form of computer network. Online games can range from simple text based games to games incorporating complex graphics and virtual worlds populated by many players simultaneously. Many online games have associated online communities, making online games a form of social activity beyond single player games.

Uses: These can be educational e.g. Teen Second Life ages 13 -17 whereby learners create avatars, or online personas which can explore, meet other residents, socialise, participate in individual and group activities, and create and trade virtual property and services with one another, or travel throughout the world (which residents refer to as "the grid"). Epistemic games offer an opportunity to build bridges between theory and practice. These games could also afford learners the opportunity to see what it is like being a scientist or doctor, etc.

Advantages:

- Developing computer skills and interacting online.
- Learning in a fun and interactive way.
- Developing social and problem skills in a more contextualised environment.
- Learning 21st century skills:

Disadvantages:

- Can form addictive behaviour and also impact on social behaviour especially if content is particularly violent/sexual in nature.
- Games, particularly games that aim to teach and not simply entertain are difficult to design and develop.
- Developing games are expensive and time consuming.
- Online gaming can also be a drain on networking resources.

Recommendations:

- Games should have clear educational goals.
- Games need to be developed that provide learners with a safe environment in which to learn and explore.

- We need to not only educate our learners in using technology but also how to use it ethically and responsibility.
- Develop epistemic games to embody professional occupations and help learners learn these cultures that define their community of practice (CoP’s).
- Games can help prepare learners for a global world, of dynamic change and possibility. An Acceptable Use Policy (AUP) in a school should specify when and what purposes the participation in online gaming is acceptable in a school.

What is Copyright?

The South African Copyright Law No. 98 of 1978 (as amended) gives authors and creators a “bundle” of special or exclusive rights over their original works which they create.

What works are protected under copyright?
Literary, musical and artistic works; cinematograph films, sound recordings, broadcasts, programme-carrying signals, computer programs and published editions.

What are the rights of authors and creators?
They have the sole or exclusive right to authorise that their works be –

- Reproduced in any manner or form;
- Published;
- Performed in public;
- Broadcast;
- Transmitted in a diffusion service
- Adapted/Translated

Copyright provides authors and creators with an incentive to create new works and to benefit financially from them.

How long are works protected by copyright?
Subject to exceptions depending on the category of work, the term of copyright protection is the lifetime of the author/creator plus 50 years from

the end of the year in which the author dies. The publisher also has copyright in the published version for 50 years from the end of the year in which the edition is first published. When this period has expired, the work goes into the public domain, which means that it can be used and reproduced freely.

May users of information use and reproduce copyrighted works?

Yes, the Copyright law has some “limitations and exceptions” to the exclusive rights of the author.

Section 12(1) of the Copyright Act allows “Fair Dealing”. Fair Dealing is not defined in the act, so one has to use one’s discretion when using other people’s intellectual property. Anyone may make a reasonable portion of a work (with proper acknowledgement), for the following purposes, without having to apply for copyright permission:

- for research or private study,
- for personal or private use,
- for criticism or review
- for reporting current events (such as in a newspaper or broadcast),

Section 12 (2-4) allows copying, without permission –

- for using the work for judicial proceedings, or for a report of such proceedings,
- for quotation,
- “by way of illustration” for teaching purposes (such as placing an extract of a work on an overhead projector or in a PowerPoint presentation, to highlight aspects of a lecture or training session).

Section 12 (5-11) have other exceptions.

Can educators/learners copy for teaching/educational purposes?
Yes, in terms of Section 13 (Copyright Regulations), a teacher may give a limited number of separate/single handouts to learners in a classroom situation without having to get permission. The copies, however, may not be included in compilations (e.g. study-packs/course-packs) or handed out with other copyrighted material.

There are a lot of publications and digital works that allow reproduction for non-commercial or educational purposes, without having to get permission. You would need to check the copyright notices inside the printed publications or read the copyright notices on websites. There is also a great deal of free material on the Web. However, remember not all material on the Web is free. Many websites and electronic databases have strict copyright conditions and you may only use or copy their material in terms of their licence agreements. Proper acknowledgement must always be given, even if the material is free.

Without first obtaining copyright permission, you would be infringing the Copyright law if you were to -

- copy a whole book or journal, or major portion of a book or journal (including an out-of-print book), except in very special circumstances,
- copy sheet music, commercial audiotapes, videos, CDs, DVDs, films or other original works,
- translate, adapt, modify or convert material into alternative formats (even for persons with sensory disabilities),
- make copies, beyond the amounts permitted in under Fair Dealing (Section 12) and the Copyright Regulations (Section 13),
- scan, digitise or place material on the Web, where permission is specifically required,
- download multiple copies of material from electronic databases or the Internet, where permission is specifically required,
- play copyrighted music or perform a copyrighted musical for a public audience,
- perform a copyrighted play or drama,
- show a video, film or DVD to a public audience, if not specifically allowed for educational purposes,

- create, replace or substitute anthologies, compilations or collective works,
- make copies of, or from, works intended to be ephemeral, including workbooks, exercises, standardized tests, test booklets and answer sheets, or similar ephemeral material,
- make copies to substitute for the purchase of books, publishers' reprints or periodicals,
- leave copies of copyrighted works for users/learners to copy from,
- make a backup copy of a computer program or an authorized copy, other than for personal or private purposes.

May a librarian make copies for teachers or library users?
Yes, a librarian may make a single copy of a reasonable portion of a work for a teacher or other library user, as long as it is for research or private use. A librarian may also obtain a single copy for a teacher or library user via interlibrary loans. However, a librarian may not make multiple copies for a teacher or other library users.

May librarians make copies for preservation and interlibrary loans purposes?
Yes, the following sub-clauses provide for some exceptions -

- Sub-clause 3(d), (e) and (h) applies to preservation and/or replacement of works, with conditions
- Sub-clause 3(f) applies to Interlibrary Loans

A librarian may make a copy or obtain an ILL copy for a user, but may not make multiple copies for a user, without permission.

Do libraries need to place copyright warnings near copying equipment?
Section 13(6) of the Act requires libraries and archives to place a copyright warning at the place where orders for copies are accepted by libraries and archives. This warning must be incorporated in all forms supplied by libraries and archives and used by their users or the general public for ordering copies. The copyright warning must also be placed where unsupervised copying equipment is located.

N.B. Article 6 (1) of Section 13 of the Copyright Act requires that the following Copyright Warning Notice should be displayed at the place where orders for copies are accepted by libraries or archive depots. It should also be incorporated in all forms supplied by libraries or archive depots and used by users for ordering copies.

The Notice should be printed on heavy paper or other durable material in type at least 18 points in size, and should be displayed prominently, in such manner and position as to be clearly visible, legible and comprehensible to a casual observer in the immediate vicinity of the place where orders are accepted or where unsupervised equipment is located.

COPYRIGHT WARNING

The Copyright Act, 1978 governs the making of photocopies of other reproductions of copyrighted material. Under the provisions of the Act, libraries and archive depots are authorized to supply photocopies or other reproductions. One of the provisions is that the photocopy or reproduction is not to be used for any purposes other than private study or personal or private use.

If a user makes a request for, or later uses, a photocopy or reproduction for purposes not permitted by the Act, that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its opinion, fulfilment of the order might involve violation of the Act.

How does infringement affect the author or creator?

If their works are copied illegally, their works are not purchased, so they lose out on sales. This has a direct impact on their income. Prices of publications and other works increase as a result. It also discourages authors from creating new works, which could result in a shortage of publications.

How does one apply for permission?

One would need to apply for permission directly to the publisher, Webmaster, newspaper editor, database supplier, film director, artist, broadcaster, computer director/programmer, e-database provider, or other copyright owners, as the case may be. For permission specifically to make photocopies, one can apply to DALRO, the Dramatic, Artistic and Literary Rights Organization, in Johannesburg. To copy music, one can apply to

SAMRO, the South African Music Rights Organization, in Johannesburg. The telephone number for DALRO and SAMRO is 011-712-8000.

Compiled by Denise Rosemary Nicholson, Copyright Services Librarian, University of the Witwatersrand, Johannesburg –
Tel. 011-717-1929 or email: Denise.Nicholson@wits.aca.za – Websites:
http://web.wits.ac.za/Library/Services/COPYRIGHT.htm;
http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Copyright+and+Related+Issues.htm and
http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Plagiarism+Portal.htm

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

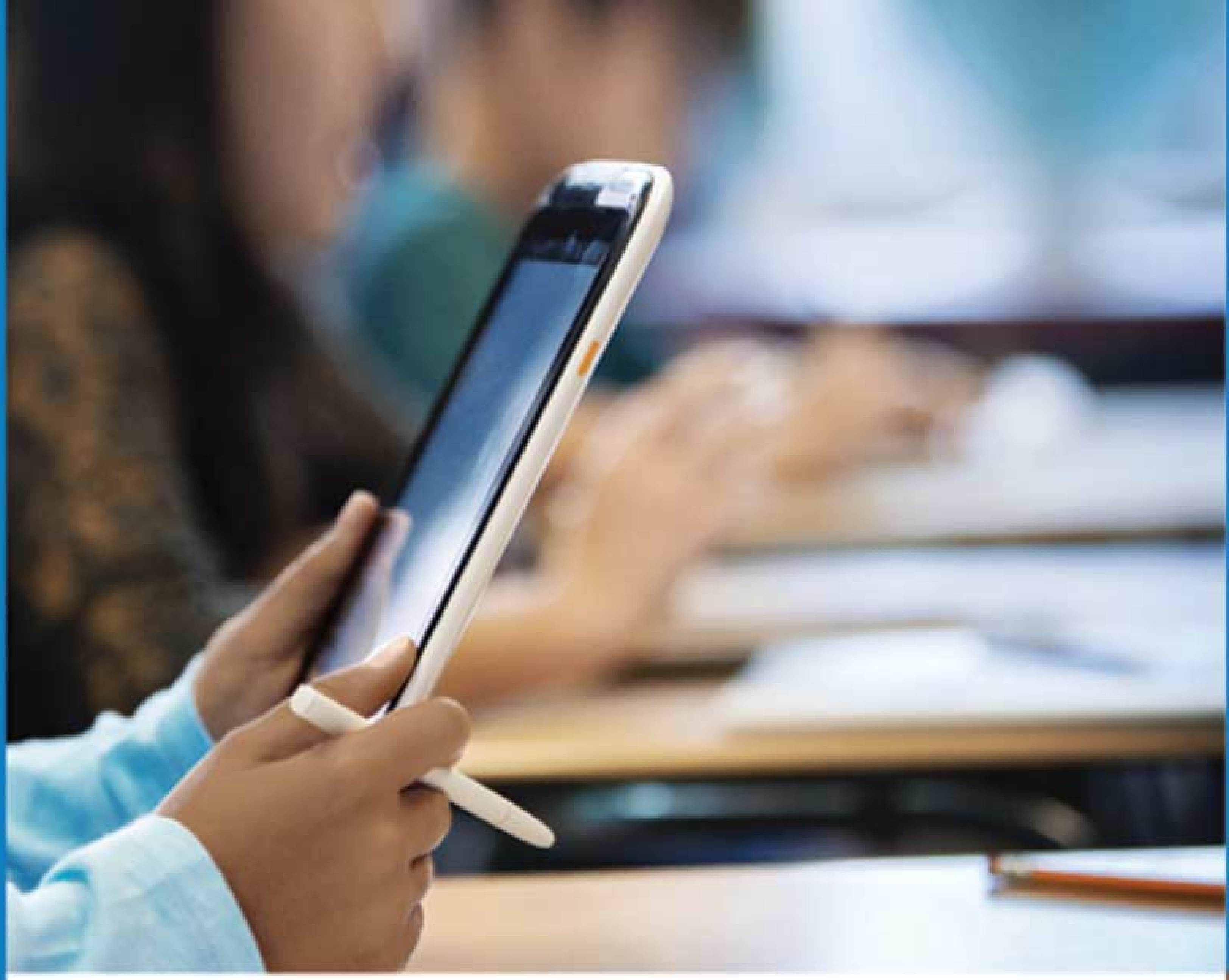
Nieuwenhuize. J. (2008). Values and Human Right in Education. Pretoria. Van Schaik Publishers.

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 261650

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

IFAP
Information for All
Programme
National IFAP Committee
for South Africa

telecommunications
& postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

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