Cyber Threat Incident Handling Procedure for South African Schools

N. Sonhera[1], E. Kritzinger[2] and M. Loock[2]

[1]ICT Department, Vaal University of Technology, Ekurhuleni Campus
[2]School of Computing, University of South Africa (UNISA), South Africa
e-mail: nausonhera@yahoo.com; {kritze; loockm}@unisa.ac.za

Abstract

With the increase of networks and electronic tools, the online antisocial behaviours have increased and cyber threats have consequently became prevalent world-wide. The new technologies are challenging current networking practices, and this has given rise to cyber threats in South African schools. Learners are not aware of what they should do when threatened online. There is a lack of procedures that can be consistently followed by South African schools, governing boards and educators. As a result, many learners remain vulnerable to the negative effects of these threats. A lack of fixed reporting procedures when dealing with incidents of cyber threats in South African schools, the potential legal obligations and the lack of research in this area has prompted this research. This paper proposes a cyber threat incident handling procedure for South African schools, based on already existing cyber safety guidelines for schools in other countries like Australia and Canada. The proposed procedure will contribute to these existing guidelines by determining and implementing characteristics specific for South African schools.

Keywords

Learner, cyber threats, incident handling procedure, cyber space, role players, cyber safety

1. Introduction

Both the academics and practitioners of the 21st century have applauded the paradigm shift in schools of encouraging learners to be computer literate (Li 2008). With the right to have and use this technology also come responsibilities on how to use it responsibly in a way that ensures no harm is caused to other learners. However access to new technology has led to an increase in misuse and abuse of technology and this has brought about many incidents of threatening, harassing, embarrassing and humiliating behaviours and actions online (Popovac & Leoschut 2012). The misuse and abuse has become a concern for parents, social psychologists, authorities of schools, colleges and universities (Fisher 2013; Kite, Gable & Filippelli 2013; Oosterwyk & Kyobe 2013). On the other hand, these behaviours are placing learners' psychological health, safety, and well-being at risk (Popovac & Leoschut 2012). This could cause low self-esteem, anger, school failure, avoidance, school violence or suicide among learners (Li 2008; Willard 2006).

This article, therefore proposes a procedure that could assist learners, who are threatened online, to alert respective role players. The procedural approach could also assist educators and parents who do not know how to deal with learners who are threatened online. The article is divided into two sections; the first section is about role players involved in the incident handling procedure. The second section is about an incident handling procedure which could help learners to be confident about alerting respective role players when they feel unsafe online.

2. Background of the study

Today's learners are no longer the learners the educational system was designed to teach. They have changed radically; they represent a first generation which is growing up with new technology. They spent their entire lives surrounded by and using computers, iPods, MP3 players, Androids, tablets, Play stations, Smart phones, and other tools of the digital age (Herther 2009). The 21st century has brought with it a different revolution; learners who are on the cutting edge of technological proficiency (Gouws 2014). They are exposed to new-age technologies, various social networking sites, unlimited access to the internet and chat rooms, and phone communications (Badenhorst 2011); (Tokunaga 2010). Their social landscape has changed completely; they constitute a generation of people who know more about technology than their parents, grandparents and, in most cases, their educators and lecturers (Gouws 2014).

As a result of this ubiquitous environment and the volume of learners' interaction with it, today's learners think and process information fundamentally differently from their predecessors. On the other hand, some adults who were born in the non-digital world have adopted many aspects of the new technology and are called Digital Immigrants (Prensky 2001). Unfortunately for Digital Immigrant educators, the people sitting in their classes grew up in the environment of hypertext, downloaded music, phones in their pockets, library on their laptops and, beamed messages and instant messaging. Digital Immigrant educators, who speak an out-dated language, are struggling to solve the cyber problems of a population that speaks an entirely new language (Herther 2009). Many educators continue to prepare learners for a world which has long since disappeared.

If educators teach today's learners as they taught yesterday learners, then they are robbing them of tomorrow – John Dewey (1859-1952).

Online threats takes place off the radar screen of educators and parents, this makes it difficult to detect in schools and more impossible to monitor off school premises (Steeves & Wing 2005). Discipline has been a problem in South African schools. Research has found that educators lack a repertoire of effective methods of maintaining discipline (Mawdsley, Ralph, Smit, Marius, & Wolhuter 2013).

With these increases in technological usage, cyber threats are also on the rise and have become a major concern in South African schools. Unfortunately, there are increasing reports of learners using these technologies to post damaging text or images that raise concern of an act of violence toward others or themselves, to cyber threaten their peers or engage in other aggressive behaviour. Victims of these horrific acts are usually school learners (Oosterwyk & Parker 2010). Therefore it is increasingly important to research in the South African context on the changing life of the learners. More focus should be on how the victims can be helped, with particular attention on how role players can support learners in coping with the demands and challenges posed by technological advances (Gouws 2014).

3. Problem Statement and Research Questions

3.1. Problem Statement

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 (Bailey 2012). As a result, many learners remain vulnerable to the negative effects of cyber threats. An example is that of a Krugersdorp High School girl who was attacked after a cyber-threat ordeal. Threats were reported by the learner to the school management yet no clear procedures were followed to assist the learner until the physical attack occurred. The gap which exists now makes educators feel unsupported and so they ignore these unethical violations rather than to follow ill-defined and unenforced policies (Pruitt-Mentle 2000). This lack of support sometimes deters learners from reporting cyber threat incidents.

3.2. Research Questions

This study seeks to understand how cyber threat incidents are handled in schools and the contribution from the role players. The article examines this new phenomenon guided by the following questions:

- What is the prevalence of cyber threats among learners within South African schools?
- How do learners react after they have been cyber threatened?
- To what extent are role players concerned about cyber threats in schools?
- What are the prevention and intervention techniques for cyber threat incidents which can be identified?
- What are the responsibilities of the role players in cyber safety?
- How can an incident handling procedure assist learners to report incidents of cyber threats?

4. Literature Review

The literature review focuses on what has been documented by other researchers in terms of the prevalence and effects of cyber threats in schools. Existing conference papers, journals, articles, books, online sources, dissertations, theses, educational and governmental documents will be examined. This section is also aimed at highlighting some incidents of cyber threats in South Africa which are online articles or anecdotal cases which have been reported by the media.

4.1. Cyber Threats Incidents

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). New technologies have resulted in an increase in cyber threats in South African schools (Jansen van Vuuren, Grobler & Zaaiman 2012). One example is of a 16-year-old girl who attends a school in Port Elizabeth, she commented that parents do not know how bad the issue of cyber threat is. This is because a learner being threatened is only known to those on a specific Facebook or BBM (BlackBerry Messenger) group (Alexander & Harvey 2012). Alexander and Harvey (2012) reported that some learners read news on websites and what most people consider as horrific stories they see them as comic and humorous. They then draw inspiration from these violent stories and do the same to hurt other learners. A new type of forum or chat room that has attracted the attention of learners in Cape Town schools called “Outoilet” - http://outoilet.wen.su/ - allows learners to post mean and hurtful things about their friends.

4.2. Efforts for Structures, Guidance and Procedures

Generally, most of the countries worldwide are addressing the problem of cyber threat incidents in schools. In Australia, a number of schools, Department of Education, different groups and organisations have focused on cyber ethics, cyber safety and cyber security in education (Department of Education and Children’s Services 2009). Epstein and Kazmierczak (2007) suggest that it is necessary to conduct periodic surveys to assess the degree of cyber threats. Bhat (2008) added that role players should address cyber threats in schools. Campbell (2007) recommends that victims need to be empowered and not to be blamed.

In South Africa, the Cabinet approved a National Cyber Security Policy Framework with some challenges on how to bridge the gap between law and technology (Minister of State Security 2012). The Policy Framework acknowledges that the South African Cyber Security Legal Framework is scattered across various pieces of legislation and is therefore administered by different government departments (Badenhorst 2011). The South African government has also promulgated a number of acts on cyber threats (Kganyago 2012). As an initiative towards cyber safety, the DBE (Department of Basic Education) has developed guidelines on electronic safety in schools (Department of Basic Education 2010). Additionally, the Centre for Justice and Crime Prevention and the DBE (2013) have produced the school safety framework which is mainly focusing on bullying in general.

The case of Le Roux v Dey is the only court ruling by South African courts involving learners’ use of cyberspace (Constitutional Court of South Africa 2011). In this case Hendrick Pieter Le Roux (1st defendant) had created a computer image at his home in which the faces of the principals and deputy principal of his school were super-imposed on an image of two naked gay bodybuilders sitting in a sexually suggestive posture. This image was shared with the whole school. Understandably, the principal and deputy principal were embarrassed and felt particularly aggrieved by this. However, despite the disciplinary steps against the learners, the tag "Dey is gay" was heard in the corridors of the school which perpetuated untrue rumours and continued to infringe the deputy principal's dignity. There is a growing tendency in South African schools to challenge the status and authority of educators with a concomitant breakdown in discipline.

4.3. Gap Identified in the Literature

Although South Africa has publicised a number of acts on cyber security and safety, there is a lack of processes in place which can be used for cyber threat incident reporting in schools. There are no fixed procedures within the schools to handle cyber threats incidents. Burton and Mutongwizo (2009) state that currently there are no specific procedures that directly addresses cyber aggression and cyber safety of learners both online and in the realm of cellular technologies. As a result of all this, the learners are facing a lot of online challenges.

The challenges are that learners are no longer safe at school or in their homes since there are no barriers for threats found online (Kite et al. 2013). An example is of a 39-year-old educator who has been suspended from Hyde Park High School after a mother had revealed that he had been sending her 16-year-old son pornographic material (Neille 2013a). On the other hand school personnel do not know how to deal with learners who are cyber threatened because of the absence of cyber threat handling procedures (Bailey 2012; Tokunaga 2010). From learners' point of view, most of the time when they do report these threats, nothing is done by the School Management Board (Alexander & Harvey 2012). It is also reported that the trend involving school learners filming their peers being beaten or bullied in order to gain notoriety is becoming increasingly apparent in South African schools (Neille 2013b). On the other hand, according to Mogotlane, Chauke and van Rensburg (2010), there is now a new family structure called a child-headed household in South Africa. As indicated by Mudhovozi (2013), aggressors often come from these families. This also implies that there is often a lack of monitoring and supervision of these children by adults. This allows cyber threats to occur unnoticed and for an extended period of time without any intervention.

5. Research Methodology

The literature study was undertaken to provide sufficient background on the existence of cyber threat incidents in South African schools. It also highlighted a lack of procedures that could be consistently followed by South African schools, governing boards and educators when handling cyber threat incidents.

This collection of theoretically valid and reliable evidence, contributed to a better understanding of learners' interactions in cyber space and how much help they get when they are in trouble. The explanatory nature of this research was aiming at revealing a wide range of opinions and experiences of cyber threat incidents in schools. This information has been utilised to help develop empirically driven prevention and intervention procedure to ensure the safety and psychological well-being of learners (Campbell 2005; Lodge & Frydenberg 2007).

6. Research Structure

This article is focusing on developing and proposing a cyber threat incident handling procedure which could help a learner who has been threatened online to alert respective role players. The procedural approach could assist the respective role players with procedure which could be taken to intervene. This article is therefore divided into two sections, namely the "Role Players" and "The Incident Handling Procedure".

6.1. Section 1- Role Players for the Framework

This section seeks to equip all role players with guidelines and ability to recognise potential dangers and to be discerning enough to avoid them. Figure 1 summarises how the role players fit together.

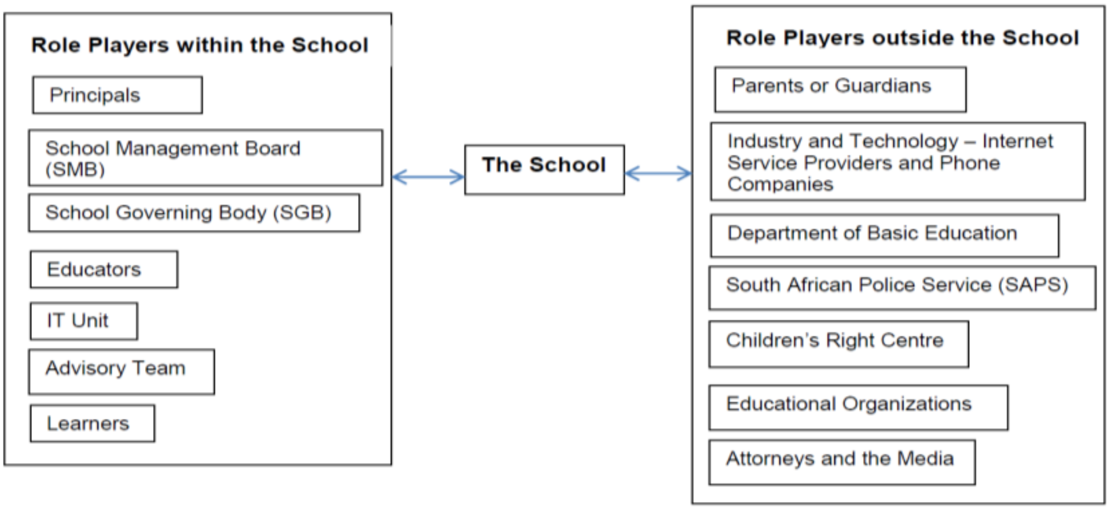
Role Players within the School
Principals
School Management Board (SMB)
School Governing Body (SGB)
Educators
IT Unit
Advisory Team
Learners
The School
Role Players outside the School
Parents or Guardians
Industry and Technology – Internet Service Providers and Phone Companies
Department of Basic Education
South African Police Service (SAPS)
Children's Right Centre
Educational Organizations
Attorneys and the Media

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

The responsibility of the school is to incorporate technology as a valuable learning tool, and to equip learners to be discerning, responsible and ethical participants in the information age (Department of Basic Education 2010). Schools should develop their own Information and Communication Technology (ICT) policies; since learners are bringing sophisticated range of handheld devices to school that give them separate access to online content that is not necessarily appropriate. The school may suspend or suspend pending exclusion the leaner(s) involved in cyber threat incidents. School do not exist in isolation; they are driven by role players, within and outside the school.

6.1.1. Role Players within the School

Role players within the school community have responsibilities in creating a school environment free from cyber threats (Centre for Justice and Crime Prevention and the DoBE 2013). Preventing and addressing these threats requires a collaborate effort and given below are the responsibilities of role players within the school.

- Responsibilities of the Principals

The principals should approve the posting of any information on school web sites, news groups, web-based forums, and should ensure that it conforms to minimum cyber safety standards (Department of Education and Children's Services 2009). They should take action if posted material might disrupt school safety. It is important that school administrators carefully assess the situation and provide evidence justifying any disciplinary action. Principals should also ensure that the school's private information is not accessible to the public on the school's websites.

- Responsibilities of the School Management Board (SMB) and the School Governing Board (SGB)

The principal, SMB and SGB should contribute to developing an ICT policy and should meet and consider what additional rules or guidelines staff and learners may need that are specific to their own school situation. This team 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 (Department of Education and Children's Services 2009). The team should be responsible for the behaviour management.

- Responsibilities of the Educators

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). During their teaching, 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 (Department of Education and Children's Services 2009).

- Responsibilities of Information Technology Unit

The Information Technology Unit should consist of the ICT Coordinator, an SGB representative, an SMB representative, a Network administrator, an ICT educator, a librarian and an RCL (Representative Council of Learners) - 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 does not contradict or impinge on other legislation, and also that child protection procedures are correctly followed.

- Responsibilities of Advisory Team

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

- Responsibilities of Learners

Learners should be able to select the most appropriate communication tool to resolve issues and not to create them, and to be responsible for their own behaviour (Department of Basic Education 2010). They should use the school's internet facilities only for learning related activities that are approved by the educators and not to access or distribute inappropriate material. Learners should be confident about alerting the adults when they feel unsafe, threatened, bullied or exposed to inappropriate material online. If cyber threats become serious, the learner(s) should contact the school Advisory Team or the SAPS and file a report. Learners who are victims of cyber threats should block or limit all communications with the accused parties and should save the harassing messages and forward them to the school Advisory Team or the SAPS.

6.1.2. Role Players outside the School

Sometime more serious or repeat cyber incidents might involve external role-players. Given below are some of the responsibilities for role players outside the school.

- Responsibilities of Parents or Guardians

Parents should monitor their children's activities on social sites by checking the content, and having clear internet and cell phone agreements with their children (The Alannah and Madeline Foundation 2007). It is vital that parents or guardians understand cyber threats and the mechanics of cyber threats. When parents discover that their children are being threatened, it is always best to contact the School Management or School Advisory Team. They should work closely with the schools for cyber threats to be prevented and early intervention measurers to be taken.

- Responsibilities of Industry and Technology – Internet Service Providers and Phone Companies

Internet Service Providers should track instant messaging and these messages could be used as evidence in a court of law (Campbell 2007). They should work with the DBE and schools in a proactive and educational way which will help make all the school stakeholders and parents aware of the cyber threats, how to prevent them and what to do whenever they occur. If threat messages are coming through mobile devices, a phone company should be able to trace the source of the message and warn the aggressor that he may lose his cell number and access to the network if the threats persist. The up-to-date filters and other useful technologies should be developed by industry and be freely accessible to schools and parents, and be easy to implement.

- Department of Basic Education

The DBE should outline the policies and repercussions of online behaviour for schools. The DBE together with the industry should adequately resource and support schools to implement cyber safety strategies. Educational laws should include guidelines for safe and emotional free environment for learners. The DBE should provide assistance in determining appropriate measures to be taken when any ICT is misused.

- The South African Police Service (SAPS)

If there is evidence of a crime and has been captured on a cell phone or other electronic device, the device should be confiscated and kept securely until handed to the investigating police officer. Criminal charges should then be laid, and the police should do the necessary investigations, in order to get hold of the necessary evidence.

- Children’s Rights Centre

If a threat is a suspected child protection issue, then a violence or suicide risk assessment should be done in accordance with DBE process. The Child Protection and Abuse Organisation should be contacted for help. It should be mandatory for educators to notify the Child Abuse or Child Protection Unit if they suspect child abuse and neglect. These organisations should educate the government about areas of specific concern for learners in cyber space (The Right Times 2012).

- Responsibilities of Educational Organizations

Educational Organizations should continue to hold workshops, do research and give presentations on cyber safety topics in order to help school communities. On the 19 August 2011, the Centre for Justice and Crime Prevention (CJCP) hosted a roundtable discussion about the nature of cyber violence in South Africa and the legislative and policy framework available pertaining to cyber threats (Centre for Justice and Crime Prevention 2011). The presentations were from the Nelson Mandela Metropolitan University (NMMU, University of Cape and Films and Publication Board (FPB). Based on FPB’s research results, it was found that there are no structures in place for parents and guardians to refer to when a case of cyber threats emerges. It was evident that the cyber aggression scourge in South Africa needs to be controlled. CJCP delineated that responses to cyber threat aggressors, are fragmented and rely on the various sections in the legislation, including common law definition of crimes and civil law.

- Attorneys and the Media

The attorneys can be of assistance in terms of pending civil action that could be taken against the aggressors. They should be able to provide a parent with sound legal advice on how to open a possible criminal case and how to get restraining orders against the accused (Cellphone Safety 2011). Exposing an aggressor in the media, should never be a first resort because a victim would be horrified at the thought of a parent going public about him being threatened and the shame that goes with it. It can however be a valuable weapon if no other options are available to parents (Cellphone Safety 2011).

6.2. Section 2 - A Proposed Incident Handling Structure

Role players need a procedure to refer to when handling cyber threat incidents. The focus of this section is to explore ways to intervene in cyber threat cases in schools after they have occurred. The article is proposing an incident handling procedure which will assist learners in reporting incidents of cyber threats and help respective role players to handle these threats. Figure 2 outlines the decision making process that should be followed. An incident handling procedure explains each step which should be considered when helping learners. It is critical that the safety and welfare of learners are considered as paramount throughout the process.

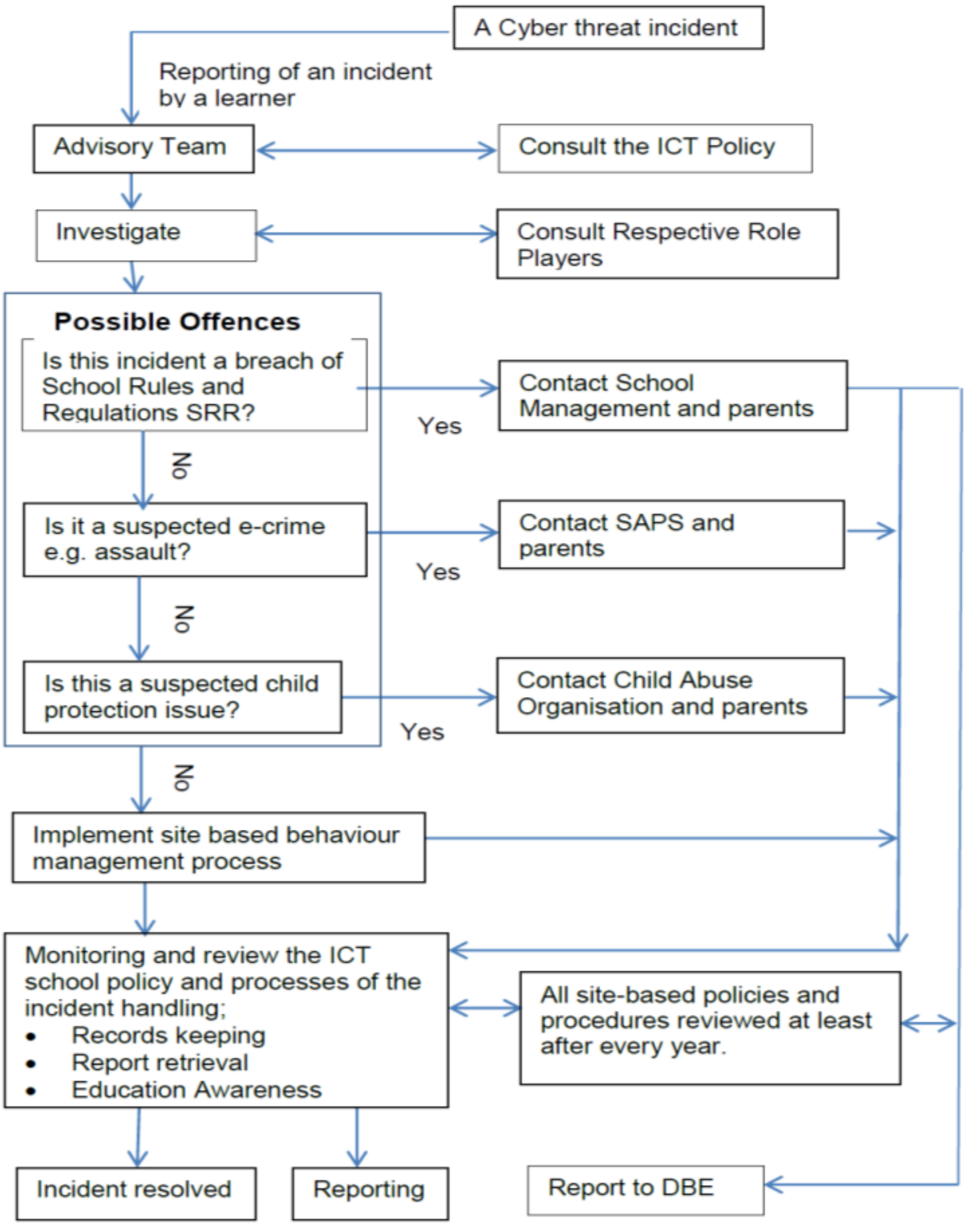
A Cyber threat incident
Reporting of an incident by a learner
Advisory Team
Consult the ICT Policy
Investigate
Consult Respective Role Players
Possible Offences
Is this incident a breach of School Rules and Regulations SRR?
Yes
Contact School Management and parents
No
Is it a suspected e-crime e.g. assault?
Yes
Contact SAPS and parents
No
Is this a suspected child protection issue?
Yes
Contact Child Abuse Organisation and parents
No
Implement site based behaviour management process
Monitoring and review the ICT school policy and processes of the incident handling;
Records keeping
Report retrieval
Education Awareness
All site-based policies and procedures reviewed at least after every year.
Incident resolved
Reporting
Report to DBE

Figure 2: A decision making process

6.2.1. Incident Handling Procedure

Advisory Team

This team can be composed of; the principal, a counsellor or psychologist, an ICT coordinator and a Life Orientation educator. 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. Optionally, if a school has a website, an online report feature on a school home page could also be considered with the provision of a Uniform Resource Locater (URL). In this case all members of the team should have the rights to override the URL filters in order to have access to records during their investigations. If a cyber threat appears to present a legitimate imminent threat of violence and danger to others learners or self then an Advisory Team should advise the School Management Board to contact law enforcement and initiate a protective response. It is also necessary for the Advisory Team to continue with the following evidence gathering steps.

Investigate

i. Gather Evidence and preserve it

All evidence gathered should be preserved. Parents, learners and staff should be advised to preserve evidence and a record of threats on computers or devices. Phone messages, record of instant message conversations, screen-grab of social network pages should be printed, saved and forwarded to the member of the Advisory Team.

ii. Determine the identity of the aggressor

The identity of the aggressor may be difficult to identify because aggressors can post their threats anonymously or impersonate someone. The advice of an ICT Coordinator could be of value in this circumstance. If there are any anonymous cyber threats or concerns of impersonation, and there be reasons to suspect that other learners could be involved, then a search of internet use records of learners should be conducted. If a criminal action is involved, law enforcement mechanisms have greater abilities to identify anonymous creators.

iii. Search for Additional harmful material or interactions

An ICT Coordinator and a librarian should assist. A search should include all suspected participants. A search of files and internet use records should be done, even if the threat appears to be an out of school activity. Conduct an additional search on the online environment where initial material appeared, and a search engine should be used to find out the name of a learner, friends, enemies, or the school name. Related activities at school should also be investigated.

iv. 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 previous threats or retaliation.

6.2.2. Possible Offences

After the investigation has been done an appropriate intervention should be considered based on the severity and history of the cyber threat incident and the learners involved. The rehabilitative measures could be considered as one of the first possible ways to help the learners involved. This may involve external role-players such as counsellors, health or social work professionals for specialised assistance. Parents or guardians should be invited to be part of measures to resolve the issue. Stated below are some of the offences which may be committed by cyber threat aggressors.

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

Determine the nature of the evidence 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 Board should impose formal discipline and get to the root of the problem. It should convene an independent tribunal to assess the case, and depending on its findings, determine appropriate sanctions. The School Management Board is responsible for recommending to the Provincial Head of Department to consider suspension or expulsion of a learner. Suspensions and expulsions should be avoided unless there are school safety concerns. More focus should be put on a restorative justice response. Fully documented evidence, decision making process, and rationale for formal discipline response should be produced and kept for future references.

ii. A Suspected E-Crime

In some instances a cyber threat crosses a line between a behavioural issue to be dealt with by school staff and parents to a criminal one that may involve the police. If the online material appears to present a legitimate imminent threat of violence and danger to others, contact law enforcement (SAPS) and a protective response should be initiated.

iii. Child Protection Issue

A violence or suicide risk assessment should be done by the member of the Advisory Team (the Life Orientation educator) to determine if the evidence gathered raises concerns that learner(s) may pose a risk of harm to others or self. 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 the Child Protection and Abuse Organisation should be contacted.

7. ICT Polices, Supervision, Monitoring and Review

Possible offences should be addressed in accordance to the ICT Policy document. Department of Basic Education (2010)'s Draft Guidelines on e-Safety states that the ICT policy should be developed and include a clear statement of actions which a school should take if a policy is breached. An ICT policy should be reviewed and updated regularly to ensure its appropriateness and effectiveness. Campbell (2005) believes that each school should adopt its own policy and guidelines that are tailored to its individual requirements and context. The school's ICT resources should be monitored and supervised to ensure that users are secure and in conformity with the school's ICT policy. The frequent change of technology requires that policies, procedures and agreements be updated and reviewed yearly. This change in technology is also a call for the introduction of Education Awareness Programs schools.

8. Education Awareness Programs

All school officials should be trained about cyber threats. Educators, coaches, after school supervisors and transport drivers, should be made aware of cyber threats and how to watch out for them. 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 could be used. Other awareness programmes should include teaching parents on how cyber threats can be prevented in the home and how they can respond to incidents. Offering conferences, information sessions and workshops about cyber threats could be another way to educate the older generation on current cyberspace practices so that they can begin to understand their children's cyber world.

9. Conclusion

The advantage of an incident handling procedure is that; 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. 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.

The cyber threat is a phenomenon that has been considered as a worldwide concern especially in first world countries. These online threats are becoming surprisingly prevalent across many different communities throughout the world. The United Nations (UN) child convention rights are part of the international legal framework which protects children and young people. They state that children and young people should be viewed and treated as human instead of passive objects of care and charity. The Government should undertake to ensure that such protection and care is necessary for their well-being (General Assembly 1989). With the increase of cyber threats in South African schools, the call to action against these threats is even more urgent. South African schools are putting a lot of effort into using ICT to support learners' learning. With this comes a responsibility to ensure that learning takes place in an environment where safe and responsible use of ICT is modelled and taught. The development of cyber threat incident handling procedure is a step ahead in trying to protect South African learners. This will ensure that learners are protected from emotional harm to the greatest degree possible. Empirical research should continue to be conducted in order to understand the cyber threat handling phenomenon in South African schools as well as evidence-based intervention programmes to control and combat cyber threats. The essential challenge is to have this procedure communicated to all stakeholders involved.

For future developments, the researcher will continue to explore ways of using a qualitative research method and research design to collect data from the role players with the intention of coming up with a cyber threat framework to help learners in cyber space. A qualitative phenomenological method will be intended to approach the role players in order to understand, describe and explain a cyber threat social phenomenon in South African schools. It will seek to unpack what role players are doing or what is happening to them in terms that are meaningful and offer rich insights (Gibbs 2007). Data collection will be done through group and individual interviews. This will be done to gain an in depth understanding into role players' perceptions of the nature, impact and successful intervention strategies for cyber threat incidents.

10. References

Alexander, W. & Harvey, J., 2012. Cyber bullying scourge. *Weekend Post*. Available at: http://myportelizabeth.co.za/cyber-bullying-scourge/ [Accessed September 12, 2013].

Badenhorst, C., 2011. Legal responses to cyber bullying and sexting in South Africa. *Centre for Justice and Crime Prevention*, (CJCP Issue paper No. 10). Available at: http://www.cjcp.org.za/articlesPDF/32/Issue Paper 10-1.pdf [Accessed September 8, 2013].

Bailey, C., 2012. Girl attacked after cyberbully ordeal: teen, 15, taunted on Facebook and BBM. *The Star*. Available at: http://www.genderlinks.org.za/article/girl-attacked-after-cyberbully-ordeal-teen-15-taunted-on-facebook-and-bbm-2012-02-29 [Accessed September 3, 2013].

Bhat, C.S., 2008. Cyber Bullying: Overview and Strategies for School Counsellors, Guidance Officers, and All School Personnel. *Australian Journal of Guidance and Counselling*, 18(1), pp.53–66. Available at: http://www.recoveryonpurpose.com/upload/Cyberbullying Overview and Strategies Australia.pdf [Accessed July 19, 2012].

Burton, P. & Mutongwizo, T., 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *CJCP*, 2012(March). Available at: http://www.cjcp.skinthecat.co.za/articlesPDF/30/Issue Paper 8 - Inescapable Violence - Cyber aggression.pdf [Accessed May 4, 2013].

Campbell, M., 2007. Cyber bullying and young people: Treatment principles not simplistic advice. *www.scientist-practitioner.com (paper of the week), 23 Feb.*, 2007(February). Available at: http://eprints.qut.edu.au/14903/1/14903.pdf [Accessed May 12, 2012].

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

Cellphone Safety, 2011. Cyber bullying 3 of 3: When all else fails. Available at: http://www.cellphonesafety.co.za/cyber-bullying-3-of-3-when-all-else-fails.html [Accessed March 24, 2012].

Centre for Justice and Crime Prevention, 2011. *Cyber bullying and "sexting" roundtable report*, Newlands, South Africa. Available at: http://cyberbullying.ezipezi.com/downloads/CJCPRoundtable-cyberbullying-report_19Aug2011.pdf.

Centre for Justice and Crime Prevention and the DoBE, 2013. School Safety Framework; Addressing Bullying in Schools - Course Reader.

Department of Basic Education, 2010. *Guidelines on e-Safety in Schools: Educating towards responsible, accountable and ethical use of ICT in education*, South Africa.

Department of Education and Children's Services, 2009. Cyber-Safety. Keeping Children Safe in a Connected World.A Guidelines for Schools and Preschools. South Australia. , 2011(July

15), pp.1–20. Available at: http://www.decd.sa.gov.au/docs/documents/1/CyberSafetyKeepingChildre.pdf [Accessed July 15, 2011].

Epstein, A. & Kazmierczak, J., 2007. Cyber bullying: What Teachers, Social Workers, and Administrators Should Know. *Illinois child welfare*, (3), pp.41–51.

Fisher, E.J., 2013. From Cyber Bullying to Cyber Coping: The Misuse of Mobile Technology and Social Media and Their Effects on People's Lives. *Business and Economic Research*, 3(2), p.127. Available at: http://www.macrothink.org/journal/index.php/ber/article/view/4176 [Accessed April 17, 2014].

General Assembly, 1989. Convention on the Rights of the Child. *General Assembly resolution*. Available at: http://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Gibbs, G., 2007. What is qualitative research? In U. Flick, ed. *Analyzing Qualitative Data*. London: SAGE Publications Ltd, pp. x – xi.

Gouws, F., 2014. The Changing Life World of the Adolescent: A Focus on Technological Advances. *J Communication*, 5(1), pp.9–16. Available at: http://www.krepublishers.com/02-Journals/JC/JC-05-0-000-14-Web/JC-05-1-000-14-Abst-PDF/JC-5-1-009-14-103-Gouws-F-E/JC-5-1-009-14-103-Gouws-F-E-Tx[2].pdf.

Herther, N.K., 2009. "Digital Natives and Immigrants: What Brain Research Tells Us" | Questia, Your Online Research Library. *Online*, 33(6), pp.14 – 21. Available at: http://www.questia.com/library/1P3-1895898431/digital-natives-and-immigrants-what-brain-research [Accessed June 3, 2014].

Jansen van Vuuren, J., Grobler, M. & Zaaiman, J., 2012. The influence of cyber security levels of South African citizens on national security. In Academic Conferences Limited, p. 138. Available at: http://researchspace.csir.co.za/dspace/bitstream/10204/5832/1/Grobler_2012.pdf [Accessed November 19, 2013].

Kganyago, K., 2012. Information Security Discussion by Microsoft South Africa's Chief Security Advisor. Available at: kganyago.org/tag/cybersecurity [Accessed December 12, 1BC].

Kite, S.L., Gable, R.K. & Filippelli, L.P., 2013. Cyber threats: a study of what middle and high school student know about threatening behaviours and internet safety. *International Journal of Social Media and Interactive Learning Environments*, 1(3), pp.240 – 254. Available at: http://www.jwu.edu/uploadedFiles/Providence_Campus/News_and_Events/Employee_News/Inside_Providence/KiteGableCyberThreats.pdf [Accessed April 19, 2014].

Li, Q., 2008. Cyberbullying in schools: An examination of preservice teachers' perception. *Canadian Journal of Learning and Technology*, 34(2), pp.75–90.

Lodge, J. & Frydenberg, E., 2007. Cyber-bullying in Australian schools: Profiles of adolescent coping and insights for school practitioners. *The Australian Educational and Developmental Psychologist*, 24(1), pp.45–58.

Mawdsley, Ralph D, Smit, Marius H, & Wolhuter & Charl, 2013. Students, websites, and freedom of expression in the United States and South Africa. *De Jure*, 46(1), pp.132–161. Available at: http://www.scielo.org.za/scielo.php?pid=S2225-71602013000100009&script=sci_arttext&tlng=en.

Minister of State Security, 2012. Statement on the Approval by Cabinet of the Cyber Security Policy Framework for South Africa. Available at: www.info.gov.za/speech/DynamicAction?pageid=461&tid=59794 [Accessed March 8, 2014].

Mogotlane, S.M., Chauke, M.E. & van Rensburg, G.H., 2010. A situational analysis of child-headed households in South Africa. *Curationis*, 33(3), pp.24–32. Available at: http://www.curationis.org.za/index.php/curationis/article/viewFile/4/7 [Accessed May 10, 2014].

Mudhovozi, P., 2013. Bullies and victims at a public secondary school: The educators' perspective. *Presentations*. Available at: http://proz.ontodo.org/presentations/196239/index.html [Accessed May 21, 2014].

Neille, D., 2013a. Hyde Park High sex pest case reveals more sexual assaults. *ENCA.Com*. Available at: http://www.enca.com/south-africa/hyde-park-high-sex-pest-case-reveals-more-sexual-assaults [Accessed June 12, 2014].

Neille, D., 2013b. Voyeurism fuelling school violence. *ecna.com*. Available at: http://www.enca.com/south-africa/voyeurism-fuelling-school-violence-analyst [Accessed June 12, 2014].

Oosterwyk, G. & Kyobe, M., 2013. Mobile Bullying in South Africa - Exploring its Nature, Influencing Factors and Implications. In *Proceedings of the European Conference on Informations Warfare*. p. 201. Available at: http://connection.ebscohost.com/c/articles/88849609/mobile-bullying-south-africa-exploring-nature-influencing-factors-implications [Accessed April 19, 2014].

Oosterwyk, G. & Parker, M., 2010. Investigating bullying via the mobile web in Cape Town schools. In A. Koch & P. Van Brakel, eds. *12th ANNUAL CONFERENCE ON WORLD WIDE WEB APPLICATIONS*. Durban, South Africa: ZA WWW 2010. Available at: http://www.zaw3.co.za.

Popovac, M. & Leoschut, L., 2012. Cyber bullying in South Africa: Impact and responses. *Centre for Justice and Crime Prevention*, (CJCP Issue Paper No. 13). Available at: http://cjcp.skinthecat.co.za/articlesPDF/63/IssuePaper13-Cyberbullying-SA-Impact_Responses.pdf [Accessed August 4, 2013].

Prensky, M., 2001. Digital Natives, Digital Immigrants. *On the Horizon*, 9(5), pp.1–6. Available at: http://www.marcprensky.com/writing/Prensky - Digital Natives, Digital Immigrants - Part1.pdf [Accessed June 3, 2014].

Pruitt-Mentle, D., 2000. C3 Framework Cyberethics, Cybersafety and Cybersecurity Promoting Responsible Use. Educational Technology Policy, Research and Outreach. , 2010(March 13). Available at: http://www.edtechpolicy.org/cyberk12/Documents/C3Awareness/C3_framework_full_final.pdf .

Steeves, V. & Wing, C., 2005. Young Canadians in a Wired World, Media Awareness Network. *Industry Canada's SchoolNet program and CANARIE*. Available at: http://www.media-awareness.ca/english/research/YCWW/phaseII/.

The Alannah and Madeline Foundation, 2007. The Alannah and Madeline Foundation, in consultation with the National Coalition Against Bullying and Center for Strategic Education. In *Cyber-Safety Symposium Report*. Canterbury, Melbourne.

The Right Times, 2012. The National Cyber Security Policy Framework for South Africa. , 2012(May 21). Available at: http://childrensrights.org.za/magazine/index.php//the-national-cyber-security-policy-framework-for-south-africa [Accessed September 4, 2013].

Tokunaga, R.S., 2010. Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), pp.277–287. Available at: http://www.sciencedirect.com/science/article/pii/S074756320900185X [Accessed March 19, 2014].

Willard, N., 2006. *An Educator ' s Guide to Cyberbullying and Cyberthreats : Responding to the Challenge of Online Social Aggression , Threats , and Distress*, Available at: http://miketullylaw.com/library/cbcteducator.pdf [Accessed March 21, 2011].