Technology, Knowledge and Learning (2022) 27:1133–1153
https://doi.org/10.1007/s10758-021-09545-y

ORIGINAL RESEARCH

An E-safety Framework for Secondary Schools in Zimbabwe

Abel Moyo[1] · Theo Tsokota[2] · Caroline Ruvinga[3] · Colletor T. Chipfumbu Kangara[2]

Accepted: 24 June 2021 / Published online: 28 June 2021

Abstract
Use of Information and Communication Technologies (ICTs) offers extraordinary opportunities for society, particularly in the education sector. Many schools in Zimbabwe are now allowing the use of ICTs devices by learners in order to access the Internet and share educational material. However, there is considerable evidence that through use of ICTs, learners will be exposed to different ICTs risks. Learners using ICTs may face Internet and social media related risks which may expose them to inappropriate content, communicating and meeting strangers, cyberbullying, ICTs addiction and cyber-harassment. Sadly, most parents, teachers and learners do not have knowledge and expertise to mitigate these ICTs risks. As such, this research aims to develop an Electronic Safety (E-Safety) framework for Secondary Schools in Zimbabwe that teaches and safeguards learners from ICTs related risks. Researchers used a qualitative research method to gather information on the use of ICTs, risks faced by learners and how these risks can be mitigated. A case study of two secondary schools in Zvishavane District (Zimbabwe) was used. Data was collected using face-to-face interviews and questionnaires from learners. Data from teachers, parents and officials from Ministry of Primary and Secondary Education, Child Protection Services and Ministry of Information Communication and Technology, Postal and Courier Services was collected using face to face interviews. Collected data was analysed using thematic analysis. A framework was then designed by researchers based on the results from the thematic analysis and reviewed by two experts.

Keyword ICTs · Internet · Risks · Social media · Learner · Addiction · E-safety · Framework

1 Introduction

Use of Information Communication and Technology (ICT) devices is increasing at an a very fast rate in Zimbabwean schools (Ncube & Tshabalala, 2016). ICT devices are now being used in numerous ways by both teachers and learners in schools. ICT are devices to

✉ Theo Tsokota
tsokotat@staff.msu.ac.zw

[1] Information System Management Graduate Student, Midlands State University, Gweru, Zimbabwe

[2] Department of Information and Marketing Sciences, Midlands State University, Gweru, Zimbabwe

[3] Department of Computer Science, Midlands State University, Gweru, Zimbabwe

compose, capture, transmit and display data and information electronically (Zuppo 2012). These devices include mobile phones, smartphones, computers, game consoles, personal digital assistance, network, hardware and software. In trying to scale up utilisation of ICT devices in schools, the Minister of Primary and Secondary Education (MoPSE) directed all schools in Zimbabwe to allow use of smartphones, tablets and laptops by learners at school (Ngara, 2019). Thus, utilisation of ICTs in school was done to enable learners' access to Internet resources and sharing of educational information. If ICT devices are connected to the Internet they allow learners to communicate, access latest academic information and perform various activities wherever they are, in the comfort of their classes and homes (Mandina, 2015).

In the past, learners in Zimbabwean schools were not permitted to bring ICT devices to school (Bhukuvhani, 2017). Schools disregarded the fact that some learners had access to ICT devices without any guidance at home or after school. Also noteworthy is the fact that some parents were unacquainted in the use of ICT devices as they were unaccustomed and unaware of the activities their children get while using their ICT devices. At the same time, teachers who were expected to be more knowledgeable negated their duties to parents who were in most cases not knowledgeable about ICT. Consequently, learners were left on their own without guidance and at risk of suffering negative consequences of using these ICT devices. Most parents lacked knowledge on how to use and give guidance to their children. On the other hand, children are more knowledgeable on the use of ICT gadgets as compared to their parents to the extent that children teach their parents on the use of ICT gadgets. A situation where children teach parents create a moral quandary. Under most circumstances, parents and guardians do not understand their children's cyber activities (Bryant, 2013; Chung, 2004). Resultantly, this gave rise to additional concerns as most parents and guardians did not have the education and expertise to keep their children protected and safe from online predators (Fisk, 2014). Tomczyk and Kopecký (2016) postulate that it should be the responsibility of schools and teachers to raise e-safety awareness amongst learners and young people. Thus, the focus today is no longer on whether ICT should be integrated into the school setting, but on how their integration should be safely done to benefit all parties in a typical school.

Allowing learners to access ICTs has elicited different views from parents, teachers and various stakeholders in education. Ngwenya and Pelser (2018), Ncube and Tshabalala (2016) and Gomba (2016) concur that allowing ICT devices, especially smartphones, tablets and laptops without putting in place measures to mitigate mishandling in secondary school learners will exacerbate risks at the expense of benefits in schools. Cranmer et al. (2009) proposed acceptance of tablets, smartphones and phablets in schools will cause disruptions, behavioural problems, theft and expose children to abuse and ICT risks. Therefore, something could be done as a matter of urgency to safeguard learners from abuse and ICTs online risks. As such, the acceptance of mobile ICT tools has affected the security of secondary school learners when using ICTs for educational purposes, Internet, entertainment and social media (Camacho et al., 2018). In light of this, the security of learners is of paramount importance adopting the matra 'catch them young'. Although it is generally known that allowing ICT devices in schools without adequate measures to prevent misuse by learners could generate more risks than benefits. There is lack of any apparent and clear context-specific e-safety framework for Secondary Schools in Zimbabwe. Consequently, this research seeks to cover that gap in literature and practice.

The main objective of this study, therefore, is to develop a framework for Secondary Schools in Zimbabwe that teaches and safeguards learners from ICTs related risks. In order to achieve the purpose of the study, two critical research questions are raised: 1)

How can Zimbabwe create safe digital environments for secondary students and help them understand what appropriate behaviours are when using technology as part of everyday life, including life at school? 2) What are the e-safety challenges being faced by secondary school learners in Zimbabwe? This paper begins by extensively reviewing literature to highlight critical issues on e-safety. Subsequently, the methodology used in conducting this study is provided, thereafter findings presented as well as the framework followed by the conclusion.

2 E-safety

Electronic safety (e-safety) is a way of educating, protecting, monitoring and supporting learners to use ICT in a responsible way that safeguards them from risks and harming others. Katz (2016) further explains that e-safety includes inculcating in learners and members of staff the responsible use of ICT to minimise risks. Presently, there is no consensus among scholars on what electronic safety is since other researchers refer to it as 'online safety', 'internet safety', or 'web safety' (Shillair et al., 2015). In this study, e-safety relates to the safe and responsible use of ICT resources, including educating, protecting, monitoring and supporting learners from emerging risks.

The Internet provides vital activities in the life of young people, teachers, parents and business organisations. With Internet people can perform various activities which include e-mailing, audio and video conferencing, gaming and videos, file sharing, instant messaging, participating on internet forums, social networking, online shopping, and transfer and banking services. In addition, Hinduja and Patchin (2013) postulate that ICT facilitates information production, storing, editing and communication. ICT devices facilitate instant communication and collaboration. Hence, communication can be done using videos, pictures, audio and written messages. Therefore, ICT can be summarised as the application of technologies that promote production, browsing, sending and receiving information between two or more people over a communication network.

While the Internet facilitates speedy creation, production and dissemination of vast information across the globe, it can be used as a tool to perform illegal activities. Atkinson et al. (2009), Hinduja and Patchin (2013) and Tennakoon et al. (2018) postulate that young learners can abuse ICT devices by performing illegal and engage in unacceptable activities like addiction, harassment and sexual risks. ICT addiction is defined as compulsive Internet use, problematic Internet use, pathological Internet use, Internet dependence, computer addiction or net addiction. Symptoms of the Internet and ICT addiction that can be observed in learners include spending much time online gaming consoles, videos and music. On the other hand, harassment as an act or behaviour that torments, annoys, terrorises, offends, or threatens an individual via e-mail, instant messages, or other means to harm users. While sexual risks include aggressive sexual solicitation materials, child prostitution, child sex tourism, and production as well as consumption of pornographic materials. Learners are easily exposed to sexual risks through the Internet and social media communication with dangerous consequences for their social life. Madden et al. (2013) further explained that learners who spend over 4–6 h a day using ICT resources could be exposed to addiction, harassment and sexual exploitation. Cao et al. (2007) concur that when connected to the Internet, learners spend most of their time downloading voluminous information that is age-restricted such as games, music, videos, pornographic materials, posting comments and plagiarising other

learners' assignments. In addition, the Internet and social media increase the risk of learners falling prey to online scams that seem friendly and attractive, resulting in data and identity theft. Patchin and Hinduja (2018) contend that the use of the Internet and social media cause distraction to the students present in the class.

Previous studies noted that most teachers are not aware and not trained and equipped to manage ICT risks (Gamira, 2019). Therefore, learners are not helped if intimidated, are abused or abuse others using ICT devices. Livingstone and Palmer (2012) as well as Patchin and Hinduja (2018), concur that learners are not able to differentiate threats from games, genuine friends form pretenders, and what information to share while online. On the other hand, many school learners may also negatively be affected by bloggers and those who post wrong information on social sites which can mislead them in their education.

This section defined ICT, e-safety and noted risks faced through the use of ICTs devices. Invariably, this was done to provide background as well as insight, understanding and clarity on critical issues around e-safety. The next section presents the theoretical foundation of this study.

3 Social Construction of Technology (SCOT)

This study is guided by Bijker, Hughes and Pinch's Social Construction of Technology (SCOT) (Bijker, Hughes, and Pinch 1987). The choice for the theory emanated from notable previous studies (Alnesafi, 2018; Jones & Bissell, 2011; Klebl, 2008) which used the theory in educational technology in an educational changing environment. SCOT is based on the assumption that technology is socially constructed and interpret instead of being clearly defined product (Selwyn, 2013). SCOT enables understanding of socio-technical issues of the adoption, development and utilisation of technology including Information and Communication Technology. Furthermore, SCOT can be used as a framework to analyse how different social group groups perceive technology thereby explaining why certain technologies are accepted or resisted among different competing groups. In this study, there are various groups interested in e-safety in schools which include learners, teachers, schools, parents, NGOs, MoPSE and the Government of Zimbabwe (Goz). Thus, success or failure in e-safety in schools' depend on the meanings from these groups and their needs.

The SCOT theory comprises of three related components which are; relevant social groups, interpretive flexibility and closure. Relevant social groups consist of entities that share the same set of meaning to a particular technology. Social groups are distinguished or identified by shared or divergent interpretation of meanings to a particular technology. These relevant groups have been identified in the previous paragraph. Interpretive flexibility means that relevant social groups have different interpretations of a particular technology. In this case, the government may have directed use ICT to enable access to Internet resources and shared educational information, while teachers and learners may have different uses and safety concerns. Closure refers to a state where different interpretations given by relevant groups amalgamate thereby achieving consensus on a particular technology. In this case, closure will occur when learners are e-safe, when they will be able to cope with the new mode of learning using ICT devices in a responsible manner deriving benefits and dealing with ICT risks. Thus, e-safety is a result of interplay and role clarity of the major relevant groups. These relevant groups are the; MoPSE, School, Parents, Learners and other role players.

4 Methodology

Interpretivism research philosophy guided this study. Interpretivism involves study of social practices in the context of an information system (Oates, 2007). This philosophy predominantly deals with qualitative data, employing an inductive reasoning strategy in order to infer conclusions about the research findings. The researcher sets up a platform to interact with respondents in order to understand behaviours and meanings attributed to them. Thus, qualitative research was employed in this study. In qualitative research studies, people's lives are under real-world conditions without depending on numerical measurement by focusing on discovering true inner meaning from respondent perspectives and occurrences at close viewpoint (Creswell, 2015). This was supported by Maxwell (2013), who explains that qualitative researchers collect data in the field at the site where the respondents' experiences, views, inspirations as well as the problem is under investigation. In this research, the questions mainly focused on the ICT uses and possible risks that learners were facing both at school and home. Learners were also asked about their parents or guardians' response to their ICT uses at home. Parents and officials were asked how e-safety could be inculcated, prevented and mitigated in learners when utilising ICT devices in Zimbabwean secondary schools. Therefore, the strength of this research lies in the fact that it positions learners at the centre of the investigation under real-world conditions.

4.1 Sampling

Schools and organizations that formed part of this study were purposefully chosen to provide a proper representation of the various relevant social groups who are concerned with e-safety in Zimbabwean secondary schools. A total of two secondary schools in Zvishavane District (Midlands Province, Zimbabwe) were used. Zvishavane District was used as representative of a town with diverse tribes and cultures as well as diverse economic activities in Zimbabwe (Ndhlovu, 2006). Schools were selected as typical and represented rural and urban school respectively. Thus, the chosen schools and district were observed as the microcosm of the schools in Zimbabwe.

4.2 Data Collection Strategies

Data was collected between end of 2018 and mid-2019. Data was collected from Form 4 learners after consent from their parents or guardians. During collection of data, face-to-face open-ended interviews and open-ended questionnaires were used. Questionnaires were personally distributed and collected by the researchers. Before the study was done, researchers were given written permission by the Ministry of Primary and Secondary Education (MoPSE), School Heads as well as approval of learners' guardians. This study focussed on Form 4 learners who were between 16 and 18 years. This is the age when most learners are entering puberty and peer pressure is at its climax, learners are making life decisions, about their career, making life friendship and learners are entering maturity and legal age of majority. Respondents (especially learners) were assured that their responses were going to be treated in confidence and would not be disclosed to their teachers, school administration and parents.

The relevant group which was purposively chosen had the following respondents; 38 Interviews with learners consisting of 20 Interviews from urban School A and 18 from rural School B. In addition, 68 questionnaires from learners consisting of 36 from School

A and 32 from School B. Data was also collected from one Director of Policy in Ministry of Education, two directors from Ministry of Information Communication and Technology, Postal and Courier Services, and three officials from Non-Governmental Organisations dealing with children-related issues, five parents, four ordinary teachers, two school heads using face-to-face interviews. The composition of respondents is presented in Table 1.

5 Data Analysis

Thematic Analysis Method was used to manually analyse the collected data from interviews and questionnaires, according to Creswell (2015). Data was transcribed and each respondent was numbered according to the relevant groups during the transcription of data. Accordingly, the frequency of each code was tallied and converted into a percentage for each of the categories. Consequently, the coded data were presented using tables, graphs and texts. The following section is a discussion of the results.

6 Findings

This section presents findings from the data collected from the relevant groups which included learners, parents, teachers, government officials and other role players. Findings were grouped under four appropriate headings which are ICT uses, ICT risks faced by learners, Guardians Response to ICTs uses at home and Challenges of Preventing ICTs Risks.

6.1 ICTs Uses

All learners responded by stating their ICT uses at home and school. The narrative of all respondents indicated that learners are indeed using ICT devices for entertainment, academic and socialising through social media. However, after further analysis, it was found out what learners are using ICTs devices more for social and entertainment purposes rather than for academic activities.

Table 1 Respondents

Description	Number	Institution	Data collection Method
Director of policy	1	MOPSE	Interview
Director	2	MICTPCS	Interview
Officials	3	NGOs	Interview
School head	1	School A	Interview
School head	1	School B	Interview
Parents	5		Interview
Teachers	2	School A	Interview
Teachers	2	School B	Interview
Learners	36	School A	Questionnaires
Learners	32	School B	Questionnaires

6.2 ICT Risks Faced by Secondary School Learners

This section presents ICT risks faced by learners when using ICT devices which include exchanging and receiving inappropriate content, stored inappropriate materials in ICTs devices, accepting and meeting strangers, meeting online friends physically and pornographic as shown in Fig. 1.

6.2.1 Received Inappropriate Content

From the findings, 15 interviewed learners indicated that they have seen pornography somewhere in their mobile phones or computers. For instance, Interviewee: Learner_3schoolA said "*Naked pictures, vulgar stories, amazing pictures.*" Still on the same issue, Interviewee: Learner_5schoolA added that *"Vulgar stories, love stories, love letters, sex videos"*. Furthermore, Questionnaire: Learner_7schoolB added ***"Naked pictures, porn videos, erotic images, hip-hop music."*** Thus, it was evident that learners had already been exposed to inappropriate sexual content.

6.2.2 Stored Inappropriate Materials in ICTs devices

All learner's responses show that there was something stored in their ICTs devices and hidden from parents or guardians. From follow-up questions, responses indicated that the stored information, included music, videos, pornographic material and love messages. Respondents were assured that their responses were going to be treated in confidence and would not be disclosed to their teachers, school administration and parents. Storage of inappropriate materials in ICT devices may indicate that some learners do not detest inappropriate materials.

6.2.3 Accepting and Meeting Strangers

Analysis of the findings revealed that 52% of girls and 2% of boys accepted to meet their online friends. Thus, most learners accepted that they had met someone whom they did not know before who had requested friendship online. Interestingly, most girls requested the purpose of the meeting before accepting the invitation to meet. Those who accepted

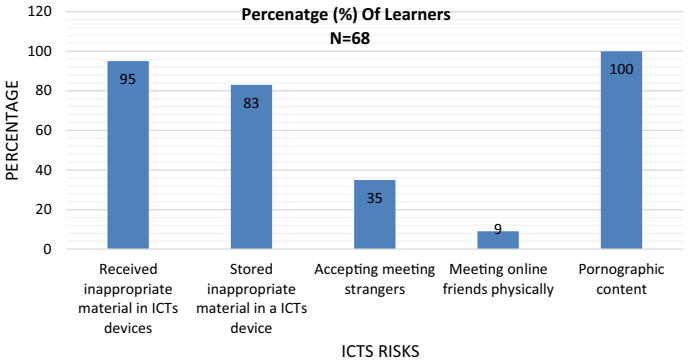

Fig. 1 ICT Uses (Own compilation)

to meet demanded more pictures and made further interrogations before giving in to the invitation than boys**.** Only a few learners accepted that they had met strangers they had first see on WeChat (40%), SMS (15%), Facebook (36%) and WhatsApp (92%). These findings infer that girls are exposed to online predators more than boys as they accepted to meet strangers. This implies that girls are at risk of being raped, kidnapped or murdered and their educational time wasted while online. As a result, teachers and guardians ought to provide measures to keep them safe from risks of online friendship.

6.2.4 Meeting Online Friends Physically

More girls than boys confirmed that they agreed to meet people who had liked their profiles online. The meeting places most cited include streets, churches, schools and township recreational points. Thus, responses from girls confirmed they are at risk of being kidnapped, raped and killed by these online friends and their academic performance can deteriorate due to spending much time on friends. Even in rural areas, only girls confessed to meeting peoples who invited them online at the shops and outside their homes. Accepting and meeting online friends show that girls are exposed to many risks; as such, they need education about the risk of liking and meeting strangers physically who befriend them on social media.

6.2.5 Pornographic Content

The respondents were asked if they had ever received pornographic material on their mobile devices. All learners (100%) indicated that they had received pornographic material as depicted in Fig. 1. This is further supported by comments from some respondents who said that they had seen "*Naked pictures, porn videos, erotic images, hip-hop music."* (Questionnaire: Participant_13schoolB). Similarly, another respondent noted that *"Naked people, pornography, romance movies."* (Questionnaire: Participant_11schoolA). Thus, responses from learners indicated that they had been exposed to pornographic material.

6.3 Guardians Response to ICTs Uses at Home

The question about guardians' response to ICTs uses at home was asked to find out whether their guardians at home say or do anything to the learners when seen using the ICTs device. Figure 2 displays percentages (%) of their responses.

Responses from learners' show that most guardians complained about use and time spent using ICTs gadgets while at home. Figure 2 shows that 22% of the guardians advised their children to do school work while 15% would question the children on what they were doing on ICT devices; 20% just did nothing. On another hand, 9% said their parents did don't know they have mobile phone and they use it away from their parents. However, 9% took the ICT device away from the children and 9% controlled time children had access to devices. On the other hand, guardian responses showed that learners spend much time on ICT gadgets than on academic resources at home. Most guardians did nothing (20%). Comments from parents and guardians suggest lack of knowledge on how to deal with e-safety concerns as well as indifference on the part of parents and guardians.

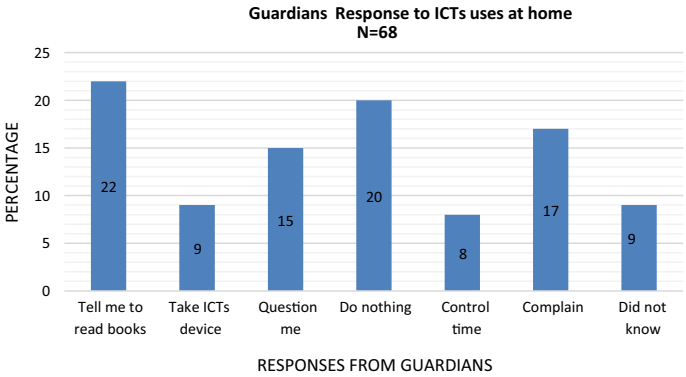

Fig. 2 Responses from guardian (Own compilation)

6.4 Information Hidden From Parents

Most learners responded fairly well on that question. This question was included in the interviews and questionnaires respectively, so as to give learners room to write their answers down if they are shy or afraid to talk freely about their secrets in the ICTs device. Other wrote the *'porno'* but deleted and rubbed the word. Responses provided by learners showed that they have been exposed to pornographic materials, and there was no noticeable difference between the responses from urban and rural school. In addition, learners were aware that parents and teachers detest pornographic materials which could explain why learners were hiding such material from their parents. Furthermore, it shows that some pornographic materials are still stored in learners' mobile phones and computers. All learners indicated that they have watched pornography somewhere in mobile phones or computers. Exposure to pornography may indicate that learners need education about the negative effects of watching and storing such content in their ICTs devices. Most parents, teachers and officers interviewed agreed that learners can view pornographic materials at school if smartphones, tablets and laptops are allowed at school.

7 Proposed Solutions to ICT Risks

This section covers ICT risk prevention strategies that can be implemented at home, school and the Ministry of Primary and Secondary Education.

7.1 Prevention of ICTs Risks at Home

Analysis of the responses on how ICTs risks could be prevented at home revealed that most parents are not attentive to their children's ICTs behaviours at home. Therefore, parents/guardians are not well-informed about ICTs uses, capabilities and how to educate as well as deal with risks that may arise from the use and abuse of ICT devices. It was indicated that *"some of us do not have expertise than learners in terms of using the ICTs devices. The learners know much than the parent, therefore, supervision is*

difficult." (Interviewee: HeadschoolA). Parents/guardians are not able to periodically check learners' activities and surrendered such responsibility supervising learners' activities to teachers at school. Guardians' responses show that the safety of learners while using ICT devices is of primary concern. Thus, parents and teachers can work jointly in order to come up with ways to safeguard learners from online risks.

7.2 Prevention of ICTS Risks at School

The teachers in selected schools did not have any educational, reporting and preventive mechanisms for ICT risks at their stations. Most teachers explained that they were not interested in coming up with mechanisms to make learners safe, and they viewed it as extra work that is outside their primary duty of teaching. The teachers proposed banning hand-held devices, especially laptops, mobile phones, smartphones and tablets, as the best solution. Proposed banning of ICT devices was echoed by one respondent who said *"The learners to be banned from bringing their tablets and smartphones to school and use the provided computer at school*." (Interviewee: TeachersSchoolB2). However, some explained that they could be easily smuggled and used in classroom and school premises secretly by learners. In addition, other teachers proposed building and furnishing computer laboratories at schools as better than allowing mobile phones and tablets at school. It was submitted that *"I think computers are better than allowing smartphones and tablets. Computers can be programmed to deny certain information through the firewall. Computers have more storage space, bigger screen size and can be connected to the projector when doing a presentation. More Software can be installed and well managed that in small handheld devices. Information stored in the phone can be easily monitored by the teachers that stored in the private smartphones."* (Interviewee: TeacherschoolA1).

It appears that there was consensus among teachers that acceptance and use of smartphones and tablets in schools create more problems that distract learning and divert learners from concentrating on academic matters. Therefore, learners could use the ICT resources provided by the school and not their ICT devices from home. Computers in the laboratory have to be configured to filter unwanted access to certain sites, and they use these under the supervision of qualified ICTs teacher, not everyone. One respondent echoed the following sentiment; "*The school must put Wi-Fi for teachers and computer lab for learners. Learner can be asked to use the internet in school computer lab only."* (Interviewee: TeacherschoolA2).

Teachers did not have a solution than banning the use of smartphones and to use computers only designated in the school laboratories. They see building computer labs at school as better than allowing mobile phones and tablets to be allowed in schools. However, teachers who are computer literate did not agree with the idea of not accepting ICTs devices in their classrooms.

7.3 Prevention of ICTS Risks by the Ministry of Primary and Secondary Education

Currently, there is no policy dealing with abuses of ICTs in the primary and secondary schools' national curriculum. Teachers, parents and the community proposed that the absence of ICTs framework shows that the Ministry of Primary and Secondary Education (MoPSE) is creating confusion in schools through hurriedly acceptance and utilisation of ICTs by learners at schools. It was noted that *"currently the ICT policy is under development and it will address the issues that arise from the use of technology*. The *policy is*

under development by the Ministry of ICTPCS and the education is going to develop their own policy that will deal with all the risks that arise for the use of technology in schools." (Interviewee: DirectorMICTPS1). Similar sentiments were echoed by another respondent who said "*MoPSE have to develop a policy that clearly explains how the ICTs related problems will be addressed. There must be a way to train learners, teachers about ICTs risks and measure to mitigate them. In addition, there must be a way of communicating with parents and measures to safeguard learners at home form online risks, criminals and unacceptable behaviour.* (Interviewee: DiectorMoPSE2).

Most of the responses (96%) show that MoPSE should include electronic safety lessons in the curriculum for both primary and secondary schools. The MoPSE is advised to develop National ICTs Educational laws and Policies that manage ICTs crimes in education. In addition, possibly national, provincial and district offices that could advise schools and investigate ICTs issues encountered by schools without delay. Furthermore, at least two qualified teachers could urgently assist learners in every school to manage ICTs issues. In addition, when developing ICT Educational Policy, the government and the MoPSE may possibly consult more stakeholders and renew the Child Protection Policy.

8 Challenges of Preventing ICTs Risks

This section explains the problem that can be faced by learners from the use of ICT devices at home and school.

8.1 Challenges of Prevention of ICTs Risks at Home

Parents were asked to identify challenges they face in preventing ICTs risks at home. Most parents responded that they were not able to control children from using ICTs for non-academic activities. They explained that they are not always available to see what learners are doing. Parents who share smartphones with their children accepted that they do check because they are sharing the same phone with their children. Parents who desire to check responded that it is difficult due to software used to hide the content stored. Hiding content by learners shows that there is something inappropriate stored in the ICT devices. Hiding content by learners was supported by responses from parents indicating that their children are keeping their activities private from them and are not willing to let their parents the content. A parent indicated "*Children put password and pin code. Therefore, it is difficult even to see what is stored inside.*" (Interview: Parent_1). Another said, ***"My child goes with the phone wherever he/she is. If left by mistake, it will be locked***" (Interviewee: Parent_4). This was buttressed by another who said, *"I am not able to browse or found where the picture and videos are stored.*" (Interviewee: Parent_5). The other concluded *that "the learners are using software to hide their materials. Therefore, it is difficult to check, even if you want, you can create war at home if you insist to check"* (Interviewee: Parent_2). Hiding content by learners demonstrate that there might be many inappropriate and harmful material stored and hidden by learners in the ICT devices.

8.2 Challenges of Prevention of ICTs Risks at School

Respondents were asked about the challenges of preventing ICTs risks at school. Most teachers, parents and officers criticised the use of smartphones and tablets and indicated

these as a significant source of problems at school. Teachers and parents argued that learners' behaviour and attitude while using the devices is not predictable and can compromise their education because they know little about the consequences of misusing these devices. They all agreed that most learners' performance would drop and only a few who are disciplined in their use of ICT devices can pass. This was supported by officers who agreed that allowing laptops, smartphones and tablets in a classroom is just like giving a child a gun to do whatever they wish with it.

Most parents, teachers and officers concur that learners can hide devices and utilise them for non-academic activities in the absence of a teacher and even use them clandestinely in the lesson thereby affecting their performance. Comments infer that interviewed teachers, parents and officers were not comfortable with the idea of allowing learners to use ICT devices freely in school premises. This was supported by parents and officers who proposed that allowing smartphones in the classroom was just like giving a child a gun to experiment with. It was indicated that,

"*it is difficult to supervise whether the learner is using the ICTs gadget for academic purpose whilst the teacher is delivering his lesson. Learners might be on Facebook, WhatsApp, and Skype chatting with other learners or online friends.* L*earners can be recording what the teacher is doing whilst not listening. This will distract the learners. The devices may not have the necessary storage to record and store all the daily activities "*(Interviewee: DirectorMoPSE2).

Furthermore, another respondent supported this view by saying *"Learners can lie their location; the reason for not coming to school can trick teachers and school administrative staff. Learners are clever they can record and post videos on YouTube that can tarnish the image of teachers, themselves and school; this will distract the learning process."* (Interviewee: NGOOfficer2).

Most parents agreed that learners could hide mobile phones under their desks and use them for non-academic purposes while the teacher is not looking. This shows that parents are against the idea of allowing learners from being allowed to use smartphones and tablets at school. Therefore, to reduce the tendency of learners need continuous education, monitoring and control regarding the acceptable use of ICT tools at home.

8.3 ICT Challenges Faced by MoPSE

This section explores challenges faced by the MoPSE in implementing ICTs in schools. As indicated by the MoPSE officials, ICT devices, especially smartphones and tablets, have brought several problems to young learners. Similarly, responses from officers, parents and teachers showed they are against the idea of allowing Ordinary Level learners to use laptops, smartphones and tablets in schools. In addition, as a prevention strategy, they proposed that schools put in place education, monitoring, security and safety mechanisms. Allowing devices such as smartphones, tablets and laptops at secondary schools would make maintenance of order, the security of the devices and control of usage very difficult.

Furthermore, officers, parents and teachers are currently understaffed in schools and there are no qualified teachers and personnel to supervise use and no binding regulations to deal with risks that may arise from ICT abuse. Furthermore, much time will be wasted in dealing with abuses and ICT crimes experienced at school. Based on the lengthy discussions done, it shows that Zimbabwe is not yet ready to allow gadgets such as personal smartphones, tablets and laptops in schools. Much could be done and mechanisms enforced to prevent protruding risks. An extract of the interview below buttresses this point that,

"*currently the MoPSE have no adequate finance to speed up the Computerization program. There are no experienced teachers to cater for the use of ICTs in all the schools. Not all schools have electricity and funds to electrify their schools. In the use of smartphones, there is resistance in some school, parents and community to allow learners to use mobile phones in schools."* (Interviewee: DirectorMoPSE2).

"*Not all learners will be able to purchase the ICTs devices which can be used in teaching and learning." The other parents are very poor and not able to acquire these smartphones for their learners. The school has no funds to implement, train and maintain the ICTs infrastructure needed to monitor the learners' activities.* (Interviewee: NGOOffer3).

Officials revealed that use of ICT devices especially smartphones are a threat to learners. It was equated to giving guns to learners to protect themselves. It was one of the most discussed questions in the interview. The cited challenges need to be addressed before allowing learners to bring their ICT devices to school in order to prevent problems identified. Moreover, most teachers explained that they have heard that ICT devices are now acceptable on the informal media, and there was no formal communication made to the schools.

9 Discussion

This section synthesises and interprets the findings of the study, comparing them with previous literature in an endeavour to answer the main research question: How can Zimbabwe create safe digital environments for secondary students and help them understand what appropriate behaviours are required when using technology as part of their everyday life, including life at school?

In the preceding section, the prevailing situation related to e-safety in Zimbabwe secondary schools was presented. Findings from both rural and urban were very similar regardless of different geographical and social settings. Confirming that Whitty (2020) thinking that regarding, e-safety everyone, irrespective of geography and social standing. It was apparent that there is lack of e-safety training and education for secondary learners in Zimbabwe. This dovetails with views by researchers such as Matyokurehwa et al. (2020), Ngara (2019) and Gamira (2019). Perhaps more worrisome was the fact that ICT devices were being used more for social and entertainment rather than academic activities. Use of ICT devices for social and entertainment was consistent with the findings of Tsokota, Mahlangu, Rebanowako, and Furusa (2017) who argue that in Zimbabwe, gadgets are mainly used for social purposes. Consequently, this may also explain why ICT devices in schools were resisted by both parents and teachers. This, therefore, points to the need for education for learners to understand what appropriate behaviours are expected when using technology as part of their everyday life, including life at school.

Sharing videos, pictures, and jokes take valuable time of learners that might otherwise have been used for sharing educational materials. Therefore, learners could be encouraged to reduce non-academic activities because these reduce academic concentration, occupy much space in the ICT gadget and distract their studies.

Findings also confirmed that learners were involved in unacceptable and risk behaviour like receiving and storing inappropriate materials on their ICT devices, accepting to meet strangers, meeting online friends physically and pornographic material. It is important to note that risks emanate mainly from hiding of information from parents or guardians and teachers. Therefore, parents and teachers are encouraged to be friendly

and be able to gain trust of learners so that they can open up on their activities and get appropriate guidance**.** From the findings narrated and displayed, learners are already exposed and have access to inappropriate materials.

All learners testified that they had watched pornographic material. Exposure to pornographic material by learners is consistent with the views by scholars such as Patchin and Hinduja (2018) who found that in European countries, most learners are exposed to pornography and victimisation from the use of technology in colleges. Evidently, learners in developing countries, including in Zimbabwean schools, are also exposed to these risks caused by globalisation as a result of technology. Findings also noted that girls are exposed to online predators more than boys based on their risk behaviour of meeting strangers whom they have never met before. This finding contradicts the findings of Matyokurehwa et al. (2020) who asserted that there was no significant association between gender and cybersecurity awareness. This could be attributed to the different nature of risks that that were studied. Matyokurehwa et al. (2020) studied social engineering attacks, malware attacks, IoT attacks which are generally the same irrespective of gender.

The findings show that there is no framework or policy in place to deal with abuse of ICTs in school by learners. There is no standardization of using ICT in schools. Evidently, the absence of an ICT framework shows that the government is hurriedly creating confusion in schools about the implementation of ICTs. Some schools implemented ICT without resources thereby increasing the gap between rich and poor schools.

Findings also indicate that e-safety is a contentious subject with Zimbabwean society. While relevant groups have divergent views on how e-safety can be enforced in secondary schools they seem all to agree on the need for e-safety in schools. Teachers seem to agree on suppressing use of ICT devices as a mechanism to enforce safety. This contradicts views by Gcaza (2018) who argues that to ensure e-safety, education should be at the centre of all e-safety efforts. Thus, ICT risk education and reporting mechanism could be considered crucially influential and can be at the core of e-safety efforts. Total ban results in learners using gadgets but nonetheless hide their activities from parents and teachers. Hiding activities from parents and teachers adversely heighten mistrust between learners and parents as well as teachers. In addition, parents/guardians may well be ready to gain knowledge of the latest applications that have been developed and find solutions to the problems arising from using them. Gaining knowledge by parents and guardians equips them with knowledge about the positive and negative effects of ICTs on their children.

Schools are currently developing their own ICT rules and regulations that differ from school to school. A national schools ICT policy is suggested to give guidance on the above. This will guarantee standardization of using ICT in schools. Presently, there is no framework or policy in place to deal with abuse of ICTs in school by or to learners. Based on this, it could be concluded that absence of ICT framework shows that the government hurriedly created confusion in schools by calling for the implementation of ICT without any clear policy or framework. Thus, the government could consider developing a national e-safety framework and implement it in all schools. In addition, the framework must be constantly evaluated and updated. Resources made available in terms of development of teaching material is woefully inadequate. Furthermore, staff have not been developed to instil and inculcate acceptable e-safety behaviour. Teachers need to be empowered through education and workshops on e-safety.

Based on the findings of this study, an e-safety framework can be developed to assist learners to deal with ICT risks irrespective of location. Inclusion of all relevant groups and their roles and responsibilities can help in reaching a point of agreement described as

closure in the SCOT theory. At this point, problems related to e-safety in schools would have been solved. The next section describes the proposed e-safety framework.

10 Proposed E-safety Framework for Secondary Schools in Zimbabwe

From the analysis of results, an e-safety framework for secondary schools in Zimbabwe is suggested shown in Fig. 3. The proposed e-safety framework was validated by two expert reviewers who were chosen based on their knowledge and experience in the field. The first expert reviewer is both an academic and a practitioner. He holds a doctorate in Educational Technology and has published extensively in peer-reviewed journals and has been a secondary school teacher for 15 years before joining the university as a lecturer for 10 years. The second reviewer also holds a doctorate in Information Technology and has 15 years experience as a university lecturer. The experts agreed that the framework could help inculcate e-safety, mitigate and control ICT risks faced by learners at home, school and the community.

According to the proposed framework, the e-safety is a result of interplay and role clarity of the major stakeholders. These are, MoPSE, School, Parents, Learners and Role Players.

10.1 Ministry of Primary and Secondary Education (MoPSE)

All early childhood, primary and secondary education in Zimbabwe fall under the remit of MoPSE. MoPSE provides policies, strategies and regulation that guide all early childhood, primary and secondary education. On this basis, the proposed framework recognises MoPSE as the developer of all policies in education, including ICT policies. The MoPSE could consider incorporating ICT risks and e-safety in all primary and secondary

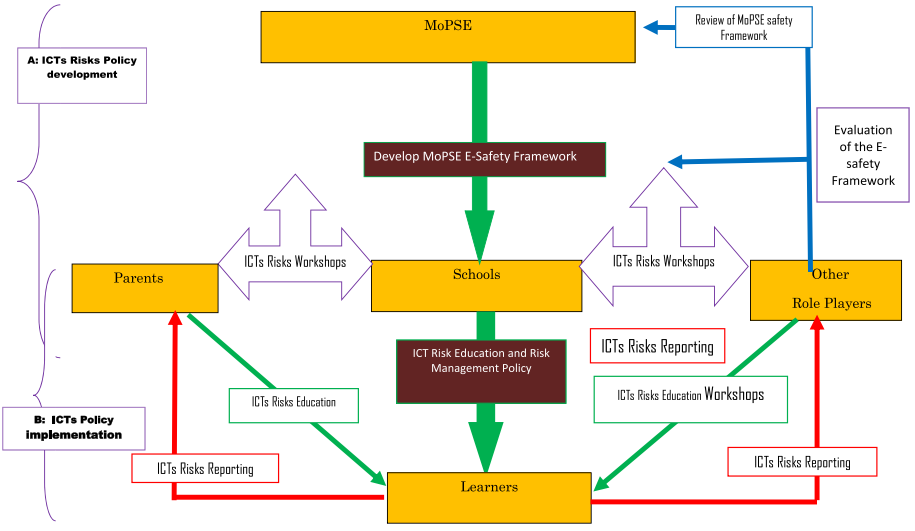

Fig. 3 An E-safety framework for secondary schools in Zimbabwe

curriculum. In addition, MoPSE could consider conduct workshops with in-service teachers to equip them with expertise about ICTs risks, crimes and misuses. Equipping teachers enabling them to be able to teach, manage and control ICT risks in schools.

Moreover, the MoPSE could provide funds for ICT research and development for teachers in schools and colleges. In other words, the MoPSE ought to work with other ministries which include Ministry of Home Affairs, Ministry of Justice and Parliamentary Affairs, Ministry of Information Communication Technology, Postal and Courier Services and non-governmental and international organisations which deal with young people to develop strategies that apply to all ministries.

10.2 Schools

The Schools are at the centre of the framework. They are expected to implement the National Curriculum by providing conducive environments for teaching and learning for learners. In addition, schools formulate their school syllabus from the National syllabi and teach learners ICTs risks and ways of managing them when exposed to the risks. The school could consider developing its own rules and regulations about uses of ICTs, which include acceptable and unacceptable activities. In addition, schools are expected to be supervised by the MoPSE to establish if they are teaching and providing learners with education and security and controlling measures that keep them safe.

Schools could also develop ICTs crime reporting structures that are taught to all learners at school continuously. Each school may possibly provide a well-detailed list of acceptable, unacceptable activities and how to respond to ICT issues that affect learners. In addition, schools could work continuously with police services for further investigation of the crimes if needed. Schools could be used as venues for workshops for learners, teachers and NGOs. Schools could be provided with Internet services from accredited, reputable suppliers who can configure and block unwanted materials from being accessed by learners at schools.

In addition, teachers could consider continuously providing education about responsible and acceptable online behaviour to learners who utilise ICT devices. Teachers, through interaction with learners at school, can easily identify activities learners spend most of their time on. Such interactions help identify uses, risks and effective control measures to keep them safe when they come across new things while using ICTs devices. Teachers with appropriate training can investigate ICTs risks and provide valuable services to learners. Most learners in school follow instructions about acceptable and unacceptable behaviour, legal and illegal activities explained to them by teachers. Therefore, teachers play a crucial role in the life of learners at school and after school. Teachers act as role models for learners and are trusted by learners.

10.3 Parents

A parent's primary duties and responsibilities are to acquire the ICT devices for the learners as well as provide ICT education to learners. In addition, parents ought to be knowledgeable about uses, benefits and ICT risks that may be faced by the children when utilising the ICT device. It is suggested that parents at home be friendly to gain trust of their children as this helps them observe, identify and control activities done by their children as well as to get ICT risk reporting. If parents are not friendly, their children will not open up on ICT risks challenges they face. While parents observe children activities at home, it

is suggested that they be consulted in the development of ICT policy document at school and made to agree and sign for what is expected from the children when using ICT devices at school. Furthermore, parents can receive more knowledge from teachers on how to keep children safe through consultations and workshops from schools and NGOs. In addition, parents could also be instrumental in teaching their children on ICT education.

10.4 Learners

Learners are at the core of this study. They are supposed to be protected from all emerging ICT risks in various forms. Learners are generally expected to use the ICT resources responsibly at school and home. They have to be oriented, cultured, guided and provided with reporting procedures if faced with something not proper when using ICT devices. Education, according to the framework, could come from parents, schools and other role players. Learners have to be clear on which activities are acceptable, unacceptable and legal to avoid being continuously affected in their academic activities. They could be provided with different types of activities that might be used by online predators to attract them and the consequences of not following the stipulated ICT policies, rules and regulations. In addition, they have to be taught what to report, where and how if the need arises and be alert when they receive or are exposed to something they are not comfortable with while using ICTs devices.

10.5 Role Players

In addition, the frameworks all recognise other role players. These are the stakeholders who include non-governmental organisation and other government ministries. Role players could assist teach learners, train teachers, school administration staff and parents. They also help to investigate ICT crimes reported and how the learners can be kept safe while using ICTs for education purposes. Role players could consider holding workshops with teachers at schools, learners and parents about emerging threats and how they can make learners safe. Conducting workshops helps share ideas, identify types of risks, consequences and note measures that might be taken to mitigate them.

11 Conclusion

The education sector in Zimbabwe is still ill-prepared to deal with e-safety issues in schools. Moreover, most parents, teachers and learners do not have knowledge and expertise to mitigate these ICT risks. This study has provided empirical evidence from Zimbabwean schools through insights and lived experiences of stakeholders such as learners and other role players in the education sector. Stakeholder involvement is crucial in devising policies and frameworks and their implementation. The major research questions in the study were answered by developing an e-safety framework for schools in Zimbabwe. Thus, the proposed e-safety framework may help learners, teachers, schools, parents, NGOs, MoPSE and the policymakers on how to safeguard learners when utilising ICT resources. The proposed e-safety framework was validated by expert reviewers in the ICT field. It is, therefore, concluded that it can help to inculcate e-safety, mitigate and control ICT risks faced by learners at home, school and the society at large. There have been no previous empirical studies that considered e-safety issues in Zimbabwe.

Consequently, this study is a useful addition to the body of knowledge as it has contributed to an increased understanding of e-safety in developing countries, especially in Zimbabwe. An Electronic Safety (E-Safety) framework for Secondary Schools in Zimbabwe that teaches and safeguards learners from ICTs related risks was developed to assist with the problem. In addition, this framework can also be adopted by other developing countries in a similar context to Zimbabwe. Furthermore, the research has also contributed to the ICT4D literature.

The findings of this study differ from previous studies such as Matyokurehwa et al. (2020) who argued that there was no significant association between gender and cybersecurity awareness. Unlike other studies of e-safety (Lorenz, Kikkas, Sõmer, & Laugasson, 2019; Tomczyk and Kopecký (2016) which are based on the analysis of the initiatives in developed countries the strength of this research lies in the fact that it positions learners from a developing country at the centre of the investigation under real-world conditions. Thus, this study is a shift from frameworks developed without encompassing local peoples' concerns and contexts. This empirical, qualitative and micro-level study is based on MoPSE, School, Parents, Learners and Role Players' interpretations and real-life stories. It reflects the realities of how e-safety is experienced and responded to on the ground. Respondents were afforded the opportunity to describe their experiences thus providing detailed descriptions of their e-safety experiences. Previous researches (Barros & Lazarek, 2018; Šimandl & Vaníček, 2017) marginalised the voices of learners in Zimbabwe, regardless of the fact that they are key stakeholders who can either constrain or enhance e-safety in schools in any country. Therefore, the strength of this research lies in the fact that it positions learners in Zimbabwe at the centre of the investigation.

Thus, the novelty of this study lies in its development of a context-specific framework for e-safety in secondary schools in Zimbabwe. As such the distinctiveness of the proposed e-safety framework is grounded in the unique challenges being faced by the schools in Zimbabwe.

12 Implications for Theory, Methodology and Pedagogical Practice

This study has implications for theory, methodology and pedagogical practice. At theoretical level, the study has provided a context-specific novel e-safety framework for effective, sustainable and safe use of ICTs in Zimbabwe. As such, it also provided appropriate interventions from government and other role-players in the education sector. Practically, this research has helped create an e-safety framework for schools to help them create safe digital environments for students and help them understand what appropriate behaviours are when using technology as part of everyday life, including life at school. The e-safety framework can be applied in any ICTs risks faced by learners irrespective of location. Moreover, inclusion of all stakeholders and their roles and responsibilities helps avoid conflicts and disagreement about acceptable uses and criminal behaviour. Ignorance by other stakeholder in what the government, ministries, NGOs, parents and learners are doing when using ICTs devices and the associated risks that they may face and the appropriate action to do is also catered for.

Methodically, the sophistication of this research lies in the fact that it deployed a multi-cross-sectional case study approach, combining MoPSE, School, Parents, Learners and Role Players Such an approach undoubtedly provides pertinent insights into the phenomenon under investigation. This is phenomenal in understanding experiences,

insights and behaviours of learners, especially under the growing concern of the phenomenon of e-safety risks. Thus, the uniqueness of this framework stems from the fact that it is informed by the needs and challenges currently prevailing on the ground which happen to be influenced by factors that uniquely define e-safety in secondary schools in Zimbabwe.

At a pedagogical practice level, this study has contributed an e-safety framework for secondary schools in Zimbabwe based on empirical study. The framework provides strategic responses to e-safety informed by the centrality of secondary school learners. Unlike other studies which just looked at e-safety at organizational level. Thus, the novelty of this study lies in its development of a context-specific framework which is informed by the empirical data. Unlike, previous researches which mainly focused on e-safety at the organisational level and ignores the grassroots level. Consequently, lessons gain in this study can offer guidance in the design and implementation of education.

campaigns e-safety for school learners. The study discussed the challenges faced with leaners in coping with the new mode of learning using ICT devices which end up posing risks of bad behaviour. An Electronic Safety (E-Safety) framework for Secondary Schools in Zimbabwe that teaches and safeguards learners from ICTs related risks was developed to assist with the problem. However, the framework is yet to be tested for practicality. In addition, this study has divulged pertinent issues and added to the body of knowledge, the customised details on culture-safety and how they can be utilised to cultivate e-safety in the Zimbabwean context. It will also aid a basis to develop, implement and review e-safety strategies in Zimbabwean secondary schools. Furthermore, it is imperative to involve learners in designing a curriculum relevant to their needs based on knowledge gaps to remove misconceptions and misinformation about e-safety that may occur. From the reviewed literature, most of e-safety frameworks do not include the government, ministry of education responsible for education and NGOs. Inclusion of Government helps speed up the process of e-safety in school, colleges, universities and other government ministries, since the government is responsible for directing and controlling all the academic operations in these institutions. In addition, the government could consider funding the research and development of ICTs research specializing in ICT and e-safety as well as include them in National School Syllabus for the whole country than each school producing their own interventions. Considering that the government is the employer of all teachers, it can add ICT specialists in schools if necessary. If excluded, there will be no ICT specialist in certain schools especially those without good financial footing to pay for the extra teachers employed. Further future work could consider testing the framework for usability and improvement.

Acknowledgements I thank the anonymous reviewers for their helpful comments

Author contributions All authors read and approved the final manuscript.

Funding No outside funding was used to support this work.

Availability of data and materials The authors declare that [the/all other] data supporting the findings of this study are available within the article.

Declarations

Conflict of interest The authors declare that they have no conflict of interest

References

Alnesafi, A. (2018). Blended learning and accounting education in Kuwait: An analysis of social construction of technology. *Academy of Accounting and Financial Studies Journal, 22*(3), 1–19.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security, 2009*(7), 13–19.

Barros, M., & Lazarek, H. (2018). A cyber safety model for schools in Mozambique. Paper presented at the ICISSP 2018. In: 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal

Bhukuvhani, C. (2017). Students' perceptions on the politics of mobile phones usage among learners. *International Open and Distance Learning Journal, 2*(2), 8–13.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. MIT press.

Bryant, V. R. (2013). *21st century youth using critical thinking skills and practicing cyber safety when making digital decisions: An analysis of the digital devices and decisions of youth and parental perspectives of the same*. Fielding Graduate University.

Camacho, S., Hassanein, K., & Head, M. (2018). Cyberbullying impacts on victims' satisfaction with information and communication technologies: The role of perceived cyberbullying severity. *Information & Management, 55*(4), 494–507.

Cao, F., Su, L., Liu, T., & Gao, X. (2007). The relationship between impulsivity and Internet addiction in a sample of Chinese adolescents. *European Psychiatry, 22*(7), 466–471.

Chung, K. (2004). Development of an integrated chat monitoring and web filtering parental control for child online supervision. (Computer Science Technical Reports; No. CSBU-2004-13). Department of Computer Science, University of Bath.

Cranmer, S., Selwyn, N., & Potter, J. (2009). Exploring primary pupils' experiences and understandings of 'e-safety.' *Education and Information Technologies, 14*(2), 127–142.

Creswell, J. W. (2015). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (5th ed.). Pearson.

Fisk, N. (2014). "… when no one is hearing them swear"-Youth Safety and the Pedagogy of Surveillance. *Surveillance & Society, 12*(4), 566.

Gamira, D. (2019). The Integration of ICT in geography in selected kadoma high schools, Zimbabwe. *i- Manager's Journal on School Educational Technology, 15*(1), 18.

Gcaza, N. (2018). *Cybersecurity awareness and education: A necessary parameter for smart communities.* Proceedings of the 12th International Symposium on Human Aspects of Information Security & Assurance, Dundee, UK, 29-31 August 2018, 80–90

Gomba, C. (2016). Transforming rural secondary schools in Zimbabwe through technology: Lived experiences of student computer users. *International Online Journal of Education and Teaching, 3*(2), 108–120.

Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence, 42*(5), 711–722. https://doi.org/10.1007/s10964-012-9902-

Jones, A., & Bissell, C. (2011). The social construction of educational technology through the use of authentic software tools. *Research in Learning Technology*. https://doi.org/10.3402/rlt.v19i3.17116

Katz, A. (2016). *Making your secondary school E-safe: Whole school cyberbullying and E-safety strategies for meeting ofsted requirements*. Jessica Kingsley Publishers.

Klebl, M. (2008). Explicating the shaping of educational technology: Social construction of technology in the field of ICT in education. *Readings in Education and Technology: Proceedings of ICICTE, 2008*, 278–289.

Livingstone, S., & Palmer, T. (2012). *Identifying vulnerable children online and what strategies can help them*. UK Safer Internet Centre.

Lorenz, B., Kikkas, K., Sõmer, T., & Laugasson, E. (2019). Cybersecurity within the curricula of informatics: The Estonian perspective. In S. Pozdniakov & V. Dagienė (Eds.), *Informatics in schools. New ideas in school informatics* (Vol. 11913, pp. 159–171). Estonia: Springer.

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). *Teens and technology 2013* (pp. 1–19). Pew Internet & American Life Project.

Mandina, S. (2015). Integrating ICTs into the environmental science primary school classroom in Chegutu district, Zimbabwe: Problems and solutions. *European Journal of Science and Mathematics Education, 3*(1), 90–96.

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2020). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy, 2020*, 1–11.

Maxwell, J. A. (2013). Qualitative research design: An interactive approach (3rd ed.). Thousand Oaks, Califonia 9132: SAGE Publications.

Ncube, A. C., & Tshabalala, T. (2016). An investigation into the challenges faced by secondary school teachers in integrating internet into the teaching and learning process in Zimbabwe: A case study of Harare Province. *Nova Journal of Humanities and Social Sciences, 3*(3), 1–21.

Ndhlovu, F. (2006). Gramsci, doke and the marginalisation of the Ndebele language in Zimbabwe. *Journal of Multilingual and Multicultural Development, 27*(4), 305–318.

Ngara, R. (2019). Barriers to the use of ICT by students on teaching practice: Student teacher and lecturer input. *Zimbabwe Journal of Educational Research, 31*(1), 1–12.

Ngwenya, B., & Pelser, T. (2018). Competencies, attitudes, acceptance and their impact on ICT diffusion in educational institutions in Bulawayo, Zimbabwe. *Progressio, 40*(1), 1–19.

Oates, B. J. (2007). *Researching information systems and computing*. Sage Publications India Pvt Limited.

Patchin, J. W., & Hinduja, S. (2018). Deterring teen bullying: Assessing the impact of perceived punishment from police, schools, and parents. *Youth Violence and Juvenile Justice, 16*(2), 190–207.

Selwyn, N. (2013). *Education in a digital world: global perspectives on technology and education*. Routledge.

Shillair, R., Cotten, S. R., Tsai, H.-Y.S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior, 48*, 199–207.

Šimandl, V., & Vaníček, J. (2017). Influences on ICT teachers knowledge and routines in a technical e-safety context. *Telematics and Informatics, 34*(8), 1488–1502.

Tennakoon, H., Saridakis, G., & Mohammed, A.-M. (2018). Child online safety and parental intervention: A study of Sri Lankan internet users. *Information Technology & People, 31*(3), 770–790.

Tomczyk, Ł, & Kopecký, K. (2016). Children and youth safety on the Internet: Experiences from Czech Republic and Poland. *Telematics and Informatics, 33*(3), 822–833.

Tsokota, T., Mahlangu, G., Rebanowako, T. G., & Furusa, S. S. (2017). *Can the social construction of technology be used to explain the perception of social media in Zimbabwe? Paper presented at the 11th Zimbabwe International Research Symposium, Harare, 16–17*. Research Council of Zimbabwe.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research, 26*(3), 399–409.