Education Tech Research Dev (2022) 70:639–655
https://doi.org/10.1007/s11423-022-10078-z

CULTURAL AND REGIONAL PERSPECTIVES

# A strategy to enhance e-safety among first-year students at Zimbabwean universities: an action research

**Theo Tsokota**[1] · **Vurayai Mhloza**[2] · **Colletor Tendeukai Chipfumbu-Kangara**[1]

Accepted: 3 January 2022 / Published online: 19 February 2022


**Abstract**
The widespread use of ICT offers considerable opportunities to society. However, there is ample evidence that students are exposed to various e-Safety challenges and risks through the use of ICT. Most Zimbabwean students who are not adequately prepared for e-Safety are now entering universities and are thus exposed to the risks posed by ICT. Therefore, this action research developed a strategy to enhance e-Safety among first-year students in Zimbabwean universities. The overarching research strategy was action research, which used qualitative research methods to collect information on e-Safety, usage and risks students face, and how these risks can be mitigated. Data was collected using an online questionnaire, interviews, observation and netnography. The results showed that the understanding of e-safety issues is still in its infancy. Therefore, an e-safety strategy was formulated to clearly indicate *what to report, to whom and how* concerning safety. This strategy was based on the overall reflection of the research, which recommended that education plays a central role in e-safety, as perpetrators or victims may not be aware of the challenges of e-safety. Thus, this research contributes to the existing body of knowledge by providing a clear strategy for dealing with e-safety challenges in Zimbabwean universities. Furthermore, this research is important in understanding the future of ICT use in developing countries like Zimbabwe.

**Keywords** e-Safety · Strategy · Information and communication technologies

## Introduction and background of the research

Information and Communication Technologies (ICTs) are crucial and permeate all facets of the economy and impact every sector (Carvalho et al., 2015; Demirer, 2016). According to Hamelink (1997 p. 3), the term ICT—"encompasses all those technologies that enable the handling of information and facilitate different forms of communication among human actors, between human beings and electronic systems, and among

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

[1] Department of Information and Marketing Sciences, Midlands State University, P. Bag 9055, Gweru, Zimbabwe

[2] Mkoba Teachers College, P. Bag MK20, Gweru, Zimbabwe

electronic systems." The diffusion of ICT is becoming a key driver of global, regional and local socio-economic change. It is also a critical resource and an essential component of any economic activity (Kabanda, 2015). Moreover, ICTs can accelerate the foundation of any economic activity such as education, consumption, investment, government service delivery and export competitiveness (Jorgenson & Vu, 2016).

In the education sector, ICTs are shaping the future of education and learning (Schmid, 2016). ICT will largely contribute to achieving universal education through the delivery of education and the training of teachers, as well as providing improved conditions for lifelong learning. Such lifelong learning involves people outside the formal education process and thus improves professional skills (Nicholls, 2014). ICTs can improve critical thinking, information handling, conceptualisation, and problem-solving capacity (Liem et al., 2014). When used properly, various ICT help expand access to education and strengthen the relevance of education to the increasingly digital workspace. Furthermore, ICTs enhance educational quality by helping to make teaching and learning an engaging, activating process that is connected to real-life (Veletsianos & Kimmons, 2016).

Despite all the benefits of ICT, there are inherent challenges which include safety concerns. Safety in the use of ICT resources is often referred to as e-Safety. Vanderhoven et al., (2015 p. 286) define-Safety as encompassing "not only internet technologies but also electronic communications devices such as mobile phones and wireless technologies." Siyam and Hussain (2021) refer to e-Safety as a way of protecting children and young people from harm. e-Safety ensures that children and young people are supported to gain the maximum benefit from new and developing technologies without putting themselves or others at risk (Cilliers & Chinyamurindi, 2020). In a study by Williams and Pearson (2016) e-Safety is described as the school's ability to protect and educate students and staff in the use of technology. This includes having appropriate mechanisms in place to intervene and assist, if necessary, in the event of an incident.

It highlights the need to educate students and young people about the benefits, risks and responsibilities of using information technology. Thus, e-Safety protects and raises awareness so that users can control their online experiences. Therefore, e-Safety education and awareness should be raised to improve the behaviour of people using the internet.

In Zimbabwe, schools and pre-university colleges have not allowed their students to bring electronic mobile devices to school (Bhukuvhani, 2017). Therefore, these schools and colleges ignored the fact that students had access to electronic devices after school and at home without any guidance from parents or teachers. Inevitably, some parents were ill-prepared and unaware of the activities done by their children while using electronic devices (Nani & Sibanda, 2020). Students were left on their own without guidance. They were at risk of suffering negative consequences from the use of these electronic gadgets. Teachers and education administrators focused on developing strict policies and procedures to keep mobile devices out of the education system rather than developing comprehensive strategies that integrated Information Technologies into the teaching and learning process (Kahari, 2013).

Nonetheless, students have become more involved in using Information and Communication Technologies such as social media networks and other online activities than in the past. It is therefore important that e-Safety is promoted in universities. When ICT is used without proper guidance, it poses a risk to users and other students. Therefore, the responsible and meaningful use of ICT devices must be consciously and carefully cultivated. Students should be educated about the dangers of ICT and how to protect themselves online (Vanderhoven et al., 2015).

On the other hand, most parents in Zimbabwe lack knowledge on how to use, monitor and give guidance on the use of electronic devices compared to their children (Nani & Sibanda, 2020). In most circumstances, parents and guardians do not understand their children's cyber activities (Bryant, 2013; Chung, 2004). As a result, this often leads to additional concerns because parents and guardians do not have the education and expertise to protect their children and keep them safe from online predators (Fisk, 2014). At the same time, schools that were supposed to impart cyber skills, knowledge, and behaviour, commonly referred to as netiquette, were busy denying students access to use electronic devices within school grounds (Bhukuvhani, 2017). As a result, schools neglected their duties and responsibilities to parents who, in most cases, were not knowledgeable about e-safety issues. As a result, most students may not have developed the right cyber skills, knowledge and behaviour in using the internet, which is increasingly becoming an important life skill in any society (Stavrou, 2020). Thus, most Zimbabwean students enter universities without adequate e-Safety preparation and are thus exposed to the risks posed by ICT. Compounding the problem is that students entering universities are further exposed to intensive use of ICTs as university learning is, by its very nature, research-intensive. In addition, the demand for ICT has increased due to the recent outbreak of COVID 19, which now requires online teaching and learning. Thus, making ICT an integral part of every university student.

Consequently, the number of ICT users has increased, exponentially increasing the risks associated with the internet and the need for proper e-Safety education and strategy. Thus, it is no longer a question of whether technology should be integrated into schools but how it should be done safely to benefit all stakeholders in a typical school or university setting. e-Safety education is an essential component of cybersecurity education (Zhang-Kennedy & Chiasson, 2021). Tomczyk and Kopecký (2016) state that schools, universities and teachers should raise e-Safety awareness among students and young people rather than other stakeholders. Against this background, the main objective of this research was to develop an e-Safety strategy for first-year students in Zimbabwean universities. To achieve the research objective, four research questions are raised: (1) What is the current awareness level of e-Safety of first-year students in a state university in Zimbabwe? (2) What are the experiences and perceptions of first-year students in a state university in Zimbabwe? (3) Which elements constitute an effective e-Safety strategy for first-year students in universities in Zimbabwean? (4) How can e-Safety be effectively achieved among first-year students at universities in Zimbabwe?

This paper first presents the background and introduction to the research. The following section looks at the research methodology that was used in conducting this research. It then presents the context of the study and the pre-intervention phase. The discussion of the findings is followed by the proposed strategy for e-Safety in Zimbabwean Universities and the conclusion.

## Methodology

The overarching methodology for this research was an action research approach. Action research is defined as a form of collective self-reflective research conducted by respondents in their social or educational practices, beyond the understanding practice (Herr & Anderson, 2014). Action research requires collaboration. However, it can only be achieved by investigating the actions of individual group members. Therefore, Action research

can be considered as teacher-initiated and school-based research. This definition agrees with Coghlan and Brannick (2014) who argue that by doing or changing something, the researcher becomes the focus and centre of the research. The main aim of action research in education is to engage educators in improving their classroom practices by critically examining their practice and changing their long-held beliefs and perceptions. Therefore, some educators are involved in researching their students, classrooms and schools, which was the case in this research.

Action research was deemed necessary for this research for two reasons. Firstly, it creates an environment or situation where researchers and students work together to overcome the challenge of a lack of e-Safety awareness. Secondly, the research required a systematic approach that involved careful planning. Accordingly, the researchers had to develop an action plan, act on it, observe and reflect on the observation results. This process was iterative, after which a strategy was then be formulated. In this research, e-Safety relates to the safe and responsible use of information communication technologies (ICTs), including computers, the internet, mobile, and communication technology devices and technology tools designed to hold, share or receive information such as mobile phones, digital cameras and pagers.

The Zimbabwean education sector does not have e-Safety strategies and could therefore learn from other sectors where safety is important and entrenched, such as the mining sector. For this reason, the study collected data on safety issues from a mining company in Zimbabwe. The rationale was to use this knowledge to inform e-Safety strategies in the education sector as the local mining sector has well-established safety strategies. While the mining company, like other mining companies, emphasises safety in general, the objective was to find ways in which the education sector can adapt and build e-Safety strategies to suit its circumstances. In general, given the high risks associated with the mining environments and operations, mining companies' safety strategies can be considered best practices for e-Safety. The mining sector was also identified as one of the industries that generally promote safety awareness within their community. Therefore, with the help of Action research, the research was able to gather knowledge from a mining company to adapt safety concepts, especially on how they impart safety awareness to their employees.

The reason for this, as mentioned earlier, was that mines have extensive safety programmes. Therefore, the education sector could learn from their strategies and possibly adopt them for university settings. Furthermore, both universities and mines are mainly made up of adults, and a lack of safety in any area can have a negative impact on many people. Consequently, safety deficiencies in all areas of the organisation negatively affect the reputation of these institutions. Therefore, data was collected from a mining company on how it promotes safety awareness and teaches safety to its employees. The use of mining company data was done to inform the university on how it could apply e-safety in its context.

As experienced lecturers teaching an introductory Information Technology course, the researchers designed a teaching topic on e-Safety for two first-year Programme X classes (identified as Conventional and Parallel classes). At the target university, the conventional students were the students enrolled on the regular degree programs. On the other hand, parallel students were full-paying students who conducted their studies after hours and on weekends. At the time of the research, these students were not eligible for government grants. Through conversations with students during and after lectures and observations. It was established how some students used technology to cause harm to others. Two WhatsApp groups were set up for the two classes to improve data collection from targeted university students.

The objective was to identify the safety issues associated with the use of ICTs without adequate training. It was hypothesised that lack of e-Safety awareness could cause harm to students themselves and their peers who ridicule them or lead them to spend more time on non-educational activities.

For ethical reasons, the identity of the mine and its staff, the university, the students and their programme of study were kept secret. This was done in an effort to protect identities and avoid personal harm, conflict, bias or interest. This research employed research instruments such as an online questionnaire, observations, interviews, and netnography, which are briefly explained in the following subsection.

## Instruments

The Action research involved various data collection instruments in capturing the factors that influence e-Safety. It also required triangulation of research methods. Triangulation was achieved through the use of online questionnaires, observations and netnography and their results.

## Online questionnaire

Based on the critical components of e-Safety, the researchers administered 172 online questionnaires to first-year Program X class undertaking a module titled Introduction to Information Technology which is part of their program. The purpose of the questionnaire was to determine the student's awareness of e-Safety issues. Two *WhatsApp* groups were also set up with the researchers as co-administrators to collect data. *WhatsApp* is the most popular social media platform among university students in Zimbabwe. The students were grouped based on their respective classes and *WhatsApp* groups, which were named "Conventional Programme X and "Parallel Program X Class", respectively. Although they study separately, the same curriculum is taught by the same lecturers in these classes, with the Parallel class acting as a control class.

Therefore, the online questionnaire was designed to collect information from the students. (Cohen et al., 2017) state that the appearance and layout of an online questionnaire is significant. They also say that it must be attractive and eye-catching. Following Cohen et al. (2017) the questionnaire avoided compressing and being cluttered as this would make the instrument uninviting, thereby discouraging respondents. The questionnaire then provided ample space for questions and answers to attract and engage respondents.

Moreover, it was designed after a detailed review of the literature. Furthermore, the questionnaire firstly captured the demographic data of the respondents. Secondly, it attempted to identify the level of awareness and more importantly, the e-Safety risks faced by the students.

In order to entice respondents to complete the questionnaire and in so doing generate a high response rate several measures were taken. A cover letter was attached, guaranteeing the respondents that their responses would only be used for academic purposes and that their identities would not be associated with their responses in any way (Dörnyei, 2014). To allow respondents to provide additional comments, free space was provided at the end of the questionnaire for further comments that would contribute to the research. The questionnaire was posted online at https://www.esurveyspro.com/Survey.aspx?id=6a8c5da8-0f77-40ae-814e-bd8f8e24f944. The link to the questionnaire was also sent through the

*WhatsApp* platform, e-mailed to students, and sent through their e-learning platform. The questionnaire is attached as an appendix.

### Observations

Observation involves the systematic recording, description, analysis and interpretation of human behaviour (Saunders et al., 2015). Observational techniques typically generate additional data, enable cross-checking and corroborate or challenge data from other data collection methods. At the same time, observations can capture events that cannot be represented on paper, such as physical locations, cause-and-effect, interactions and the operations of organisations. The primary goal of observation was to obtain first-hand information to understand what was going on rather than what people reported. In this research, the questionnaire enabled the researchers to determine how the ICT devices were used by the university students involved. Observations were used in an iterative cycle by combining data from a variety of sources. It was also important to observe things that did not emerge from the questionnaire or literature in order to achieve triangulation. In addition, WhatsApp usage patterns and student behaviour were also observed.

### Interviews

Interviews are guided, purposeful conversations between two or more people in which the interviewee(s) are questioned in a structured, in-depth, semi-structured or unstructured manner (Yin, 2017). Semi-structured face-to-face interviews were used for this research, following Saunders et al. (2015) who note that interviews contain a list of topics and questions to be covered and questions can be added or omitted from interview to interview. The main advantage of semi-structured interviews was that specific answers could be given to specific questions. This was very useful given the limited time available to the researchers. Thus, face-to-face, semi-structured interviews were conducted to find out how mining companies impart safety awareness to their employees. Interviews were also conducted with three Safety, Health and Environmental officers of the mine concerned. In addition, a Departmental Manager and six workers from different departments were interviewed. The interviews focused on how the mine in question handles safety and imparts safety awareness to its employees, as mines are known to have a strong safety consciousness (Jo & Khan, 2017). Therefore, the main interview questions were: how do mining companies inculcate safety awareness amongst their employees? What are the consequences of non-compliance with safety measures put in place by the company?

Research in Zimbabwe is very difficult, especially when private organisations are involved (Mazango, 1998). Takavarasha et al. (2011) also state that research in Zimbabwe can be very risky because one can be mistaken for a journalist, spy or activist in disguise. These difficulties were anticipated, but researchers managed to obtain permission from an international platinum mining company with a subsidiary in Zimbabwe. Thus, access was granted to conduct research at the mine in question.

### Netnography

Kozinets (2016) defines netnography as a novel, innovative and unobtrusive qualitative research methodology that applies and adapts ethnographic research techniques to the study of computer-mediated communication. Mkono (2017) argues that the rapid development of

social networking technologies has led to internet users posting messages, reviews, compliments, complaints and comments on message boards. Researchers took advantage of these message boards as they provided fertile ground for data posted inconspicuously and anonymously. This information allowed researchers to accurately understand users' thoughts, opinions, motivations and concerns (Massa, 2013). Moraes et al. (2014) note that the use of pseudonyms and the anonymous nature of online interactions allow for unsolicited comprehensive, rich and candid accounts of internet users. Compared with other qualitative data collection methods, netnography was favoured as less time consuming, unobtrusive and generally less costly (Lynch & Mah, 2017).

Therefore, the research used netnography as part of a non-participant observation technique to triangulate the data from the questionnaires completed by the respondents. The main reason for choosing non-participant observation was so that the researchers could understand the *WhatsApp* messages posted by the students on the class *WhatsApp* platforms. It was not possible to obtain permission from the University to open a social media platform for the classes. Accordingly, the comments on *WhatsApp* complemented the data obtained from the questionnaires.

### Triangulation

This research used different data collection methods commonly referred to as data triangulation. Data triangulation involves using different data collection methods to study a phenomenon in different ways (Tunarosa & Glynn, 2017). It allows the results of one data collection method to be validated or compared to the data from another method. Triangulation was therefore beneficial because it provided multiple perspectives on a phenomenon. It also provided more information about emerging concepts, allowing for greater authentication of a phenomenon (Venkatesh et al., 2016). Action research allows for a variety of data collection methods which helps to test the dependability of findings. Triangulation therefore became relevant in this research as results from a variety of data collection methods were used to support the findings.

## Context of the study and pre-intervention phase

This research was conducted in Zimbabwe, a developing country that is currently recovering from a decade-long economic recession. In addition, this country has been implementing educational reforms. There has been a controversial debate and various solid views on whether schools should allow the use of mobile ICT devices (Bhukuvhani, 2017; Chidavaenzi, 2015). A former ICT Minister and leader of the country's largest opposition party once compared the use of mobile devices by students to the promotion of terrorism (Gweshe, 2015). Traditional leaders have argued that the use of mobile devices by students would lead to moral decay (Murwira, 2015).

On the other hand, some educators are pushing for the introduction of ICT devices in schools (ZimTechReview, 2019). It is against this background that most Zimbabwean students who were denied access to electronic devices in high schools and colleges are now going to universities. In addition, some students from resource-constrained environments who had little or no access to ICT devices are also entering universities. These students will have more access to the internet and ICT devices without having been adequately

trained in netiquette and proper use of ICT in high school and thus exposed to risks posed by ICT. These risks include disruption, behavioural problems, theft and cyberbullying.

Consequently, something could be done to curb abuse and protect students. Therefore, the objective of this research was to develop a strategy to enhance e-Safety among first-year university students. To achieve the above research objective, the Action research method was used. Action research is qualitative, cyclical, participatory and reflective (Herr & Anderson, 2014). Action research also suggests four linear but iterative steps for conducting research. These four steps include planning, acting, observing and reflecting (Stringer, 2013).

The planning process allows for the identification of the target population. It determines the data sources and sample selection. Since this research addressed safety issues, it was prudent to identify and draw on best practices in promoting safety amongst adults, especially in safety-intensive industries in Zimbabwe. Consequently, the mining industry was identified as the most appropriate industry (Jo & Khan, 2017). Once identified, the best safety practices were applied in teaching e-Safety in Zimbabwean universities. Accordingly, the aim of this research was to find out whether the safety awareness strategies used in the mining industry can be adopted in promoting e-Safety in universities.

## Results

A total of 159 out of 172 questionnaires were completed. This represents 92% of the respondents. There were no differences in the results between Conventional and Parallel students. Some of the responses to the question of how they would react if they received a text, e-mail, photograph, video, comment or tagging that was humiliating were:

> I will retaliate if I know the person, but if I do not, I will just keep quiet. R3.

Another answer was "*I will be angry*" R4 and went further to say, "*I will be hurt and unfriend the person*". To the same question, another response was "H*mmm, it depends on your relationship with that person…if you are close to them, I do not think it is wrong… but if u don has such a relation, it is wrong" R107.* A total of 60 respondents simply wrote simply *"ignore",* and 20 respondents said *"delete immediately".*

> When asked why they would take a video or take photos with their mobile phones while a group laughs and forces another person to do something humiliating or ridiculous, the other responded, "Good memories" R138. Another response was, some people deserve it. It's a tit for tat kind of thing. Suppose you humiliate me in the real world. In that case, it is much easier to resort to online retaliation as it is easier and much more effective. R115.

The results of the questionnaire revealed that 133 out of the 159 respondents, that is 83% of the respondents had suffered or caused someone to suffer from at least one e-Safety problem. This confirms that e-Safety problems are rampant at the state university. Students openly abused cyberspace by using ICT devices and social networking sites to torment fellow students. Most of the respondents did not know how bad the situation was as the person suffering from the e-Safety challenge was known only to those invited to a particular group in a particular cyber forum. The *WhatsApp* group showed similar results for the 651 messages in the first period. All messages were considered appropriate and relevant.

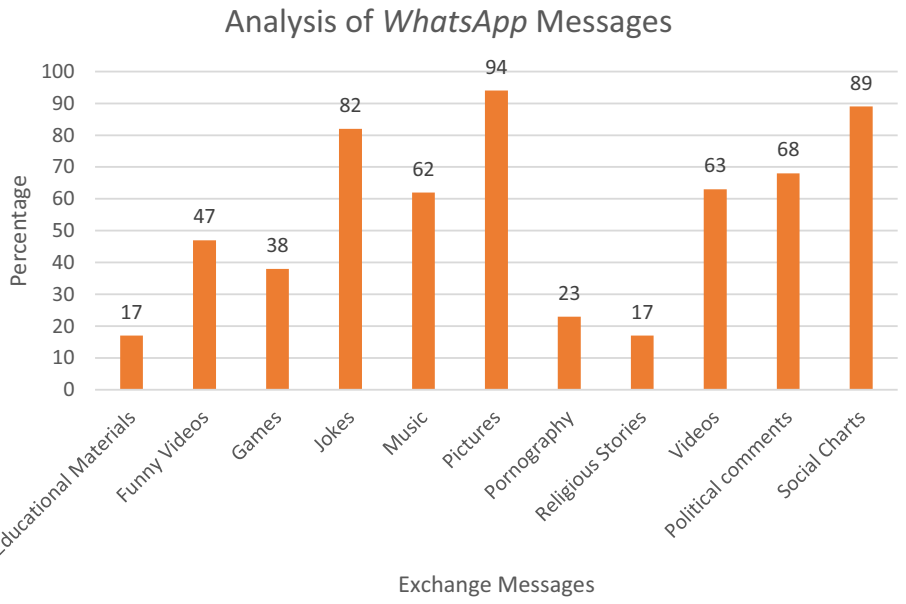
Therefore, these messages were qualitatively analysed following Creswell (2009). Different themes were identified from the messages, extracted and coded in a spreadsheet. The frequency of each theme was summed up and converted into a percentage for each of the categories. In this way, the following themes were identified: educational materials, funny videos, games, jokes, music, pictures, pornography, religious stories, political commentary and social charts. Several iterations ensured that the identified themes were accurate and complete. The analysis of WhatsApp messages is shown in Table 1. Interestingly, only 17% of these messages were related to academic work.

## Results and reflections

The research results showed that the awareness of e-Safety among university students was indeed low. There was a need for an e-Safety strategy as most students spend most of their time on non-educational content. It is also unfortunate that the volume of messages suggests a high level of addiction to social media. This is in line with the findings of Kritzinger et al. (2019) who argue that many citizens are unaware and unprepared for the challenges of e-Safety. In addition, a lot of music is sent, indicating a lack of appreciation of intellectual property rights.

A high number of pictures also indicates the vulnerability to cyberbullying as well as pictures that ridicule people in some regions of Zimbabwe and causing regional and tribal tensions. Having established that e-Safety awareness among the students is indeed low, there was a need to establish how other sectors that require a high level of safety deal with safety challenges. This led to the second activity to find out how the mining sector deals with e-Safety challenges.

**Table 1** Analysis of WhatsApp messages



After analysing findings from the mining industry where safety is considered critical, the researchers taught the conventional class on e-Safety. The lessons included definitions of e-Safety issues, risks and impact on victims. The lectures also included active participation and heated class discussions. A total of three students privately expressed shock at unintentionally bullying and vilifying others. Five students reported having been victims of sexting and harassment, and they were grateful for the lectures. The next step was to appoint peer educators who were selected to act as contacts for those who suffered from e-Safety challenges. Five students were selected from the group –two male and three female. These students had received peer education and counselling training from the university and knew how to handle sensitive information. The peer educators also had access to university authorities.

In the Conventional class, the number of messages in the *WhatsApp* group decreased by 60% after class and was mainly about school. Students who continued to send messages that were deemed inappropriate were reprimanded by their classmates, indicating that the "brother's keeper" concept had borne fruit. In the Parallel class, which served as the control group, there was no change. Members did not reprimand each other for offensive and inappropriate messages.

On the other hand, peer educators reported a total of 24 cases setting, harassment, denigrating and cyberbullying to the university administration. The increase in the number of reports was directly attributed to a clear reporting structure. Some students also made comments:

> It's very wrong because once it's on the Internet, the whole world knows what happened and a person's right to privacy would have been violated and it's against the law. R42.

The lectures that were given to the Conventional class were also given to the Parallel class. The same structure of a reporting structure was immediately created. Surprisingly, the results were the same: a massive 70% decrease in *WhatsApp* messages and a 79% increase in education-related content. Insults, disparaging and denigrating messages were reduced by 87%. Respondents would now restrain and reprimand each other to stop disparaging or bullying others. One such comment advised colleagues against denigrating people from Masvingo, one of the ten provinces in Zimbabwe. The other comment was made by one of the respondents after the presentation of the lesson to the Parallel class:

> My suggestion is that something needs to be done to combat online bullying through awareness campaigns, whether in school or wherever because it has degrading effects on a person's social being and can even lead to preventable deaths. I firmly believe that it starts with me, you and us. Thank you for the informative lessons. I enjoyed them. They were very informative. R50.

It was clear from the questionnaire that education and clear reporting structures are vital to raise awareness of e-Safety. Students agreed that victims of e-Safety suffer in silence and therefore called for critical interventions with a clear reporting structure. Victims suffering in silence is consistent with the findings of Vanderhoven et al. (2013) who argued that victims of e-Safety challenges often suffer in silence. In other words, education and a clear reporting structure must be explicit about what needs to be done by whom and how. Accordingly, education and promotion of what constitutes e-Safety and what needs to be done to promote e-Safety must be provided. Providing a reporting structure can actually help victims of e-Safety problems. Victims will know what to report, who to report it

(whom) and how to report it, and they will be reassured that their problems will be listened to and resolved.

## Post-intervention phase

The purpose of this research was to develop with an e-Safety strategy for first-year university students. The assumption is that the Ministry of Primary and Secondary Education does not adequately support students in the use of mobile ICT devices as they are used without guidance. As a result, most parents are unaware of or do not know how to deal with e-Safety problems. As an intervention, research was conducted with 159 participants. Using an online questionnaire, data was collected from first-year students at a state university in Zimbabwe. To put the research in perspective, interviews were conducted with representatives from a platinum mine. The rationale was to identify safety challenges, promote safety awareness and develop appropriate strategies.

Netnography on WhatsApp messages was also used to triangulate the results and it was found that only 17% was being used for academic work. The other uses were jokes, forwarding and insults. There was a significant improvement after an educational intervention to increase e-Safety awareness, as evidenced by 58% of the control group results. The e-Safety promotion strategies used in mining were found to be very useful in promoting e-Safety. These strategies included education and the "brothers" keeper. Education and the "brother's keeper" strategy were thus indeed useful in addressing the challenges of e-Safety. The following section looks at the discussion and reflections that emerged from the research.

## Discussion

Lack of awareness was the main cause of e-Safety problems. This is consistent with the views of scholars such as De Kimpe et al. (2019) who argue that most e-Safety problems are due to a lack of knowledge. Interventions implemented through education helped raise awareness of e-Safety issues for which help could be sought. The increase in awareness is in line with the views of scholars such as Tomczyk and Kopecký (2016) that awareness and education play a crucial role in empowering victims of e-Safety.

The results of the questionnaires, and netnography, show that the first-year students had low awareness of e-Safety issues. The university did not have proper mechanisms to intervene and support victims of e-Safety problems, as 83% of the respondents had suffered or caused someone to suffer from at least one e-Safety problem. Lack of intervening and support strategies can negatively affect students and the people they interact with. This view is supported by Gcaza and Von Solms (2017) who argue that e-Safety can affect a large number of people through the irresponsible use of ICT by one person. After the educational interventions, there was a marked improvement in the students' actions, as they were more responsible with using technology. This is in line with the views of Vanderhoven et al. (2013) who also argue that education is crucial in promoting e-Safety.

After implementation in the Conventional class, the results showed improved and more responsible use of ICT devices. Improved and more responsible use of ICT devices was also confirmed by the results of the control group which also showed improvement in the responsible use of ICT devices. After raising awareness, respondents were also

observed to help their peers by reprimanding them. The respondents acted as "brother's keepers". Consequently, after awareness, respondents succeeded in working together and helping each other to be e-Safe. These efforts can only be successful if they are supported and encouraged by the university through clearly defined policies. Moreover, the number of reported cases increased after a clear reporting structure was established. Reported cases were a sign of confidence in the reporting medium and assurance that their complaints would be resolved. The medium of reporting included telephone calls, e-mails, letters, suggestion boxes and personal visits. This is in line with what Gcaza and Von Solms (2017) refer to as robust stakeholder engagement and empowerment of victims to report. In addition, reported cases could be resolved in various ways, such as punishments and escalation of issues to higher authorities where appropriate.

The first minor research objective was to examine the current e-Safety awareness, experiences and perceptions of first-year students in Program X at a state university in Zimbabwe. Results revealed that there was low initial awareness of e-Safety and its problems. Most students seemed to be unaware of the e-Safety issues. Another minor research question that contributed to answering the major research question was how e-Safety could be effectively achieved. This question was effectively answered by the strategy shown in Fig. 1.

This research helped in developing a strategy to address the challenges of e-Safety challenges. In addition, this research provided an opportunity to motivate students to address e-Safety problems and reflect on their behaviour. Students became aware of the dangers that ICT poses to themselves and others and thus became responsible citizens.

A clear reporting structure and the use of peers were quite effective in helping respondents deal with e-Safety challenges. Education about e-Safety can take various forms such as lectures, competitions, awareness campaigns, discussions and other relevant methods. In addition, this research has also helped to identify key stakeholders in safety education. These may include university authorities, peers and other stakeholders who interact with students online and offline. The proposed strategy for e-Safety in Zimbabwean universities is presented in the next section.

| | **Stage 1** | **Stage 2** | **Stage 3** | **Stage 4** | **Stage 5** |
|---|---|---|---|---|---|
| **What** | Education | Clearly defined Policy | Clearly defined friendly alerts/communication ways | Clearly defined response | Complaints Resolution |
| **Who** | University<br>Peers<br>Other Stakeholders | University | University | University | University<br>Complaints Resolution |
| **How** | Lectures<br>Competitions<br>Awareness-campaigns<br>Other relevant methods | Craft comprehensive-safety policy | Phone<br>E-mails<br>Letters<br>Suggestion box<br>Personal visit | Clearly defined contact person with known designation and responsibility.<br><br>Representative and knowledgeable complaints committee | Resolving<br>Recommending<br>Punish<br>Escalate the problems to higher offices where necessary |

**Fig. 1** Strategy for e-Safety for universities in Zimbabwe

## Proposed strategy for e-safety in Zimbabwean universities

In order to propose an e-Safety strategy for Zimbabwean universities, it was necessary to refer to findings obtained from the operations of a studied mine on safety issues. Findings from the mine revealed that each employee is adequately briefed before they are allowed to perform their duties for which they were hired. Observation revealed that the mine has a clearly defined safety, health and environmental department. It was also reported that the mine has a clear reporting structure for safety-related incidents. From the interviews, it was observed that the philosophy of the mine is that safety does not discriminate on the basis of status or employment position. This was noted as a driving aspect of safety awareness and programmes in all areas of the mine.

It was also reported that the concept of "brother's keeper" is applied in the mines, meaning that everyone is responsible for reminding, admonishing, warning or persuading their peers on safety issues. It was also revealed that the mine has a deterrent mechanism in the form of a bonus cut if a safety violation occurs within a certain period. In addition, the person responsible for a safety violation is either fined, reprimanded or even dismissed. Such measures were seen as helpful in maintaining sound safety policies, thereby conditioning actions and behaviours that respect safety issues within the mine. It has been reported that harm can be severe, resulting in disability, loss of life, property damage, or all of the above.

It was also noted that the mine regularly conducts training on safety issues, which shows that education is critical in promoting safety awareness. In the event of a safety violation, there is a clear reporting structure that is easy to use and follow. In addition, the principle of "everyone is his brother's keeper" was presented as a clear reminder to protect peers. It was also observed that posters were strategically placed within the mine site and in the surrounding areas outside the mine as a constant reminder to adhere to safety-related issues. It was also noted that contests and rewards for safety compliance, as well as educational programmes or safety awareness campaigns conducted by the mine from time to time, further reinforced the mine's safety programme. Ultimately, the message was that the responsibility for safety lies with each member, who is also responsible for the safety of the other members. In terms of the findings at the state university, it is clear by comparison that there is no e-Safety strategy for university students.

Based on the above, an e-Safety strategy for university students in Zimbabwe is therefore proposed. This strategy is based on the overall reflection of the research, which recommended that education is central to e-Safety as perpetrators or victims maybe not aware of e-Safety challenges. The strategy has been formulated to make clear *what to report, to whom and how* in relation to e-Safety. Figure 1 presents this information graphically and explains it in detail.

The proposed strategy is based on the key finding that university students studied lacked sufficient knowledge about e-Safety. Accordingly, the proposed strategy is rooted in education as a key component of e-Safety, as shown in Fig. 1. There is a need to educate students on e-Safety issues. E-Safety is a multi-disciplinary issue that involves universities, students, peers and other relevant stakeholders throughout the educational process. The educational process needs to be conducted through various methods such as lectures, competitions, awareness campaigns and others. It is important to use a variety of methods to ensure that every student understands the e-Safety issues.

The university needs to establish a clear policy on e-Safety. During the research, it was found that students were not aware of any clearly defined e-Safety policy. Therefore, the policy needs to be comprehensive enough to cover all forms of e-Safety problems. The

research found that the number of reported incidents increased dramatically after a clearly defined communication procedure was put in place. This strategy therefore requires a variety of communication channels and contacts for e-Safety issues. These channels include e-mails, letters, telephone calls, personal visits and suggestion boxes. Students need to feel comfortable and confident in the reporting system if they are to report their issues. This tallies with the recommendations of Alfano and Huijts (2018) who argue that trust in governance institutions increases the willingness of citizens to report their queries.

If the strategy is to be successful, students must have confidence that their issues will be resolved. There must be a variety of committees with clearly defined mandates at different levels of the university to address such issues depending on the severity of the e-Safety problem involved. It is also important to note that there must be a committee as university governance in Zimbabwe is based on committees. The respective committees must have the power to resolve issues, recommend solutions or refer the complaints to higher authorities in the university or national bodies such as the police for further redress.

## Conclusion

The results showed that there was an embryonic understanding of e-Safety issues among first-year university Zimbabwean students. Consequently, education is a key element of e-Safety as some perpetrators or victims were not aware of the problems of e-Safety. Lack of awareness was therefore, the main cause of e-Safety issues. As a result, most respondents had at least one e-Safety problem or had caused someone to suffer from an e-Safety problem. The perpetrators did not know that what they were doing was wrong.

e-Safety requires a concerted effort from all involved. Therefore, educational interventions and awareness raising can significantly assist in improving e-Safety. Thus, the research has shown that education and clear reporting structures are crucial to enhance e-Safety awareness. This is because victims are more likely to open up if they know *what to report, who to report it to, how* to report it, and trust that their issues will be heard and resolved. Any e-Safety strategy to be formulated must clearly identify *what, who and how* to report when it comes to e-safety.

The research proposed a strategy based on the overall reflection of the research, which recommended that education is central to e-Safety as perpetrators or victims may not be aware of the challenges of e-Safety. Therefore, this research contributes to the existing body of knowledge by providing a clear strategy for addressing e-Safety challenges in Zimbabwean universities. Furthermore, this research is important in understanding the future of ICT use in developing countries like Zimbabwe. It has also empirically shown that strategies from comparable situations can be applied to classroom situations. Therefore, universities should ensure that students are e-Safe by continuously implementing e-Safety strategies.

This research has also helped to understand better e-Safety in developing countries based on empirical research that draws on the experiences of students and lecturers. In addition, it has suggested an appropriate e-Safety strategy that can be implemented based on the real experiences of students and lecturers. The researchers also hope that the students who participated in this research have gained valuable information that they can apply in their lives and improve their well-being and that of others.

The research has also shown the effects of not introducing students to the use of ICT in primary and secondary schools and the effects of not integrating ICT into the classroom

at an early age. As a result, they already know about technology by the time students complete their secondary education. However, they do not exhibit acceptable behaviour when they use it. Therefore, policymakers and curriculum developers can take appropriate interventions.

Further research could explore the possibility of extending this research to other universities, polytechnics and Teachers Colleges. Further research could also be conducted to test the strategy in a real-world setting. This is important to examine the transferability of the findings to other countries in the same context and technological situation as Zimbabwe.

**Supplementary Information** The online version contains supplementary material available at https://doi.org/10.1007/s11423-022-10078-z.

**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.

**Data availability** 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 competing interests.

## References

Alfano, M., & Huijts, N. (2018). Trust and distrust in institutions and governance. *The Routledge Handbook of Trust and Philosophy.* Routledge Taylor & Francis Group.

Bhukuvhani, C. (2017). Students' perceptions on the politics of mobile phones usage among learners. *International Open and Distance Learning Journal*. https://doi.org/10.1108/PRR-03-2018-0007

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.

Carvalho, J., Francisco, R., & Relvas, A. P. (2015). Family functioning and information and communication technologies: How do they relate? A literature review. *Computers in Human Behavior, 45*, 99–108.

Chidavaenzi, P. (2015). Cellphones in schools: storm continues to gather. Retrieved July 31, 2021, from https://www.newsday.co.zw/2015/03/cellphones-in-schools-storm-continues-to-gather/

Chung, K. (2004). *Development of an integrated chat monitoring and web filtering parental control for child online supervision*. University of Bath.

Coghlan, D., & Brannick, T. (2014). *Doing action research in your own organisation*. Sage.

Cohen, L., Manion, L., & Morrison, K. (2017). *Research methods in education*. Routledge.

De Kimpe, L., Walrave, M., Ponnet, K., & Van Ouytsel, J. (2019). Internet safety. *The international encyclopedia of media literacy* (pp. 1–11). Wiley.

Demirer, V. (2016). Information and communication technologies. *Instructional process and concepts in theory and practice* (pp. 493–523). Springer.

Dörnyei, Z. (2014). *Questionnaires in second language research: Construction, administration, and processing*. Taylor & Francis.

Fisk, N. (2014). "…When no one is hearing them swear"-Youth safety and the pedagogy of surveillance. *Surveillance & Society, 12*(4), 566.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries, 80*(1), 1–17.

Gweshe, E. (2015). Dokora creating ground for terrorism: Chamisa. Retrieved July 31, 2021, from https://www.newsday.co.zw/2015/02/dokora-creating-ground-terrorism-chamisa/

Hamelink, C. J. (1997). *New information and communication technologies, social development and cultural change. UNRISD discussion paper* (Vol. 86). United Nations Research Institute for Social Development.
Herr, K., & Anderson, G. L. (2014). *The action research dissertation: A guide for students and faculty*. SAGE Publications.
Jo, B. W., & Khan, R. M. A. (2017). An event reporting and early-warning safety system based on the Internet of things for underground coal mines: A case study. *Applied Sciences, 7*(9), 925.
Jorgenson, D. W., & Vu, K. M. (2016). The ICT revolution, world economic growth, and policy issues. *Telecommunications Policy, 40*(5), 383–397.
Kabanda, G. (2015). Pedagogic possibilities of ICTs and technology affordances in an increasingly networked environment in support of sustainable development. *Journal of African Studies and Development, 7*(5), 126.
Kahari, L. (2013). The effects of cell phone use on the study habits of University of Zimbabwe first year faculty of arts students. *International Journal of Education and Research, 10*, 1–12.
Kozinets, R. V. (2016). *Netnography: Understanding networked communication society. The SAGE handbook of social media research methods*. Sage.
Kritzinger, E., Loock, M., & Goosen, L. (2019). Cyber safety awareness-through the lens of 21st century learning skills and game-based learning. *International conference on innovative technologies and learning* (pp. 477–485). Springer.
Liem, G. A. D., Martin, A. J., Anderson, M., Gibson, R., & Sudmalis, D. (2014). The role of arts-related information and communication technology use in problem solving and achievement: Findings from the programme for international student assessment. *Journal of Educational Psychology, 106*(2), 348.
Lynch, M., & Mah, C. (2017). Using internet data sources to achieve qualitative interviewing purposes: A research note. *Qualitative Research, 18*, 741.
Massa, F. G. (2013). *Insurgency on the internet: Organising the anonymous online community*. Boston College.
Mazango, E. (1998). *Telecommunications sector reform: Liberalisation and universal service policy in Zimbabwe*. University of Oslo.
Mkono, M. (2017). Netnography: Redefined. *Tourism Management, 59*, 106–107.
Moraes, C., Michaelidou, N., & Meneses, R. W. (2014). The use of Facebook to promote drinking among young consumers. *Journal of Marketing Management, 30*(13–14), 1377–1401.
Murwira, Z. (2015). Dokora defends phones in schools. Retrieved August 2, 2021, from https://www.chronicle.co.zw/dokora-defends-phones-in-schools/
Nicholls, G. (2014). *Professional development in higher education: New dimensions and directions*. Routledge.
Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). *Research methods for business students*. Pearson Education Limited.
Schmid, E. C. (2016). *Interactive whiteboards and language learning. The Routledge handbook of language learning and technology* (p. 281). Routledge.
Stavrou, E. (2020). Back to basics: Towards building societal resilience against a cyber pandemic. *Journal on Systemics, Cybernetics and Informatics (JSCI), 18*(7), 73–80.
Stringer, E. T. (2013). *Action research*. Sage Publications.
Takavarasha, S., Bednar, P., & Adams, C. (2011). Using mixed methods for addressing researcher's safety in a conflict area: An innovative use of mixed methods research in Zimbabwe. *International Journal of Mixed Methods in Applied Business and Policy Research, 1*(1), 29–52.
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.
Tunarosa, A., & Glynn, M. A. (2017). Strategies of Integration in mixed methods research: Insights using relational algorithms. *Organizational Research Methods, 20*(2), 224–242.
Vanderhoven, E., Schellens, T., Valcke, M., & Montrieux, H. (2015). Son, are you on Facebook? The impact of parental involvement in school interventions about E-safety. In: Proceedings of American Educational Research Association 2015. pp. 1–13
Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the usefulness of school education about risks on social network sites: A survey study. *Journal of Media Literacy Education, 5*(1), 285–294.
Veletsianos, G., & Kimmons, R. (2016). Scholars in an increasingly open and digital world: How do education professors and students use Twitter? *The Internet and Higher Education, 30*, 1–10.
Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435.
Williams, M. L., & Pearson, O. (2016). Hate crime and bullying in the age of social media.
Yin, R. K. (2017). *Case study research and applications: Design and methods*. SAGE Publications.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys, 54*(1), 1–39.
ZimTechReview (2019). Headmasters stifling ICTs in schools. ZimTechReview. Retrieved August 1, 2021



**Theo Tsokota** holds a Bachelor of Science (Honours) in Information Systems from the Midlands State University, a Postgraduate Diploma in Education from Zimbabwe Open University and a Master of Business Administration -Management Information System from Maastricht School of Management and PhD Information Technology from Nelson Mandela Metropolitan University, South Africa. He is a Senior lecturer at the Midlands State University, in the Department of Information and Marketing Sciences.

**Vurayai Mhloza** holds a Bachelors and Masters in Education (Early Childhood Development) from the Great Zimbabwe University. Currently, he is a lecturer at Mkoba Teachers College. He has 20 years' experience in the Zimbabwe Education sector.

**Colletor Tendeukai Chipfumbu-Kangara** holds a Bachelor of Science (Honours) in Information Systems, Postgraduate Diploma in Education and a Master of Science Information Systems Management from the Midlands State University. In addition, she holds a PhD Information Technology from Nelson Mandela Metropolitan University, South Africa. She is a lecturer at the Midlands State University, in the Department of Information and Marketing Sciences.