Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 5, 23-31 (2021)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Cyber Incident Handling and the Perceptions of Learners on Cyber Incidents in South African Schools

Naume Sonhera[*,1], Elmarie Kritzinger[2], Marianne Loock[2]

[1]*Information and Communication Technology, Vaal University of Technology, Vanderbijlpark, 1911, South Africa*

[2]*School of computing, College of Science, Engineering & Technology, University of South Africa, Florida, 1709, South Africa*

ARTICLE INFO

Article history:
Received: 21 April, 2021
Accepted: 27 August, 2021
Online: 10 September, 2021

Keywords:
Aggressor
Cyber Incident
Learner
Role Player
Schools
South Africa

ABSTRACT

With increases in technological usage, cyber incidents are also on the rise and have become a major concern in schools across the globe. What is of significant concern is that cyber incidents in South African schools are also on the rise. Existing evidence suggests that, in South Africa there are no clear procedures that are consistently followed by schools on how to report cyber incidents. The aim of this research is therefore to propose cyber incident handling procedures to enhance the effectiveness in handling cyber incidents as well as ensuring that each role player has an important contribution in the intervention process that is designed to reduce cyber incidents in South African schools. The study also assessed the perception of learners on cyber incidents in South Africa. Using the literature review approach and thematic analysis of the data collected from learners the study highlighted the procedures and roles of role players that can assist in cyber incident handling in South African schools. The study also came up with a detailed analysis of the views of learners on cyber incidents in South Africa. The results presented can help to provide a framework that will act as a guide on reporting cyber incidents and directing school management, and all within the school, towards appropriate reporting procedures and intervention processes. The study also found out that the rise in cyber incidents in South African schools, if left unaddressed, can have a devastating effect on learners. Therefore, the government of South Africa, through the Department of Basic Education, must prioritize the handling of cyber incidents in schools as cyber incidents are now a threat to the efficient and effective execution of the mandate of the department.

1. Introduction

The 21st century came with changes in almost all the sectors of the world economies. In the education sector, both the academics and practitioners of the 21st century have applauded the paradigm shift in schools of encouraging learners to be computer literate [1-4]. The technological paradigm shift has been complemented by the efforts of schools through promoting access to technology in education [5-6]. The socialization patterns among learners have also changed drastically because of the growth and proliferation of electronic communication devices. Learners access social network sites to communicate with their friends at any time of the day or night [7]. However, access to new technology has led to an increase in misuse and abuse of technology by learners and this has brought about incidents of threatening, harassing, embarrassing, and humiliating behaviour and actions online [8]. Cyber incidents have consequently become prevalent in schools worldwide, and it is evident that they present certain unique problems for schools in the regulation thereof [9-12]. What is of significant concern is the fact that cyber incidents in South African schools are also on the rise [13].

South African schools are adopting Information and Communication Technologies (ICTs) as part of an educational and social approach to prepare learners for the future. However, there is a lack of supporting cyber incident handling procedures to empower schools to deal with cyber incidents [14]. Cyber incidents are increasing among learners and yet there is very little guidance for schools on how to deal with cyber incidents [15]. With the potential for cyber incidents and their negative effects, schools have the responsibility to intervene in the occurrences [16]. Cyber incidents do not have an impact only on the physical and mental health of learners but also on the academic performance which in turn influences learners' learning outcomes negatively.

[*]Corresponding Author: Naume Sonhera, Email: nqume@vut.ac.za

Therefore, there is a need to ensure that schools are provided with cyber incident handling procedures that can contribute to a safe and caring environment for learners and all involved role players. Far from being limited to cyber victims, the effects of cyber incidents extend to the learners collectively, the school environment, and the entire school system [17]. To address the elements of cyber incidents in South African schools and to narrow the focus of this research to an educational environment, a cyber incident has been defined as: An act that violates explicit or implied cyber safety, computer safety or acceptable use of ICTs policies of South African schools or the Department of Basic Education (DBE) [18]. It is an event that involves the intentional or negligent use of digital platforms or electronic media to cause harm to other learners/self, or to impact on their confidentiality and integrity.

Some studies were done to try and understand the critical issue of cyber safety. In [14], the author investigated the maturity levels of cyber safety in South African schools. The study was intended to assess whether schools are prepared to help learners and educators to come up with cyber safety culture within the school environment. The study involved 24 schools in South Africa, and the investigation was through a critical evaluation of the elements that are important in improving cyber safety in schools. The elements in [14] which were evaluated include leadership and policies, infrastructure, education and standards, and inspection. After measuring cyber safety successfully using one of the UK approved measurement tool, the 360safe tool, the study discovered that all the schools had low levels of cyber safety maturity and compliance. In [14], the author further discovered that there is a clear lack of cyber safety awareness policies, practices, and procedures in the schools in South Africa. The study went on to propose a step-by-step cyber safety plan to empower schools to create their own cyber safety culture.

In [19], the authors stated that cyber safety is one of the critical aspects in the world today. Their study highlighted that learners require education on how to operate safely in cyber space and to protect themselves. In [19], the authors developed a cyber safety curriculum through open educational resources. The authors believed that this curriculum can empower educators in schools when educating learners about cyber safety. In [20], the author argued that business schools can meet the multidisciplinary needs of training cyber safety professionals. Motivated by these findings the study aims at proposing cyber incident handling procedures to enhance the effectiveness in handling cyber incidents as well as ensuring that each role player has an important contribution in the intervention process that is designed to reduce cyber incidents in South African schools. The study also assesses the views of learners on cyber incidents in schools.

2. The Education Sector in South Africa

The education sector in South Africa is divided into two departments, the Department of Basic Education (DBE) and the Department of Higher Education and Training (DHET) [21-22]. The DBE is responsible for primary and secondary education while the DHET is responsible directly for tertiary education and vocational training [23]. These two departments were once represented as a single department of education before 2009, then there was a split. The DBE looks after the public schools, the private schools, Early Childhood Development centres (ECD) and the special needs schools. Private schools are also known as independent schools and these private schools and public schools are known collectively as the ordinary schools [22]. On the other hand, the DHET deals with tertiary education where we have further education and training, popularly known as the Technical and Vocational Education Training colleges (TVET) [21]. The DHET is also responsible for Adult Basic Education and Training (ABET) Centres and Higher Education Institutions (HEI) [24]. In South Africa, each province has its education department which is responsible for the implementation of policies of the national department. These departments are also there to deal with local issues that are related to the execution of the mandate of the department at national level.

As of 2016, the DHE reported that there were 29 749 public and registered independent schools in South Africa [23]. The number of ordinary schools was 25 574 while 4 175 were other educational institutions such as special schools and Early Childhood Development (ECD) centres. The DBE also reported that the total number of educators were 425 000 in 2012 and 440 151 in 2016 who were reporting to the national department and the provincial department in the 9 provinces and the 86 districts of South Africa [22]. District and provincial DBE offices in nine provinces and 86 districts administer all the schools and have considerable influence over the implementation of policy. The goals of the DBE and its district and provincial offices are to improve the quality of teaching, undertake regular assessments, and improve on the Early Childhood Development, to ensure a system of outcomes-focused accountability [23].

3. Literature Review

Schools worldwide are being charged to take action to reduce cyber incidents because of the potential of cyber incidents disrupting the educational processes, creating a hostile environment, and threatening learners' feelings of safety and mental well-being [8, 12, 25]. Due to the increase of cyber incidents that cross over into both home and school environments, coupled with confusion as to who should issue consequences and how, role players must work together to create effective cyber aggression strategies [16]. The intervention during cyber incidents takes group effort from all role players and learners themselves. While it may take a village to raise a child, the virtual village inclusive of social media platforms, Internet Service Providers, phone companies, non-profit youth organisations, non-governmental organizations, educational institutions, parents or guardians, attorneys, and media need to join forces to have dialogue nationally and globally on ways to protect learners from cyber incidents [26].

The 21st century has brought with it a different revolution - learners who are on the cutting edge of technological proficiency [7]. While awareness of the use of the Internet is growing among learners in South African schools, there is no increase in awareness of safe practices in the use of ICTs [27]. Learners receive mixed messages with regard to online behaviour as they strive for technology literacy, sometimes without appropriate support [28]. Learners seem unaware of the risks of inappropriate behaviour online, viewing them as trivial. Cyber incidents are causing major challenges for school officials who are called upon to respond to

cyber incidents involving learners [29]. Online threats take place off the radar screen of educators and parents; this makes it difficult to detect cyber incidents in schools and more impossible to monitor off school premises [10]. The language that the learners use on the Internet has evolved and created a generation gap between learners and adults around them. This gap enables learners to participate in cyber incidents without fear of being discovered by adults [15, 30].

There are no clear procedures that are followed consistently by South African schools, governing boards, and educators on how to report or handle cyber incidents [10, 31]. At present, the principals, educators, and parents are not sure what procedures to follow when learners are being harassed online [32-33]. Research in South Africa (SA) that examines the procedures for schools on how to report cyber incidents are limited [10]. The lack of clear procedures for reporting cyber incidents in schools, makes educators feel unsupported. Educators will rather ignore these unethical violations than follow ill-defined and unenforceable policies [34]. In [34], the authors investigated the reason learners should be educated about risks in cyber space and the ways in which the schools can intervene to assist. The study discovered that despite the usefulness of the Internet there are still negative issues that are related directly to the Internet use. Users of the Internet across the world are being subjected to various forms of abuse such as cyber incidents, cyber bullying, online fraud, racial abuse, pornography, and gambling. In [34], the authors believe that issues related to cyber incidents are on the rise, especially among learners, because of a lack of anti-cyber incident awareness. The other argument put forward by them was that the level of awareness among the Internet users is low or moderate. As a result, in [34], the authors stated that it is important that the anti-cyber incidents awareness be cultivated among learners through various initiatives like education so that learners are able to operate safely in cyber space.

In another study, in [35], the authors verified the effectiveness of gamification in reducing cyber incidents and offer a constructive application of a framework that can help to improve cyber safety skills and capabilities for learners in schools. The study also discovered that the rise in cyber incidents shows that the traditional methodologies used to train and bring awareness are insufficient to build the necessary cyber safety skills and capabilities. The study also discovered that gamification can be a promising methodology that can bring some changes to the behaviour of learners in cyber space at early stages. In [35], the authors came up with a proposal for a cyber hero framework for information security awareness and training programs that can fight human error in cyber space. In [35], the authors discovered massive progress in the skills and capabilities of cyber safety for learners using the cyber hero framework.

In [36], the authors discussed the applicability of the safety standards and frameworks used in various industries to avoid threats of cyber incidents due to the rise in the use of technology in schools. In [36], the authors discovered that it is very critical to have strong cyber safety controls in schools due to the growth in cyber incidents. The other notable finding in [36] was that it is very important to have a cyber safety framework that accommodates safety standards and frameworks in an education environment. In [15], the authors investigated the perceptions of cyberbullying among student teachers in South African schools, in Eastern Cape. In [15], the authors found out that in South Africa cyber incidents are some of the issues affecting learners. The study went on to discover that the Department of Basic Education in South Africa is providing little guidance for schools on issues related to cyber incidents. Using a quantitative survey approach, the study discovered that cyber incidents are some of the critical issues in South African schools, but the topic has not been incorporated in the policy or even in the curriculum. In [15], the authors recommended that the Department of Basic Education should come up with a standardised policy that can be used to implement and enforce cyber safety behaviour in schools.

In [37], the authors did an investigation to assess the policies, procedures and measures which schools need to have in place to ensure that there is cyber safety awareness for learners in South African schools. They discovered that Information Communication Technology is now becoming part of the daily lives of learners, opening various opportunities and cyber risks as well. Therefore, just like in [15], [37], the authors believe that it is important for cyber users to become aware of the cyber safety issues so that they are able to protect themselves. It was also highlighted that in South Africa, cyber safety awareness and cyber education is still lacking, especially in schools. In [37], the authors also believe that it is of utmost importance for South Africa to begin the creation and implementation of cyber safety and cyber incident awareness policies, procedures, measures, and initiatives for the education sector, especially for schools and learners.

4. Research Methodology and Design

The research methodology is explaining how the literature review was done and how data was collected from learners to get their experiences and perceptions on cyber incidents. This research consists of two research methods. The first one is the literature review. The researcher conducted a systematic search on literature that reported the prevalence and impact of cyber incidents among learners in South African schools and the extent to which role players responded to cyber incidents in schools. The main idea behind the reviews was to identify the roles and responsibilities of role players in cyber incident handling for the Schools in South Africa. The systematic process included the electronic search in databases, title and abstract review and hand searches in Google scholar and article reference lists. Online databases contained bibliographic references to academic and peer-reviewed journal articles, as well as references to theses, books, and chapters. Secondly, the research used a qualitative approach and purposive sampling to collect data from the learners to get their experiences and perceptions on cyber incidents [38-40]. The rationale for selecting learners was based on reviews in [41-44], with the authors who indicated that adolescence is a peak period for involvement in cyber incidents. A total of 85 learners participated in three focus groups that ranged in size: group one had twenty participants, group two had thirty participants and group three had thirty-five participants as shown in the table1.

Forty-eight percent were male, and fifty-two percent were female. The interview questions enabled learners to explain their perspectives in depth. The questions were related to the themes that emerged from each group. All the conversations were recorded and transcribed. The data was then coded using ATLAS.ti. 7; themes

emerged, and the frequencies of these themes were noted by the researcher. Several ethical guidelines were followed to ensure that the research study was conducted ethically. In an endeavor to ensure the reliability and validity of data, the verbatim transcribed interviews were presented to the respondents to verify and sign off. The researcher reviewed all the transcripts from focus group interviews to check for accuracy, ensuring that no obvious mistakes appeared. The researcher also ensured that there was no drift in the definition of codes or shift in the meaning of codes during the coding process.

Table 1: Participants in the Three Focus Groups.

Focus Groups	Participates in the Groups
Group 1	20
Group 2	30
Group 3	35
Total	85

Source: Author's Analysis

Table 1 above shows the number of students who participated in each focus group.

5. Discussion of the Roles and Responsibilities of Role Players in Cyber Incident handling for the Schools in South Africa

The study came up with a theoretical framework that outlines the roles and responsibilities of role players in addressing the cyber incident handling needs. The responsibilities of role players within schools and relevant role players outside schools for specific and specialized interventions and support were identified during the literature review. To elaborate on the "Needs for Addressing Cyber Incidents", each need is linked to role players and recommended responsibilities. The aim of the theoretical framework and the roles of role players for schools in South Africa is to ensure that relevant role players are drawn in to create a supportive structure that can contribute to the development of the cyber incident handling procedures. To achieve this, the researcher highlighted the roles and responsibilities of role players within and outside the school when responding to cyber incidents. The framework is designed to complement normal schooling duties and activities and to integrate cyber school safety into the daily activities of the school. The framework also gives a guide on how relevant role players can assist in responding to cyber incidents. The framework may not make provision for all cyber incidents in schools or cyber safety concerns for schools but is a starting point to address cyber incidents in South African schools. The linking of "needs for addressing cyber incident" to "the role players" assisted the researcher to present the complex ideas and the theoretical concepts, from the literature review to a new structure which will assist in developing reporting procedures [41]. Table 2 is outlining the roles and responsibilities of role players in cyber handling in South Africa as discovered from the reviewed literature.

Table 2: Summary of the Roles and Responsibilities of Role Players in Cyber handling in South Africa as discovered from the Reviewed Literature.

Role Players	Responsibilities
School Principals, Learners, Parents, Guardians, school staff members, and School Governing Body	Role players should be competent in handling cyber incidents.
	All role players should be informed of the cyber incident reporting procedures.
	School procedures should be readily accessible to learners, parents, guardians, and school staff members.
	Need clear and easily understandable school procedures to address cyber incidents.
	Consistent, universal, and effective ICT policy aimed directly at regulating cyber incidents in schools, should be developed.
	Codes of conduct or code of behaviour should be formulated and adopted.
	Need a referral system to appropriate services and community partnerships to support learners and build a cyber school safe environment.

Source: Author's Analysis

Full explanation of the roles and responsibilities of role players in cyber incident handling in South Africa as discovered from the reviewed literature is given in the following section.

5.1. Role Players should be Competent in Handling Cyber Incidents.

The principal should ensure that school personnel and parents are trained in handling cyber incidents. The advisory Team should implement an effective approach in intervening and responding to all cyber incidents. Educators should participate in school cyber safety trainings. Educators should be aware of the steps to take and advice to give if learners notify them of cyber incidents. Parents should report their children's cyber aggression. This was in line with the findings that were discovered in [15] and [37], the authors discovered that it is important for cyber users to become aware of the cyber safety issues so that they will be able to protect themselves from the various forms of cyber incidents. It was also highlighted that in South Africa, cyber safety awareness and cyber education is still lacking, especially in the education sector [15]. In [36], the authors argued that it is very important to have a cyber safety framework that accommodates safety standards and frameworks in an educational environment.

"All Role Players should be informed of the Cyber Incident Reporting Procedures"

The school community should know who to approach if they become aware of or suspect any cyber incident taking place. The advisory team should establish a process that communicates the cyber incident, reporting procedures to all parents, learners, and all staff members. The School Management Board (SMB), School Governing Body (SGB) and Counsellors should explain the cyber incident reporting procedures to learners and their parents or

guardians. Educators should establish consultation and training for parents and other staff members on cyber incident reporting procedures. Social Media Service Providers (SMSP) should make their educational and safety materials easy to find and promote the materials to users regularly. Social Media Service Providers should improve the visibility, consistency, and accessibility of reporting tools on their platforms. Several studies support this. In [15] and [31], the authors pointed out that in South Africa there are no clear procedures that are followed consistently by schools, governing boards, and educators, on how to report or handle cyber incidents. The authors believe that it is very important for role players to be aware of the reporting procedures because at the moment, the principals, educators, and parents are not sure of what procedures to follow when learners are being harassed online [10, 32]. In [35], the authors emphasized that role players should be informed of the cyber incident reporting procedures especially if these frameworks are to be usable.

5.2. School Procedures should be readily Accessible to Learners, Parents, Guardians, and School Staff Members.

Provincial education departments must ensure that all schools are trained about procedures to address cyber incidents. The principal, Information Technology (IT) Unit, SGB, SMB and the Advisory Team should develop, support, and evaluate procedures to address cyber incidents. Officials from the National Department of Education, in collaboration with provincial, regional and district officials responsible for ICT school safety, should monitor the implementation of procedures to ensure that learners are safe from cyber incidents. Educators should assist in the development and implementation of anti-cyber incident procedures according to delegated roles and responsibilities. This has been supported in [37] by the authors who argued that for South Africa to have meaningful progress towards addressing cyber incidents in schools, the departments of education must be equipped with the appropriate policies, procedures, and measures to ensure that there is cyber safety awareness for leaners in South African schools. In [37], the authors discovered that Information Communication Technology is now becoming part of the daily lives of learners, with various cyber opportunities and cyber risks as well, hence the need for proper policies, education, and training for those responsible for cybersecurity.

5.3. Need Clear and Easily Understandable school procedures to address cyber incidents.

The other important aspect is that procedures outlining the school response to cyber incidents and how to report cyber incidents, should be in place and these procedures should be easily understandable. Provincial Departments of Education should ensure that school cyber incident reporting procedures are in place and should be adhered to strictly in schools. School cyber incident reports must be submitted to the district after which reports must be consolidated and forwarded to the Provincial School Cyber Safety Coordinator. A consolidated report from provinces must be submitted every quarter to the national Department of Basic Education (DBE). This was also supported in [14], [15], and [37] by the authors who agreed with many other scholars. These authors believe that it is important for learners to be aware of the cyber safety issues and the cyber incident reporting procedures so that they can get help whenever they need it. It was also highlighted that in South Africa, cyber safety awareness and cyber incident handling education is still lacking, especially in schools [14, 15, 37]. Scholars also believe that it is of utmost importance for South Africa to begin the creation and implementation of cyber safety and anti-cyber incident awareness policies, procedures, measures, and initiatives for the education sector, schools and learners in the country [14, 15, 37].

5.4. Consistent, Universal, and Effective ICT Policy aimed at Regulating Cyber Aggression directly in schools, should be developed.

The other critical aspect is that the Department of Basic Education should take a lead to ensure that ICT policies for provinces have been developed. Provincial officials must provide direction to their regional or district counterparts to ensure that the development, enforcing and reviewing of ICT policies is being implemented in schools. Public policy should also be informed by ongoing research on the prevalence of cyber incidents. A school ICT policy that includes an ICT Acceptable Use Policy (AUP), ethical use of ICTs or digital technologies and anti-cyber incidents should be developed, implemented, and enforced. All role players should be aware of the contents of these policies. The principal, IT Unit, SGB, SMB and the Advisory Team should ensure that they have an appropriate ICT school policy in place to safeguard the overall cyber safety and wellbeing of learners. The IT Unit should manage the ICT policy through recording and monitoring Internet use for compliance with ICT policies. The SMB and the SGB should convene regular meetings to review and update the ICT Policy. Parents should ensure that their children adhere to the ICT policy.

5.5. Codes of Conduct or Code of Behaviour should be Formulated and Adopted.

The information gathered also reveals that the provincial education departments should ensure that all schools have a Cyber Safety Code of Conduct for learners. The principal, SGB, SMB and the Advisory Team should develop, support, and evaluate the Cyber Safety Codes of Conduct for learners. Learners should adhere to the Code of Conduct and to ensure appropriate behaviour always. All schools should be obliged to comply with Child Protection legislation, which includes Internet safety for learners. DBE needs to develop and integrate cyber safety programs into existing curricula to support human rights and child protection. The Child Protection and Abuse Organization should be contacted for help if a cyber incident is a suspected child protection issue.

5.6. Need a Referral System for appropriate Services and Community Partnerships to support Learners and build a Cyber School Safe Environment.

The South African Police Service (SAPS) should be obliged to investigate any unlawful cyber incident in schools. SAPS should advise and educate learners, parents, and school personnel about legal responses to serious cyber incidents. Law enforcement authorities must ensure that the all-role players have a clear awareness and understanding of how existing criminal offences can be applied to cyber aggression behaviour. Learners should contact SAPS in case of any cyber incident. Counsellors should give immediate support to all affected learners. Parents should

partner with schools to ensure that their children are following appropriate guidelines for online behaviour. Parents of the victims should be able to work with the Internet Service Provider, Cell Phone Service Provider, or Content Provider to investigate the cyber incident or to remove the offending material. Internet Service Providers should track instant messaging which could have been used as evidence in a court of law. SA Depression and Anxiety Group (SADAG) should assist learners suffering emotionally because of the cyber incident ordeal. Educational Organizations should continue to hold workshops, do research, and give presentations on cyber incidents and cyber safety topics to help the school communities. The attorneys should be able to provide parents with sound legal advice on how to open a possible criminal case and how to get restraining orders against the accused.

5.7. Findings of the Focus Group Interview

The interviews revealed learners' perspectives about cyber incidents and were specific to cyber incidents as they manifested within the schools. The results indicated the negative cyber incident effects on victims, the no or ineffective consequences for aggressors, and the inability to stop or control cyber incidents once they have started. The themes which emerged are Learners' Perceptions about Victims, Aggressors and Bystanders; Learners' Perceptions about Technology; Learners' Perceptions about Cyber Incidents, and Learners' Perceptions about Adults. A collection of the conceptual valid and reliable evidence contributed to a better understanding of learners' interactions in cyber space and how much help they need when they are in trouble. The results of the focus group interview also showed that learners are acutely aware of cyber incidents occurring in their schools and how they are reluctant to report the experiences of cyber incidents when they occur. The researcher recognized that cyber aggression, especially if left unaddressed, can have a devastating effect on learners; it can create a barrier to learning and have serious consequences for mental wellbeing. The views of learners are summarized in the table below.

Table 3: The Findings from the Focus Groups on the Views of Learners about Cyber Incidents

Findings From Focus Groups	**Description**
	Learners' Perceptions about Victims, Aggressors and Bystander
	Learners' Perceptions about Technology
	Learners' Perceptions about Cyber incidents
	Learners' Perceptions about Adults

Source: Author's Analysis

The table above is summarizing the views of learners on issues related to cyber incidents and the full description of these views is given below.

5.8. Learners' Perceptions about Victims, Aggressors and Bystanders

The themes generated from the focus group interviews were linked to the suggestions from learners and from the literature reviewed. Pillars for reporting procedures were derived from the whole integration process. Themes from Learners' Focus Group Interviews indicated the Challenges for Victims, Aggressors' Behaviour, and Learners' Perceptions about Bystanders Supporting Aggressors. The results revealed that the challenges for cyber victims are that cyber victims are humiliated and harassed online. Also, learners were of the view that victims fear aggressors and are affected psychologically which will lead them to suffer in silence. On the behaviour of aggressors, the results revealed that aggressors gain power by controlling victims and most of them are mean; they seek attention, are insecure, and they take out their pain or anger on other learners. The results also revealed that technology allows the aggressors to hide behind screens and in many circumstances, they are perceived as mentally unstable. The study went on to check the learner's perception about bystanders supporting aggressors. The study found out that usually bystanders are afraid to become the next victims and to suffer rejection by peers and sometimes uncertainty about whom to tell.

In summary, the results pointed to the fact that cyber victims feel like outcasts, are hurt, offended, embarrassed and feel inferior. These victims fear aggressors because aggressors take out their pain or anger on other learners. The results also pointed out that bystanders support aggressors because of fear of becoming the next victims, being rejected by peers or uncertain of whom to report to. The identified pillars for reporting procedures derived from the discussions are Legislation, Referral System, Cyber Incident Reporting Platform and Cyber Awareness. Learners suggested that all schools should be compelled to comply with Child Protection Legislation. There is a need for a referral system to appropriate services, and need for community partnerships to support learners. Learners should report cyber incidents to the principal or ICT personnel, school staff members should provide support and counselling, school psychologists should help affected learners, school assemblies and public service announcements should be used for awareness. Learners need to be educated about cyber incident problems, there should be a hotline for reporting cyber incidents and finally there must be consequences for the aggressors.

5.9. Learners' Perceptions about Technology

Leaners are of the view that technology aggravates cyber incidents, and, in many ways, technology has decreased empathy among learners. The results indicated that aggressors use profiles of innocent people to threaten other learners. The anonymity online makes threatening behaviour more readily achievable and protects aggressors. The other aspect that was highlighted is that technology enables aggressors to have the biggest audience, making it difficult for those who want to champion anti-cyber incident awareness. Learners also indicated that due to technology some learners put themselves at risk by taking naked videos of themselves and these videos end up going viral on social media. In a nutshell, the results from the interviews have revealed that technology has decreased empathy for victims due to space differences, instant gratification and communication with the biggest audience. As a result, learners are of the view that schools need to have a clear ICT policy, procedures, and codes of conduct in place to regulate cyber incidents among learners. Parents and learners should be given the sets of ICTs rules so as to guide learners against cyber incidents. Learners are also of the view that

schools should introduce education against cyber incidents and independent service providers should assist to solve cyber incident problems, for example, the network companies should be able to identify phones that could have sent the harassing messages. It was also highlighted that learners should stop taking photos which could later be used against them, they should avoid instigating cyber incidents. Lastly, it was discovered that the ICT Policy, School Codes of Conduct, Identification of Aggressors and Anti-Cyber Aggression Awareness were the pillars contributing to the development of reporting procedures for cyber incidents in schools.

5.10. Learners' Perceptions about Cyber Incidents

The results indicated that cyber incidents among peers could be perceived as harmless or humorous and with no ways of stopping cyber incidents once they are viral. Learners are of the view that cyber incidents are not reported as often as they should. At times learners do not have the courage to talk about the incidents; in most cases victims are only willing to report to someone they feel comfortable with or someone they can trust. The other important observation is that in most cases it is not known how these issues are solved or what the outcomes are. Aggressors perpetrate incidents to seek revenge and sometimes a victim may become an aggressor due to revenge. The other way learners manage cyber incidents is physical fighting. The results also pointed out that to facilitate learner confidentiality and trust towards adults, learners must be able to report cyber incidents anonymously and their confidentiality must be respected. Learners' voices are essential, and their positive suggestions should be included in the design and implementation of the cyber incident handling procedures. However, without a confidential, voluntary, and anonymous reporting system, it is unlikely that learners will feel free to report cyber incidents. Learners fear being singled out; they fear that someone might retaliate against them. The results indicated that the Reporting System and Management of Cyber Incidents were the pillars for reporting procedures.

5.11. Learners' Perceptions about Adults

The study also assessed the leaner's perception about adults. The results indicated that in most cases learners are scared that adults will worsen the situation because of them being too judgmental about the behaviour of learners. Many parents are seen to always remind their children of the issues which they would have done wrong. Leaners also believe that adults do not have any role in the intervention of cyber incidents and are ineffective when they attempt to intervene. Leaners are also of the view that educators are not helping when it comes to cyber incidents to an extent that some learners are not comfortable telling them about their cyber incident problems. This is why some learners end up being absent from classes, avoiding being embarrassed. All these results point to the fact that there is no open and good relationship between learners and the adults around them. The results indicated that learners wish their parents could be more involved in their online lives from an early age. Most learners want parents to have a good relationship with them, to communicate with them, to spend more time with them, to support them and even to join them in cyber space. Learners believe that the most important issues that many parents are interested in are about schoolwork. As a result, many parents do not know what is happening in their children's daily lives. The other critical factor is the huge generation gap between children and their parents; there is a great difference between how children are being raised and how their parents were raised. As a result, this gives learners the idea that adults are not confident to help and intervene during cyber incidents. Some learners pointed out that it is not known how principals are handling cyber incident cases and the outcomes are not known. This is due to adults being absent from cyber space, which compromises their ability to assist. Leaners believe that the fact that most parents are not using social media, makes it very difficult for them to identify cyber aggressors.

In summary, learners indicated that they do not have confidence in adults, especially when it comes to their online problems. Role players need to be competent in handling cyber incidents and learners need to be assured of their safety when reporting cyber incidents, and their reports should be taken seriously and acted upon. All role players should be informed of the cyber incident reporting procedures and should be aware of how important it is to report cases as early as possible. The school community should know whom to approach if they become aware of or suspect any cyber incident taking place. Parents should check their children's phones if they notice any behaviour change. Parents should block the aggressor, notify their service provider, and report cyber incidents to the school and law enforcement. Parents should tell their children not to go about taking naked pictures of themselves and posting them online. All school role players should be educated about cyber incidents. Parents need to learn the legal issues associated with cyber aggression. Severe cyber incidents should be considered as crime. Law enforcement should have a specialised task team to deal with cyber incidents. SAPS should have a cyber division. The pillars for reporting procedures derived from the themes are Competence in Handling Cyber Incidents, Awareness of The Reporting Procedures, Learner Assistance from Parents, Cyber Aggression Awareness, Legislation, And Cyber Division for Law Enforcement.

6. Summary and Conclusion

Access to new technology in schools has led to an increase in misuse and abuse of technology by learners and this has led to a rise in cyber incidents related to threats, harassment, embarrassments and humiliating behaviour, and various bad activities online. The study, therefore, proposes that cyber incident handling procedures, and the roles and responsibilities of role players should be in place for cyber incidents to be addressed in South African schools. Using the literature review approach and thematic analysis of the data collected, the results indicated that it is important that role players should be competent in handling cyber incidents, and they should be informed of the cyber incident reporting procedures. The other important finding was that the cyber incident handling procedures should be readily accessible to learners, parents, guardians, and school staff members and they should be clear and easily understandable. The other issue that was highlighted was the need for a consistent, universal, and effective ICT policy directly aimed at regulating cyber incidents in schools. The codes of conduct or a code of behaviour should be formulated and adopted. The study also discovered that there should be a need for a referral system to appropriate services, and community partnerships to support learners and build a cyber school safe environment.

The study also come up with the views of learners on various aspects of cyber incidents in schools which include their perceptions on victims, aggressors and bystanders; learners' perceptions about technology; learners' perceptions about cyber incidents and learners' perceptions about adults. For instance, learners' perceptions on cyber victims, aggressors and bystanders were that cyber victims feel like outcasts, hurt, offended, embarrassed and inferior. These victims fear aggressors because aggressors take out their pain or anger on other learners. The results also pointed out that bystanders support aggressors because of fear of becoming the next victims, being rejected by peers or uncertain of whom to report to. The results presented helps to provide a framework that will act as a guide on reporting cyber incidents and directing school management, and all within the school, towards appropriate reporting procedures and intervention processes. The study also found out that the rise in cyber incidents in South Africa if they are left unattended, can have a devastating effect on learners. Therefore, the government of South Africa through the department of basic education must prioritize the handling of cyber incidents in schools as cyber incidents are now a threat to the efficient and effective execution of the mandate of the department.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] E. B. Meier, "Designing and using digital platforms for 21st century learning," Educational Technology Research and Development, **2021**(1), 1–4, 2021, doi.org/10.1007/s11423-020-09880-4.

[2] M. Finn-Stevenson, Schools of the 21st century: Linking child care and education, Routledge, 2018.

[3] S. McCoy and S. Lyons, Digital Technologies and Student Learning. Ireland's yearbook of education 2018-2019, Education Matters, 2018.

[4] J. Remón, V. Sebastián, E. Romero, and J. Arauzo, "Effect of using smartphones as clickers and tablets as digital whiteboards on students' engagement and learning.," Active Learning in Higher Education, **18**(2), 173–187, 2017, doi.org/10.1177/1469787417707618.

[5] L. K. Butola, "E-learning-A New Trend of Learning in 21st Century During Covid-19 Pandemic.," Indian Journal of Forensic Medicine & Toxicology, **15**(1), 422–426, 2021.

[6] J. Byrne, D. Kardefelt-Winther, S. Livingstone, and M. Stoilova, Global Kids Online Research Synthesis, 2015-2016, London, 2016.

[7] I. . Ogaji, P. Okoyeukwu, I. Wanjiku, E. A. Osiro, and D. Ogutu, "Pattern of use of social media networking by Pharmacy students of Kenyatta university, Nairobi, Kenya," Computers in Human Behavior, **100**(66), 211–216, 2017, doi.org/10.1016/j.chb.2016.09.035.

[8] Queensland Government, "Adjust our settings: A community approach to address cyberbullying among children and young people in Queensland," Queensland, 2018.

[9] J. D. Shapka, H. Z. Onditi, R. J. Collie, and N. Lapidot-Lefler, "Cyberbullying and cybervictimization within a cross-cultural context: A study of Canadian and Tanzanian adolescents.," Child Development, **89**(1), 89–99, 2018, doi.org/10.1111/cdev.12829.

[10] C. A. Hills, Developing a law and policy framework to regulate cyber bullying in South African schools, PhD Thesis, University of South Africa, 2017.

[11] J. M. Lee, J. S. Hong, J. Yoon, A. A. Perguero, and H. J. Seok, "Correlates of adolescent cyberbullying in South Korea in multiple contexts: A review of the literature and implications for research and school practice.," Deviant Behavior, **39**(3), 293–308, 2017, doi.org/10.1080/01639625.2016.1269568.

[12] D. Cross, T. Shaw, K. Hadwen, P. Cardoso, P. Slee, C. Roberts, L. Thomas, and A. Barnes, "Longitudinal impact of the cyber friendly schools program on adolescents' cyberbullying behavior," Aggressive Beviour, **42**(2), 166–180, 2016, doi.org/10.1002/ab.21609.

[13] P. Burton, L. Leoschut, and J. Phyfer, "South African Kids Online: A glimpse into children's internet use and online activities, Cape Town," http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf, Accessed: 17-Nov-2017.

[14] E. Kritzinger, "Improving cybersafety maturity of South African schools," Information, **11**(10), 471–488, 2020, doi.org/10.3390/info11100471.

[15] L. Cilliers and W. Chinyamurindi, "Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa.," Electronic Journal of Information Systems in Developing Countries, **86**(4), 1–10, 2020, doi.org/10.1002/isd2.12131.

[16] S. G. Denby, Cyberbullying: School Administrators' Perceptions of Law and Prevalence, and Roles in Prevention, Intervention, and Discpline., PhD Thesis, Virginia Commonwealth University, 2020, doi.org/10.25772/NQZM-FM42.

[17] M. Astatke, C. Weng, and S. Chen, "A literature review of the effects of social networking sites on secondary school students' academic achievement.," Interactive learning Environments, **2021**, 1–17, 2021.

[18] L. M. Hellsten, An Introduction to Cyberbullying, Macerata, 2017.

[19] R. Von Solms and S. Von Solms, "Cyber safety education in developing countries," Journal of Systemics, Cybermetics Informatics, **13**(2), 14–19, 2015.

[20] S. C. Yang, "A meta-model of cybersecurity curriculums: Assessing cybersecurity curricular frameworks for business schools.," Journal of Education for Business, **96**(2), 99–110, 2021, doi.org/10.1080/08832323.2020.1757594.

[21] D. Mhlanga, "Industry 4.0: The Challenges Associated with The Digital Transformation of Education in South Africa.," https://www.researchgate.net/publication/344230555_Industry_40_The_Challenges_Associated_with_The_Digital_Transformation_of_Education_in_South_Africa, Accessed: 02-Aug-2021.

[22] South African Market Access, "Education Statistics - South African Market Insights," https://www.southafricanmi.com/education-statistics.html, Accessed: 02-Aug-2021.

[23] Department of Basic Education, Education Statistics in South Africa 2016. Department of Basic Education, 2018.

[24] D. Mhlanga and T. Moloi, "COVID-19 and the Digital Transformation of Education: What are we learning on 4IR in South Africa?," Educatin Sciences, **10**(7), 180, 2020, doi.org/10.3390/educsci10070180.

[25] A. DeSmet, N. Aelterman, S. Bastiaensens, K. Van Cleemput, K. Poels, H. Vandebosch, G. Cardon, and I. De Bourdeaudhuij, "Secondary school educators' perceptions and practices in handling cyberbullying among adolescents : a cluster analysis," Computers and Education, **88**, 192–201, 2015, doi.org/10.1016/j.compedu.2015.05.006.

[26] J. L. Tinstman Jones, L. O. Campbell, J. Stickl Haugen, and C. C. Sutter, "Cyberbullying considerations for school counselors: A social media content analysis," Professional School Counseling, **23**(1), 2020, doi.org/10.1177/2156759X20919365.

[27] C. A. Myers and H. Cowie, "Cyberbullying across the lifespan of education: Issues and interventions from school to university," International Journal of Environmental Research and Public Health, **16**(7), 1–14, 2019, doi.org/10.3390/ijerph16071217.

[28] P. Redmond, J. V. Lock, and V. Smart, "Developing a cyberbullying conceptual framework for educators.," Technology in Society, **60**, 101223, 2020, doi.org/10.1016/j.techsoc.2019.101223.

[29] C. Angus, "Cyberbullying of Children: E-Brief," Australia, 2016.

[30] D. H. Tustin, G. N. Zulu, and A. Basson, "Bullying among secondary school learners in South Africa with specific emphasis on cyber bullying; South African Professional Society on the Abuse of Children: ISSN 1562-1383 Child Abuse Research," A South African Journal 2014, **15**(2), 13–25, 2014.

[31] M. Bulger, P. Burton, B. O'Neill, and E. Staksrud, "Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online," new media & society, http://www.cjcp.org.za/uploads/2/7/8/4/27845461/protecting_children_online.pdf, Accessed: 03-Mar-2018.

[32] P. Burton, L. Leoschut, and J. Phyfer, "South African kids online: barriers, opportunities, and risks. A glimpse into South African children's internet use and online activities. Techical Report.," Cape Town, 2016.

[33] J. Phyfer, P. Burton, and L. Leoschut, "South African Kids Online.," Cape Town, 2017.

[34] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," International Journal of Information and Education Technology, **10**(5), 378–382, 2020, doi:10.18178/ijiet.2020.10.5.1393.

[35] H. Qusa and J. Tarazi, "Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High Schools Students," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 0677–0682, doi:10.1109/CCWC51732.2021.9375847.

[36] M. Torres and N. Thompson, "Toward a Cyber Security Adoption Framework for Primary and Secondary Education Providers," in 31st Australasian Conference on Information Systems, 2020.
[37] D. Scholtz, E. Kritzinger, and A. Botha, "Cyber Safety Awareness Framework for South African Schools to Enhance Cyber Safety Awareness," in Computer Science Online Conference, 216–223, 2020, doi:10.1007/978-3-030-51974-2_19.
[38] A. S. De Vos, H. Strydom, and C. B. Fouche, Research at Grassroots for the Social Sciences andHuman Service Professions, Van Schaiks, 2009.
[39] J. H. McMillan and S. Schumacher, Research in education: A conceptual introduction, Longman, 2001.
[40] S. Hymel and S. M. Swearer, "Four decades of research on school bullying: An introduction.," American Psychologist, **70**(4), 293–299, 2015, doi.org/10.1037/a0038928.
[41] D. Adom, E. K. Hussein, and J. A. Agyem, "Theoretical and conceptual framework: mandatory ingredients of a quality research," International Journal of Scientific Research, **7**(1), 158–172, 2018.
[42] P. K. Smith, Cyberbullying and cyber aggression, Routledge, 2012.
[43] E. Maramwidze-Merrison, "Innovative methodologies in qualitative research: Social media window for accessing organisational elites for interviews," The Electronic Journal of Business Research Methods, **12**(2), 157–167, 2016.
[44] R. S. Tokunaga, "Following you home from school: A critical review and synthesis of research on cyberbullying victimization," Computers in Human Behavior, **26**(3), 277–287, 2010, doi.org/10.1016/j.chb.2009.11.014.