A Proposed Cyber Threat Incident Handling Framework for Schools in South Africa

Mrs. N Sonhera
UNISA student
VUT, 24 Plane rd,
Isando, Kempton Park
+27 11 292 7427
nqume@vut.ac.za

Prof E. Kritzinger
UNISA, School of Computing
College of Science, Engineering & Technology University of South Africa
+27 12 429 8547
kritze@unisa.ac.za

Mrs. M. Loock
UNISA, School of Computing
College of Science, Engineering & Technology University of South Africa
+27 12 429 6381
loockm@unisa.ac.za

ABSTRACT
In South Africa, there is a lack of structure or guidance for schools on how to deal with cyber threats. There are no clear procedures that are consistently followed by schools, governing boards and educators, and the cyber threat process is not widely known and understood by educators, learners and their parents/guardians. As a result, many learners remain vulnerable to the negative effects of cyber threats. An example is a Krugersdorp High School girl who was attacked after a cyber-threat ordeal, (*The Star* 9 February 2012:1). In this paper a framework is therefore proposed that schools can implement to assist learners with cyber threat incidents.

The methodology that will be followed in this article is, firstly, to determine from the literature how a victim of cyber threat can be helped, secondly, to develop an incident handling structure that will assist learners in reporting cyber threats, and thirdly, to develop a framework which will address the lack of structure, guidance or procedures when dealing with cyber threats in schools.

The gap which exists now deters learners from reporting cyber threat incidents. To fill this gap, the authors propose an incident handling structure which will assist learners to report and receive protection against online threats. It is hoped that, in the end, learners will know what to do when they are threatened online. In addition, cyber threat policies and procedures are proposed to protect and inform learners and their parents about cyber threats. These procedures collate, outline legislation and the policies of the Department of Basic Education. The aim is to give schools rights and responsibilities in addressing cyber threat incidents.

Practical considerations such as time and costs limit the study to a sample of schools in South Africa. The framework for intervention in cyber threat incidents as part of school policies in South Africa is merely a proposal to the rightful stake holders, since policies for schools are determined by the Department of Basic Education which the authors are not members of.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues - *Abuse and crime involving computers, Ethics, Human safety, Privacy, Regulation, Use/abuse of power*

SAICSIT '12, October 01 - 03 2012, Pretoria, South Africa

General Terms
Management, Security, Human Factors, Legal

Keywords
Learner, Facebook, cyber threats, cyber security, blogs, e-mail, e-crime, chat rooms, cyber stalking, cyber bullying, sexting, social networking, framework, cyber safety

1. INTRODUCTION
Schools are encouraging learners to be computer literate and use the internet to enhance their education and prepare them for future careers (The Teacher Laptop Initiative 2010).The Teacher Laptop Initiative (TLI), which is managed by the Education Labour Relations Council (ELRC), addresses South Africa's need for a quality education system. The TLI forms part of the cohesive plan of the Department of Basic Education (DBE) and other stakeholders in education, to improve the overall quality of education. According to the Government Gazette (RSA 2009), this initiative makes computer networks, broadband connections to the internet and virtual communities available to learners and educators in the public education sector. The ELRC has highlighted that information and communication technology (ICT) integration in the classroom is an extremely positive addition to the learning environment, since it brings rich and diverse resources into the classroom. The Gauteng Online Schools Project is aimed at fully equipping 2 500 public schools in Gauteng with ICT centres. According to the 2009 Finance MEC, Nkomfe, the project demonstrates the Gauteng provincial government's vision of ensuring that all learners in public schools in the province have access to computers, the internet and email, (RSA 2009). Learners naturally take advantage of these developments in technology to personalise and expand their learning opportunities. While educators provide rich learning environments for learners as they engage with people and online resources, locally or globally (Robinson 2009). According to Robinson (2009), the DBE and schools invest in computers and network systems to manage and protect the welfare of learners. However with the introduction of wireless and mobile devices, learners can now bypass conventional network systems and this has the potential of exposing them to cyber threats. These new technologies are challenging current practices and therefore there is a need to instil confidence in the learners to inform the adults around them if or when they feel uncomfortable or threatened online, at school or outside the school premises. The chairperson of the Wireless Application Service Providers' Association in South Africa has urged parents to educate their children to prevent cyber threats or chances of meeting strangers in chat rooms or on social networks in general. He issued the warning after a pornographic video of two learners, in their school uniform, was recorded on a cell phone and circulated on Facebook (*The SOWETAN* 7 November 2011:10).

With all these challenges, this article is aimed at proposing ways that can help learners to feel confident about alerting adults when they feel unsafe online. At present, principals, educators, other staff members at schools and parents are not sure how to deal with learners who are being threatened online.

2. BACKGROUND OF THE STUDY

Learners use social networking sites (e.g. MySpace, Twitter, Facebook and YouTube), e-mail messages, instant messages, cell phones, chat rooms and blogs as environments and tools for socialising (Willard 2005). While awareness of the use of internet is growing, there is no accompanying increase in awareness of safe practices in the use of technology (APHA Annual Meeting & Exposition 2007). Learners receive mixed messages about online behaviour as they strive to use technology, sometimes without appropriate support. Some learners share derogatory messages on their cell phones with other learners before sending the messages to their victims (Campbell 2007). Campbell says that learners are ganged up on, and bombarded with "flame" e-mails, (emails that are designed to inflame or enrage). Internet and telecommunications components/devices have become the new weapons for cyber threats incidents.

The feeling of anonymity on the web makes it a perfect playground for learners to engage in cyber threats (Time Warner Cable and Cyber Angels 2007). These threats can follow learners from their schools to the privacy of their homes. Many victims are caught up in these threats from the moment they wake up and check their cell phones or e-mails, to the time they go to bed and shut off their computers or cell phones (Aune 2009). In this way learners can be the targets of cyber threats all the time. In "*The Star", (The Star* 14 February 2012:12), Burton stated that online engagement is an important part of the development of young people, but it needs to be supervised.

2.1 Pilot study survey

Literature on the incidences of cyber threats shows that cyber-related threats have become an increasingly common occurrence in schools. With all this evidence, the author of this article decided to conduct a pilot study survey to find out if cyber threats also affect learners in South African schools. No data analysis was done since the survey was intended to find out the viability of the topic.

The survey was conducted in 2011in (15) rural and (20) town schools in South Africa. These schools fell under the (DBE). The aim of the DBE is to develop, maintain and support a South African school education system for the 21st century (Department of Basic Education 2009).

The results of the pilot study survey showed that the majority of the learners were aware of the existence of cyber threats and that it could affect them mentally or psychologically. However because there were no procedures on how to deal with these threats, the learners did not tell the school authorities, their parents or other adults about these threats. In the 2008 National Cyberethics, Cybersafety and Cybersecurity Baseline Study, Pruitt-Mentle (2000) states that "educators sometimes feel unsupported and let ethical violations go rather than follow ill-defined and unenforced policies". At home many parents do not have time or do not know how to check on their children. Aune (2009), in her research paper for a Master of Science degree, states that students may even be reluctant to tell their parents or guardians of what is happening online or on their phones because they think that it is their fault, or are afraid that their online activities or cell phone use will be banned. They may also fear retaliation from the cyber threat aggressors (CSRIU 2006; Willard 2005). Finding a possible solution to deal with cyber threats will enable victims to feel safer, not only in their homes, but also at school.

Specific details of the pilot study will be presented as a separate paper in further research. The needs assessment survey, as well as other assessment instruments, will help to assess the existence of the cyber threats in schools. Evaluation and assessment will be used to modify and improve implementation efforts.

2.2 Addressing cyber threats in schools

Schools have a duty to implement policies that protect learners from cyber threats. An educational setting should offer an environment with both tools and information which can help to combat cyber threats. According to the Internet Watch Foundation's (IWF) 2011, criminals are determined to distribute images of learners who are being sexually abused, and are using new ways of exploiting legitimate online technology. They disguise websites to appear as if they host legal content, (Internet Watch Foundation 2012).

Personal and public concern about learners' online safety is the main focus of this article and study which is aimed at determining ways of dealing with cyber threats. Outlined below are some of the concerns.

2.2.1. No comfort zone for learners because of cyber threats

Aune (2009) states that threatening emails, text messages or comments can follow the victims home and can be present on their cell phones all hours of the day. The pilot study survey showed that most of the learners used their cell phones to log on to social network sites and usually this has an impact at school, because the learners are physically together at school.

2.2.2. School personnel are not sure how to handle cyber threat incidents

School personnel are not sure how to deal with learners who are cyber threatened because of a policy vacuum on how to deal with cyber threats. Shariff (2005) says that this lack of clear direction may account for inaction on the part of adults in schools, and as a result, unwillingness on the part of learners to seek help from them. In The National Cyber Security Policy Framework for South Africa it is stated that the policy framework is a starting point to put measures in place to address the cyber threat concerns, (*The Right Times* 2012)

2.2.3. Learners do not report cyber threats to adults

Learners are more likely to report instances of cyber threats to their friends than to discuss it with the adults in their lives. According to Petersen and Rigby (1999), learners do not believe that adults can solve their online problems and fear that they might make it worse. Campbell (2005) states that learners believe adults do not understand that they have an online life which adults do not have. Despite their beliefs, protecting young people from forms of relational aggression and/or verbal, social, and emotional threats via cyberspace is becoming an essential responsibility and a need for guidance, (*The Right Times* 2012)

2.2.4. It is the mandate of schools to protect learners online

Schools have a mandate to ensure that they are providing their learners with a quality educational environment. Ignoring

complaints about cyber threats because it did not happen on school grounds is not justifiable because the effects of cyber threats are experienced in schools. An example of the dire consequences of cyber threat is that of Megan Meier, a 13 year old girl in Missouri who hung herself in her closet in October 2006 (Pokin 2007). She was threatened by a 16-year-old boy named Josh on MySpace. Incidents like these can significantly impact on learners' learning which may be reflected in low school commitment, problematic behaviour, and substance abuse (Li 2008).

3. RESEARCH HIERARCHY

Two approaches which will be followed in this study, namely; literature review and the development of an incident handling structure and framework.

i. Literature review

The literature review will focus on what has been documented by other researchers in terms of defining cyber threat, and the prevalence and effects of these threats in schools. The South African reports on cyber threats will provide evidence of the existence or nonexistence of these threats. There is also a need to find out any group, organisation, etc. has advocated cyber threats as "good/bad"? If it is bad, what has been done in terms of policy, procedures or frameworks to deal with it globally, in South Africa or in other countries? Finally, it is hoped that the literature review will highlight processes and strategies that can be used in policy development and implementation at school level and government level (the DBE).

ii. The development of an incident handling structure and a framework.

The primary objective of the study is to explore ways to prevent cyber threats in schools before they happen and to intervene in cases where they have occurred. The authors will develop an incident handling structure and a framework for intervention in cyber threat incidents that will assist learners in reporting incidents of cyber threats and will combat cyber threats, in and outside schools. The aim is to fill the gap in the existing school policies, which is a lack of structure, guidance or procedures.

3.1 Literature review

3.1.1. Cyber threats

Cyber threats are direct online threats or "distressing material" – general statements that make it sound like the writer is emotionally upset and may be considering harming someone else, harming himself or herself, or committing suicide (Willard 2005). Cyber threats in schools can be a result of online abuse of learners, for example cyber bullying, cyber stalking, Identity theft, cyber harassment and sexual grooming. The DBE, in their Draft Guidelines on e-Safety in Schools, defines cyber threats as online material that raises concern about violence against others or the self. This may be direct threats or may allude to a threat of harm to one's self or to others (Department of Basic Education 2010).

Bhat (2008) states that cyber bullying involves the use of ICT to intimidate, harass, victimise, or bully an individual or a group of individuals. Cyber bullying has also been defined as 'the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others", (Belsey 2006). It involves sending or posting harmful material or using digital technology to inflict social cruelty on a victim (Willard 2006). The intent behind cyber bullying actions is to threaten, harm, humiliate, and engender fear and helplessness in the victim (Stron & Stroom 2005).

Girl attacked after cyber threat ordeal; teen, 15, taunted on Facebook and BBM. This incident happened at Krugersdorp High School, in Johannesburg, South Africa and was reported by C Bailey in The Star on Thursday, 9 February 2012. The aggressors first called the victim fat and threw diet pills at her. Then they took to Facebook and Black Berry's BBM chat service with a series of threats, name-calling and nasty comments. The four Krugersdorp High Schoolgirls then marched up to the 15-year-old learner and hit her over the head with a glass juice bottle. The attack was filmed and recorded (70-second video) by another learner who had allegedly been asked by the attackers to do so and who was once also threatened online. The victim's mother stated that the school did not handle the matter properly. The victim reported the cyber threats to the deputy principal and nothing was done before the physical attack. She then told her mother that she was no longer willing to go to school because it was uncomfortable for her.

Cyber threats cause psychological harm to victims. The harm includes low self-esteem, anger, school failure and avoidance, and, in some cases, school violence or suicide. A Research by Willard (2006) suggests that cyber threats may produce even more damage to youth, with consequences ranging from low self-esteem to youth suicide.

3.1.2. Efforts against cyber threats

A number of developed countries have already focused on Cyberethics, Cybersafety and Cybersecurity in education (Pruitt-Mentle 2000). In South African the Electronic Communication and Transactions Act 25 of 2002 promotes universal access to electronic communication and transactions and offers guidance on how to prevent abuse of information systems. South Africa has enacted the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 in 2002 (hereafter referred to as the Communications Act) to provide for the interception of direct communication as well as indirect communication such as data, text or visual images (last reviewed on 9 January 2009). According to, by then Minister Radebe, in his parliamentary briefing, stated that there is a need for all phone SIM cards to be registered in compliance with Regulation of Interception of Communication Act (RICA) in order to reduce threats through cyber technology, (Parliamentary Monitoring Group 2012). RICA increases the chances of detection of threats and the quality of evidence which can be presented before courts during trial.

The South African Police Service's (SAPS) annual report (2009/10) and the Communications Act confirm that the government is aware of the need for cyber security in the country. The South African government published a draft cyber security policy on 19 February 2010 which is aimed at creating institutional capacity to respond to cyber threats, (RSA 2010). It is envisaged that this policy will promote the development of measures to anticipate and confront emerging cyber threats, coordinate South Africa's responses to such threats, build partnerships amongst stakeholders both locally and internationally, monitor cyber incidents, and develop a culture of awareness and requisite skills as well as research and capacity development.

Although South Africa has promulgated a number of Acts on this issue, the lack of coordination in various government departments to administer various Acts that can be used to

combat cyber threat remains a challenge. There is therefore a need for coordination and harmonisation of legislation. P. Burton, (executive director of the Centre for Justice and Crime Prevention) commented in "*The Star*" (*The Star* 14 February 2012:12) that little research on cyber threat has been undertaken in South Africa, and only over the past five years has it been more fully explored internationally. It was only on 12 March 2012 that the Cabinet approved a National Cyber Security Policy Framework for South Africa (initially proposed in February 2010), with some challenges in trying to bridge the gap between law and technology, (Ministry of State Security 2012). In this National Cyber Security Policy Framework it is stated that The National Cyber Security Alliance (NCSA), an American organization, advocates a lot for cyber education programs as a way of empowering people to use the internet safely and securely at home, work and school, (*The Right Times* 2012)

One of the South African newspaper (*The Benoni City Times* 10 February 2012:2), contained an article "Safety on Facebook". This kind of educational endeavour will promote awareness and understanding of cyber threat, including equipping learners with the understanding to respond effectively to incidents of cyber threats, and recognising positive and safe uses of technology.

The Department of Education and Children's Services of the government of South Australia (Government of South Australia 2009) has produced guidelines for schools and preschools to handle cyber threat incidents. Likewise, Willard (2005) has produced an Educator's Guide to Cyber Bullying and Cyber Threat which provides educators with insight into the concerns about cyber threats, and guidelines to prevent and respond to these threats. Campbell (2007) offers some recommendations for the victims of cyber threats in his paper, *Cyber bullying and young: Treatment principles not simplistic advice.* These guidelines, recommendations and ideas will be considered by the author for inclusion in the development and implementation of an intervention framework for South Africa.

4. PROPOSED ROLE PLAYERS FOR THE INCIDENT HANDLING STRUCTURE AND FRAMEWORK FOR INTERVENTION IN CYBER THREATS

In their Draft Guidelines on e-Safety in Schools, the DBE identifies different technologies used by school communities in particular, educators and learners, and recommend strategies for managing them for appropriate and optimum use in, and for, education (Department of Basic Education 2010). It is repeatedly stated that this can be done by identifying all the role players involved and their roles and responsibilities in cyber safety. According to this document, the DBE seeks to equip all role players (educators, learners and parents / guardians) with guidelines and the ability to recognise potential dangers and be discerning enough to avoid them.

The diagram below that summarises how the role players fit

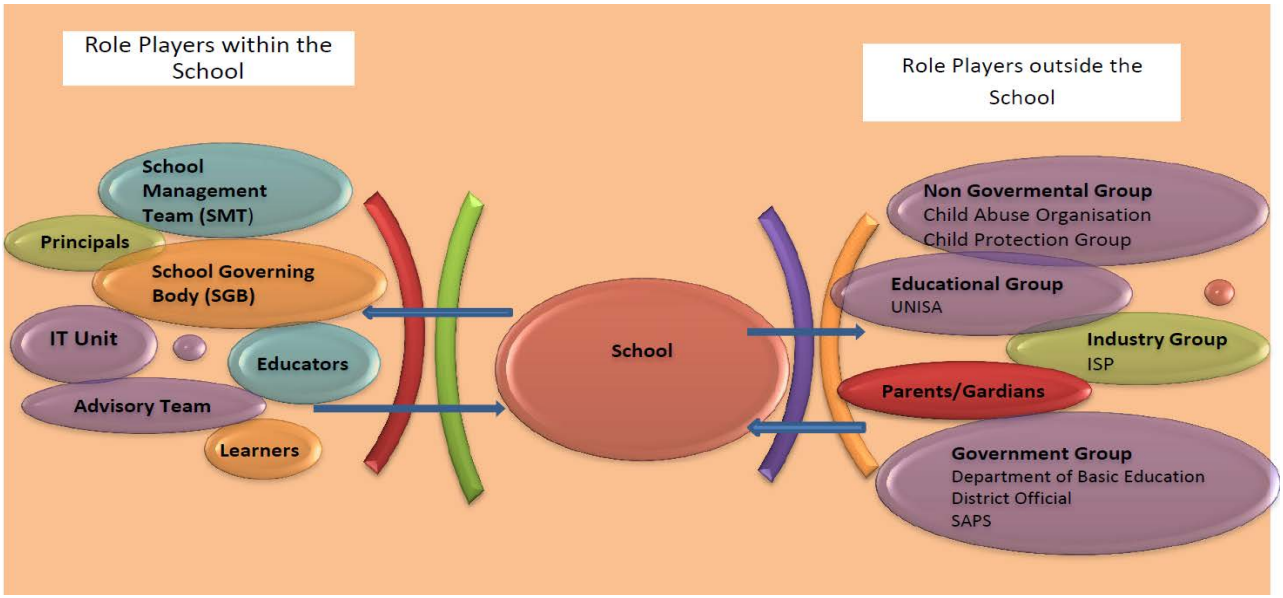

Figure 1: A summary of how the role players fit together

4.1 The responsibilities of the school

The responsibility of the school is not only to incorporate technology as a valuable learning tool, but also to equip the learners to be discerning, responsible and ethical participants in the information age. Schools should develop their own ICT policy, especially since it should be borne in mind that learners will bring a sophisticated range of handheld devices into school that will give them separate access to content.

In matters relating to cyber-threats, the schools should work with, and advised by the child protection groups, child abuse organisations and the SAPS to undertake investigations and to collect evidence after a principal has reported a suspected e-crime.

4.2 Role players within the school

4.2.1. Responsibilities of the principals

The principals should approve the posting of any information on school web sites, news groups, web-based forums etc, and should ensure that it conforms to minimum cyber safety standards. They should also ensure that the school's private information is not accessible to the public on the school's

websites. This includes that images should never include the names of the learners in the images. In addition to this, written permission from parents should be obtained before videos, photographs, comments or work samples of their children are published..

Principals should take action if the posted material might disrupt school safety. It is important that school administrators carefully assess the situation and provide evidence justifying any disciplinary action.

4.2.2. Responsibilities of the School Management Team (SMT) and the School Governing Board (SGB)

The principal, SMT and SGB should contribute to developing an ICT policy and should meet and consider what additional rules/guidelines staff and learners may need that are specific to their own school situation. These teams should develop a mandatory acceptable use agreement for all staff and learners and should put in place management protocols so that any cyber threat incidents are responded to, in an appropriate and consistent manner.

It is the task of these teams to explain the use agreements to learners and their families, and also assist educators to integrate aspects of cyber safety into the curriculum. The SMT together with SGB should convene regular meetings to maintain the school's cyber threat programme.

The teams should be responsible for behaviour management. An act of threatening through text massaging or image exchange can be dealt with by means of the school's code of behaviour and should have appropriate consequences; even if the incident occurred away from the school and or out of school hours. For example, suspected pornography or a threat to safety may constitute an e-crime that requires police notification. The school may suspend the learner involved in the incident or suspend him or her pending exclusion.

4.2.3. Responsibilities of the educators

Learners are increasingly using their cell phones to communicate, and to share and find information and educators should be able 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 (Department of Basic Education 2010). The Partnership for 21st Century Skills (2011), refers to information literacy as well as ICT literacy.

During the teaching of cyber threat awareness, educators should keep up to date with the relative risk and educational benefits of online activities in learning programmes. They should be aware of the steps to take and advice to give if learners notify them of inappropriate or unwelcome online activities by other learners or members of the public, (Government of South Australia 2009)

Staff members must be supported in making a mandatory notification if they suspect child abuse and/or neglect. As stated previously, an act of cyber-threat through text messaging or image exchange should be treated as a behaviour management issue and should be dealt with by means of the school's code of behaviour, with appropriate consequences, even if the incident occurred off the school premises and/or out of school hours.

4.2.4. Responsibilities of information technology Unit

It is very important that the school should set up a team to manage their ICT policy. The team should consist of at least; the ICT Manager, a SGB representative, a SMT representative, the Network administrator, an ICT educator, the librarian and a learner representative.

The function of the team is to develop an ICT policy for the school with attendant penalties for breach of the policy. The policy should be approved by legal professionals to ensure that it is implementable in terms of the legislation and also that child protection procedures are followed.

The team should be able to record and monitor internet use for the purpose of managing system performance, monitoring compliance with, policies, or as part of disciplinary or other investigations. Violations of the rules should result in disciplinary action, including the loss of a learner's privilege to use the school's information technology resources.

4.2.5. Responsibilities of advisory team

This team should be the first point of call for any cyber threat incident. It can be composed of; the principal, a counsellor / psychologist, the ICT coordinator and a life orientation educator.

4.2.6. Responsibilities of learners

Learning to take responsibility for one's behaviour is an important element of education and this includes using ICT responsibly. The ease with which technology can be accessed can lead to spontaneous reaction and it is important that the learners understand the need to select the most appropriate communication tool to resolve issues and not to create them, (Department of Basic Education 2010).

The learners should be allowed to use the school's Internet facilities only for learning related activities that are approved by the educators. They should not cause interference with or disruption to other learners or equipment, and should not access or distribute inappropriate material. This includes;

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, (including jokes and inappropriate images)
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (e.g. viruses, and worms)

The learners should be encouraged to inform their educators if they come across inappropriate online material or anything else that makes them feel uncomfortable. They should report threats or distressing materials and never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable. In addition to this they should not make threats online. They should learn how to avoid exposure to inappropriate material for activities, and protect themselves when they are online. They should also learn how to use technology, including mobile technologies and social networking sites, in responsible and ethical ways. In addition they should feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate material. In response, these adults should take appropriate actions to protect learners or young persons.

If cyber threats becomes serious and do not stop, the learner should contact the advisory team or the SAPS and file a report. Learners who are victims of cyber threats should block or limit

all communications to the guilty parties and should save the harassing messages and forward them to the advisory team or the SAPS.

4.3 Role players outside the school

4.3.1. Responsibilities of parents

Parents should be aware of and monitor their children's activities on MySpace and other network sites to check the content, and should have clear internet and cell phone agreements with their children (The Alannah and Madeline Foundation 2007). It is vital that parents/caregivers understand cyber threat and the mechanics of cyber threat. Parents have an obligation to monitor their children's online activities, (Shariff 2005). When parents discover that their children are being threatened, it is always best to contact the school's administrators, or advisory team. They should work closely with schools for prevention and early intervention.

Parents should talk to their children and take an interest in their social life both offline and online. There should also be open lines of communication between parents and children that focus more on online etiquette and behaviour. They should watch for mood changes in their children after they have used the computer. Many parents do set rules and forbid their children to talk to strangers or to divulge personal information online. Serious cases should be reported to the police and Internet Service Provider (ISP).

4.3.2. Responsibilities of industry

Internet service providers have policies and can track instant messaging as emails leave. New cell phone technology has just been launched which retrieves messages that are admissible as evidence in a court of law. However, as cyber threat is an embedded social problem, these are only evidence gathering solutions and not people solutions.

4.3.3. Responsibilities of government

Schools must report cyber behaviour which they suspect to be an e-crime to the police. If there is evidence of a crime, (such as an assault), and has been captured on a cell phone or other electronic device, the device should be confiscated and handed to the investigating police officer. It is important that the device should not be used to view any video clips since this may make the information inadmissible in a court of law. The principal should cease any further investigation once he/or she has decided to hand the investigation to the SAPS. If a crime is involved, (e.g. suspected child pornography or threats to safety), it may constitute an e-crime, which requires that the police be notified. E-crime occurs when a computer or other electronic communication device (e.g. cell phone) is used to commit an offence, is targeted in an offence, or use as a storage device in an offence. It is important that learners understand that the production or distribution (including texting and posting of lewd images of themselves or others) may constitute child pornography with potential a criminal penalty. Suspected activities should be referred to the SAPS with potential evidence confiscated and kept securely until given to a police officer. The school may suspend or suspend pending exclusion the leaner(s) involved in such events. The DBE can provide assistance in determining an appropriate response when any ICTs are misused.

Ethical and accountable use of technology applies at district level as well as in schools. District Officials should support the school in implementing the guidelines.

The DBE should outline the policies and repercussions of online behaviour, including cyber-threat. All schools should adopt policies that prohibit cyber-threats. School administrators "may impose consequences for acts of harassment, intimidation or any form of cyber threat that occur off school grounds, but only when these acts substantially disrupt school life and falls under the DBE policies.

4.3.3 Responsibilities of non-governmental organisations

It should be mandatory for educators to notify the Child Abuse / Child Protection Unit if they suspect child abuse and neglect. These organizations have an important role to play in educating the government about areas of specific concern for learners in cyber space, (*The Right Times* 2012)

4.3.4. Responsibilities of educational organisations

Educational Organisations should continue to hold workshops, do research and give presentations on cyber safety topics in order to help school communities. The Information Security Awareness Research Group in the School of Computing, at the University of South Africa (Unisa), presented a workshop on cyber safety on 24 November 2010. The main focus was on cyber safety issues and concerns relevant to learners and end users of ICT such as the internet and cell phones. The University of Johannesburg and the Nelson Mandela Metropolitan University were actively involved in the workshop, (School of Computing 2010).

5. A PROPOSED INCIDENT HANDLING FRAMEWORK FOR CYBER THREATS IN SOUTH AFRICAN SCHOOLS

The increasing ownership of cell phones and the internet requires that school administrators, educators, learners, and parents take steps to ensure that cell phones and the internet are used responsibly. Currently, most schools in South Africa do not have uniform consensus on how to address the problem of cyber threat, and therefore educators are not sure how to handle these incidents. Burton (in *The Star* 14 February 2012:12), states that schools and the police should standardise protocols or reporting mechanisms on how to deal with reports and incidents of cyber threat, and that educators, parents and adults in general should be sensitised on how to identify when online violence might occur. Learners rarely report these incidents to adults, and very few of them tell their educators about it, (Rigby 1997). Some learners, in South Africa, feel that educators, parents and other adults do not use Facebook and therefore cannot understand these problems. In an Australian study, Campbell (2005) found that young people believe that adults do not understand that they have an online life and therefore could not understand their online problems. Many of them felt that if they reported incidents, they would not be believed, the incident would be trivialised by adults, or they would be made to feel that they were responsible for being threatened. Worse still, advice on how to deal with those who make threats online seemed to be non-existent, since the available advice was mostly for the victims.

It is hoped that the proposed incident handling structure and framework will help learners and educators to deal with cyber threats in South African schools. The diagram outlines the decision making process that should be followed if a cyber-threat incident occurs. It is critical that the safety and welfare of learners are considered as paramount throughout the process.

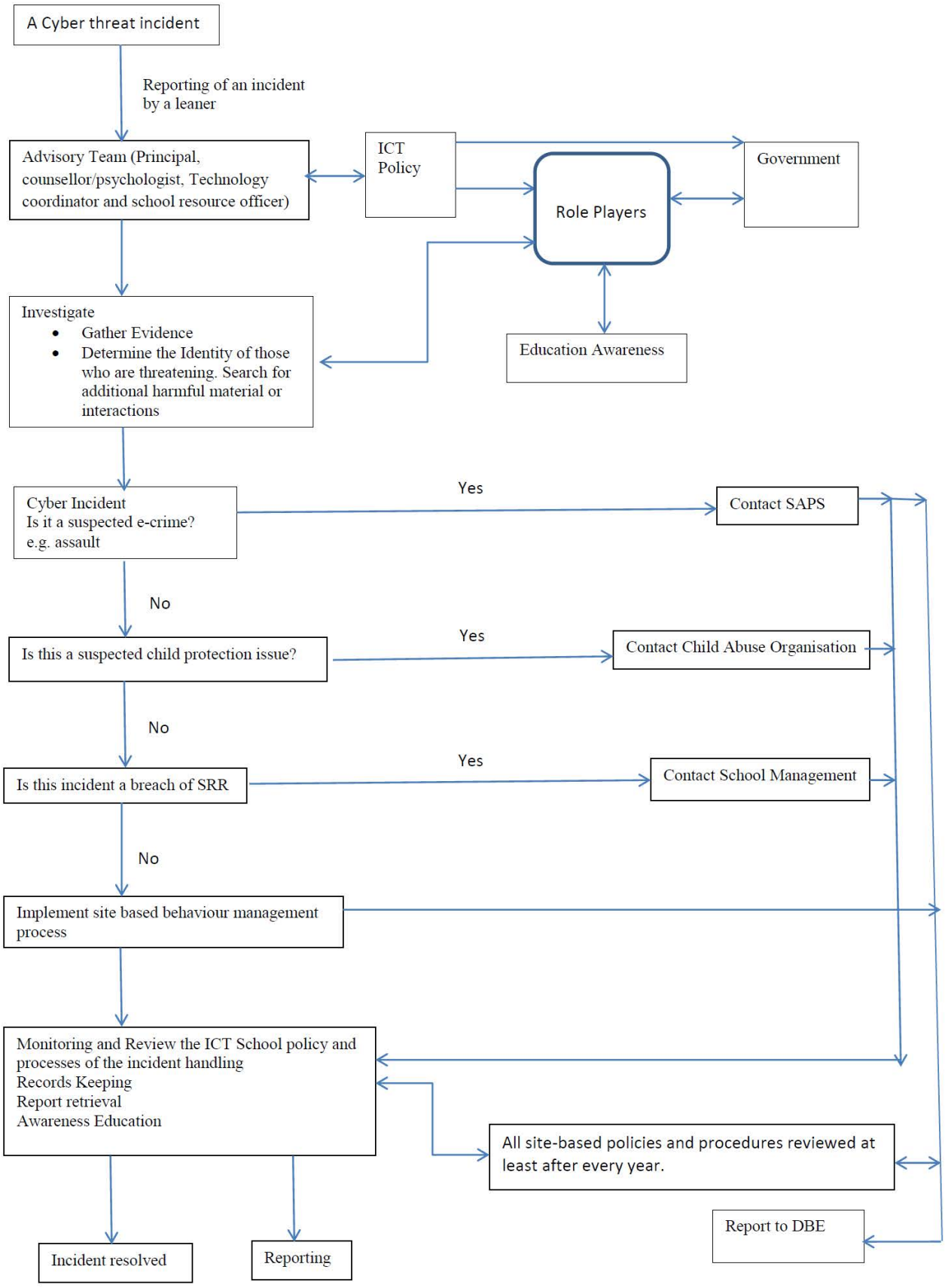

Figure 2. Proposed incident handling framework of cyber threats in schools

5.1 Incident handling procedure

5.1.1. Advisory Team

This is the first point of call for learners to report cyber threat incidents. All learners should be made aware that they can report anonymously or confidentially. Additionally, an online report feature on a school home page could also be considered with the provision of a Uniform Resource Locater. All members of the team should have the rights to override the URL filters in order to have access to records during their investigations.

5.1.2. Investigate

Gather Evidence and preserve it

All evidence gathered should be preserved. Parents, learners and staff should be advised to preserve evidence on computers or devices. The technology coordinator should assist if necessary.

Determine the identity of the aggressor

The identity of the aggressor may be difficult to access because it may be obvious, anonymous, or impersonation. The advice of a Technology Coordinator could be of value in this circumstance. If there are any anonymous cyber threats or concerns of impersonation, and there are reasons to suspect that certain learners could be involved, then a search of internet use records of learners should be conducted. If a criminal action is involved, law enforcement has significantly greater abilities to identify anonymous creators.

Search for Additional harmful material or interactions

The technology coordinator and a librarian should assist. A search should include all suspected participants. A search of files and internet use records should be conducted, even if the threat appears to be an off-campus activity. Conduct an additional search including online environment where initial material appeared, search engine for a name of learner, friends, enemies, or school name. Ask about related on-campus actions.

Review of the Investigation

Review all the material and evidence gathered. Identify a learner that could be causing harm, at school or online. Determine the roles which different learners could be playing and whether their threats are a continuation of the previous threats or retaliation.

5.1.3. Cyber incident – a suspected e-crime

If the online material appears to present a legitimate imminent threat of violence and danger to others, contact law enforcement (SAPS), and initiate a protective response.

5.1.4. Child Protection Issue

A violence or suicide risk assessment should be done to determine if the evidence gathered raise concerns that learner(s) may pose a risk of harm to others or self. The threat may come from learner(s) who could have posted the material or from learner(s) who could have been victimized. If it is a suspected child protection issue then a violence or suicide risk assessment should be done in accordance with DBE process and then contact Child Protection and Abuse Organisation.

5.1.5. A Breach of School Rules and Regulations (SRR)

Determine the nature of the material to see if there is any substantial threat or disruption. If it is a nuisance activity, ignore it but if it is something of substantial harm then the School Management should impose formal discipline and get to the root of the problem. Suspensions should be avoided unless there are school safety concerns. More focus should be put on a restorative justice response. A fully documented evidence, decision – making process, and rationale for formal discipline response should be produced and kept for future references.

5.2 ICT polices

It is strongly advised that each school should develop an ICT policy which must be agreed upon and signed by the learners and their parents to indicate that they accept the policy and related sanctions. The policy should be used as an agreement for parents to monitor their children while they are using computers and cell-phones. A signed copy of the agreement should be placed in the learner's file for reference. In order to engender a sense of personal responsibility in the learners, it is important that wording of the agreement should be value-based as opposed to rule-based.

The Department of Basic Education Draft Guidelines on e-Safety states that the ICT policy should include a clear statement of the actions, the school will take if the policy is breached. Parents and caregivers should take all reasonable steps to ensure that their children comply with the requirements. It is stressed that in cases, where disciplinary measures should be taken, the school's disciplinary procedures (including exclusions when required) should be used proportionally and appropriately (Department of Basic Education 2010). In some cases, it is best for schools to work constructively with parents/guardians. The ICT policy should be linked to and the penalties defined by, the existing code of conduct (South African Schools Act) that must be adopted by every public school. It should clearly define the penalties imposed for violation of the agreement. The policy must be reviewed and updated regularly to ensure its appropriateness and effectiveness. It must be regularly reinforced by all users. Campell (2005) believes that each school should adopt its own policies and guidelines that are tailored to its own individual requirements and context.

Prospect High School in Schaumburg, requires students to sign a 17-point agreement and cyber threat is clearly addressed in the second statement of the agreement; "While online, I will not use language [that] may be harassing, intimidating, threatening or offensive to other users. I will treat others with respect. The written and verbal messages I send while on the Internet will not contain profanity, obscene comments, sexually explicit material, or expressions of bigotry, racism, or hatred (Illinois District 214 2006)."

5.3 Supervision monitoring and review

The school, the IT manager, and other authorised employees, should monitor the use of the school's IT resources to help ensure that users are secure and in conformity with the school's ICT policy. The ICT manager and the team should 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/ other person, or to protect property. They may also use this information in disciplinary actions, and should furnish evidence of crime to law enforcement officers.

The frequent change of technology requires that policies, procedures and agreements should be updated yearly. Policies have to be reviewed to ensure that all school employees (including educators), learners and parents understand them. Learners are involved in the cyber world and therefore the school, parents and other adults should be there to guide and protect them.

5.4 Advantages of the framework

Dialogue, both verbal and nonverbal, can help learners to feel connected and cared for. If the learners know that the people around them care, it makes going to school worthwhile for both the victims and aggressors in cyber threat.

Among the learners, this will result in; caring and respectful behaviours during learner-to-learner exchanges; safe and nurturing environments for the healthy development of identity and citizenship; and tolerance and impartiality. Implementing policies and practices that encourage learners to respect each other, whether online or face-to face remains an important responsibility of the school.

5.5 Education awareness programmes

These should include:

- Make the time to conduct school wide surveys among learners and staff about their knowledge and attitudes towards cyber threat. Find out if there are specific places or times when cyber threat occurs and use this information as a tool to prevent other issues.
- The consequences of cyber threat should be known and understood by the learners. By enforcing these consequences, learners will understand the reality of cyber threat and this will force them to stop these behaviours.
- Ensure confidentiality between the learners and the school authorities and let the learners know that they can trust adults.

All school officials should be trained: not only educators, but also coaches, after school supervisors and even transport drivers should be aware of threats or listen out for cyber threats. They should know how to respond to the triggers and how to reinforce positive problem solving. Teaching aids like posters, pamphlets, wallet booklets, digital literacy lesson plans and child friendly sites can be used. Other awareness programmes should include teaching parents; how cyber threats can be prevented in the home and how they can respond to incidents.

6. CONCLUSION

South African schools are putting a lot of effort into using ICT to support learners' learning. With this comes the responsibility to ensure that learning takes place in an environment where safe and responsible use of ICT is modelled and taught. A comprehensive infrastructure of policies, procedures and use agreements has to be put in place, and understanding the responsibility that comes with technology is a key to cyber safety. Through the use of guidelines, structures and procedures, learners will be empowered to use the internet and enjoy all the positive benefits it offers. The aim of this research is to propose ways that can help learners to feel confident about alerting adults when they feel unsafe online. This article therefore serves as a proposal of guidelines, structures and procedures on how to deal with cyber threats in South African schools. "You cannot gain ground if you are standing still", (Clinton 2000).

Further research will be about the framework being applied to schools for evaluation; implementation and improvement. The framework will be transformed into a prototype. This will give the role players the chance to be involved in the design and to comment about the appropriateness and feasibility of the incident handling framework and prototype. The framework will be evaluated for use as a reference tool in the handling of cyber threats incidents. It would be reviewed and updated regularly to maintain its relevance.

7. REFERENCES

[1] APHA Annual Meeting & Exposition. 2007. Developing and implementing a state-wide policy for schools on cyber threats. Paper delivered at the 135th APHA Annual Meeting & Exposition (3-7 November). Washington, DC

[2] Aune, N. M. 2009. Cyberbullying. (Unpublished Master Research). The Graduate School, University of Wisconsin-Stout.
(http://www2.uwstout.edu/content/lib/thesis/2009/2009aunen.pdf)
Retrieved on the 20 March 2011

[3] Belsey, B. 2006. Cyber bullying: An emerging threat to the 'always on' generation.
http://www.cyberbullying.ca/pd/Cyberbullying_Article_by_Bill_Belsey.pdf)
Retrieved on 11 June 2011

[4] Bhat, C.S. 2008.cyber Bullying: Overview and Strategies for School Cousellors, Guidance Officers and All School Personnel.*Australian Journal of Guidance and Counselling,* 18(1), 53-55

[5] Campbell, M.A. 2007. Cyber bullying and young: Treatment principles not simplistic advice. QUT Digital Repository. Paper of the week 23rd February 2007

[6] Campbell, M.A. 2005. Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling,* 15(1), 68-76

[7] Clinton, B. 2000. DEPAUL CTI. School of Computing Science, Telecommunications and Information Systems.
(http://facweb.cs.depaul.edu/yele/word_wisdom.asp)
Retrieved on the 22 March 2011

[8] Department of Basic Education. 2011.
(http://www.education.gov.za/TheDBE/tabid/54/Default.aspx)
Retrieved on the 20 March 2011

[9] Department of Basic Education. 2010. Draft Guidelines on e-Safety in Schools: towards responsible, accountable and ethical use of ICT in education.

[10] Department of Basic Education. 2009. Department of Basic Education.
(http://en.wikipedia.org/wiki/Department_of_Education)
Retrieved on the 20 March 2011

[11] Gauteng Provincial Government. 2009. *Gauteng Online Schools Project.* Gauteng Provincial Government: South Africa.
http://ww.info.gov.za/speech/DynamicAction?pageid=461&sid=4329&tid=4474/)
Retrieved 26 April 2012

[12] Government of South Australia.2009. *Cyber-Safety. Keeping Children Safe in a Connected World.A Guidelines for Schools and Preschools*. South Australia: Department of Education and children's Services
(http://www.decs.as.gov.au/speced2/pages/cybersafety/)
Retrieved on 15 July 2011

[13] Illinois District 214, 2006. Cyber Bullying: What Teachers, SocialWorkers and Administrators Should Know. Illinois Child Welfare. 2006-2007. Volume 3. Numbers 1 and 2
(http://www.d214.org/parents/info/studentAUP.php

[14] Internet Watch Foundation. 2012. Internet Watch Foundation report highlights new abuse of online technology. *Internet Watch Foundation's 2011 Annual Report launched on the 26 March 2012*
(http://www.iwf.org.uk)

Retrieved on 26 April 2012

[15] Li, Q. 2008. Cyberbullying in schools: An examination of preservice teachers' perception. *Canadian Journal of Learning and Technology.* Vol. 34, No.2 Spring/printemps, 2008

[16] Ministry of State Security. 2012. Statement on the Approval by Cabinet of the Cyber Security Policy Framework for South Africa. (http://www.ssa.gov.za/Media%20Room/2012/11032012_Cabinet_appr_Cyber_Security_Framework.pdf)

[17] Parliamentary Monitoring Group, (2012). Justice Crime Prevention and Security Cluster. Briefing: Parliamentary. (http://www.pmg.org.za)
Retrieved on 21st May 2012

[18] Partnership for 21st Century Skills. 2011. Information Literacy and ICT Literacy (http://www.p21.org/)
Retrieved on 29th May 2012

[19] Petersen, L., & Rigy, K. 1999. Countering bullying at an Australian secondary school. *Journal of Adolescence*, 22, 481-492.

[20] [20] Pokin, S. 2007. Megan Meier story.*The St. Charles Journal*, 2007

[21] Pruitt-Mentle, D. (2000) C3 Framework Cyberethics, Cybersafety and Cybersecurity Promoting Responsible Use. Educational Technology Policy, Research and Outreach (http://www.edtechpolicy.org/cyberk12/Documents/C3Awareness/C3_framework_full_final.pdf)
Retrieved on 13 March 20

[22] Rigby, K. (1997). What children tell us about bullying in schools? *Children Australia*, 22(2), 28-34.

[23] Robinson C (2009), Cyber – Safety, Keeping Children Safe in a Connected World – *Guidelines for Schools and Preschools*

[24] RSA, 2010. Draft Cybersecurity Policy of South Africa. *Government Gazette,Vol. 536 (No. 32963):* Government Printer.

[25] RSA, 2009. *Government Gazette, Vol. 527 (No. 32207):* Government Printer.

[26] RSA, 2009. *South African Government Information: Gautengonline schools project reaches the 1 000-connected schools milestone,* Gauteng Shared Services Centre: Gauteng Provincial Government. (http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=4329&tid=4474)
Retrieved on the 25 March 2011

[27] RSA. 2008. *Regulation of Interception of Communications and Provision of Communication-related Information Act, 2008 (Act No. 48 of 2008)*

[28] RSA. 2002. *Electronic Communication and Transactions Act.* (ECT Act – No. 25 of 2002). Pretoria. Government Printers (www.internet.org.za./ect_act.html#INTERPRETATION_OBJECTS_AND_APPLICATION)
Retrieved on 20 August 2011

[29] RSA. 2002. *Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002. (Act No. 70 of 2002)*

[30] School of Computing. 2010. The Information Security Awareness Research Group in the School of Computing, Unisa. *Workshop presented on 24 November 2012, Unisa, Pretoria, South Africa*

[31] Shariff, S. 2005. Cyber-dilemmas in the new millennium: School obligations to provide student safety in a virtual school environment. *McGill journal of Education, 40(3).*

[32] South African Police Service Annual Report.2009/10.*South African Police Service 2009/10 Annual Report: Administration hearings.* Parliamentary Monitoring Group

[33] Starling 1979.*The politics and economics of public policy: A introductory analysis with cases*. Illinois: The Dorsey.

[34] Stron, P.S., & Stron, R.D. (2005).When teens turn cyberbullies. The *Education Digest,* 71 (4), 35-41.

[35] The Alannah and Madeline Foundation, in consultation with the National Coalition Against Bullying and Center for Strategic Education. 2007. Cyber-Safety Symposium Report. (cyber-safety symposium held on the 17-18 May 2007 at Camberwell Grammar School, Canterbury, Melbourne)

[36] *The Benoni City Times.* 2012. Safety on Facebook. 10 February:2

[37] The Partnership for 21st Century Skills, 2011 Framework for 21st Century Learning (http://www.p21.org/storage/documents/1._p21_framework_2-pager.pdf)

[38] *The Right Times.* 2012. The National Cyber Security Policy Framework for South Africa. 27 March. (http://childrensrights.org.za/magazine/index.php//the-national-cyber-security-policy-framework-for-south-africa)
Retrieved on 21 May 2012

[39] *The SOWETAN.* 2011 The dark side of cell phones: Shield your children against cyber-crime. 7 November:10.

[40] *The Star.* 2012. Girl attacked after cyber bully ordeal; Teen, 15, taunted on Facebook and BBM. 9 February:1

[41] *The Star.* 2012. Cyber bullying in context. 14 February12.

[42] The Teacher Laptop Initiative.(2010). . (http://www.teacher-laptop.co.za)
Retrieved on the 3rd of November 2011

[43] Time Warner Cable and Cyber Angels, 2007. Cyber Safety Guide.
http://www.cyberangels.org/docs/cybersafetyguide.pdf
Retrieved on 27 July 2011

[44] Willard N., M.S., J.D. (2007). An educator's guide too cyber bullying and cyberthreats. Center for Safe and Responsible Internet Use (CSRIU). (http://csriu.org/cyberbully/docs/cbcteducator.pdf)
Retrieved on 19 March 2011

[45] Willard, N.E. (2006). Cyber *bullying and cyber threats: Responding to the challenge of online social aggression, cruelty threats, and distress* (2nd ed.).Eugene, OR: Center for Safe and Responsible Internet Use (CSRIU).

[46] Willard, N.E. (2006). Flame Retardant.School Library Journal. 52(4), 55-56

[47] Willard, N.E. (2005). An educator's guide too cyber bullying and cyber threats: Responding to the challenge of online social aggression, threats, and distress. Center for Safe and Responsible Internet Use (CSRIU).