Journal of Learning for Development 11(3), 2024, 540-552.

Promoting Cyber Ethics Compliance among Teachers in Tanzania: What should be done?

Hamisi Mfaume and Margareth Bilinga

Dar es Salaam University College of Education, Tanzania

Keywords
cyber ethics, cyber crime, compliance, teacher ethics

Abstract

The invention of digital ICT devices is one of the most important developments in the history of humankind, and education can greatly benefit from it. However, cyber ethics violations by teachers have become prevalent and are expected to increase unless measures are taken. This study explored education stakeholders' perspectives on ways to promote teachers' compliance with cyber ethics in Tanzania. It employed a qualitative case study design involving three secondary schools and 27 participants selected purposively in Kinondoni Municipality in the Dar es Salaam region. Data were sought through semi-structured interviews and document reviews and subjected to thematic data analysis. The findings indicated that teachers' compliance with cyber ethics requires training of teachers on the pedagogical uses of technology, the inception of a specific national policy for the responsible use of technology in schools, integration of the cyber ethics aspects of the Teachers' Code of Conduct, improvement of teachers' living and working conditions, and promotion of teachers' awareness of the *Cyber Crimes Act of 2015*, among others. The study recommends that policymakers and education authorities implement the suggested initiatives to promote cyber ethics compliance among teachers for education excellence in Tanzania, and, possibly, elsewhere.

Introduction

Throughout the 21st century so far, there have been waves of discoveries, advances, and dynamics in Information and Communication Technologies (ICTs) that never occurred previously in human history (Aderibigbe & Owolabi, 2021). Of these enormous discoveries, the evolution of networked digital devices, such as tablets, smartphones, and laptops, has become a basic feature of modern society (The International Telecommunication Union [ITU], 2018; Mutunhu et al., 2022). These devices have transformed different social and economic sectors, including education, by opening up new opportunities (Angello, 2015).

In this context, most Sub-Saharan African countries have recognised these devices as potential catalysts for improving access to quality education (UNESCO, 2017). Hence, concerted efforts in creating enabling infrastructure and providing training for teachers to encourage the educational utilisation of the devices have been prominent (Njiku et al., 2022; Traxler, 2016). As key agents of academic development, teachers are expected to deploy these devices to access educational resources and communicate on various education-related matters (UNESCO, 2017; Oyewole, 2017; Wright & Akgunduz, 2018). The devices can also enable teachers to facilitate more interactive and independent student learning (Kartal & Çinar, 2018). Furthermore, they can give teachers access to various in-service professional development opportunities (Mfaume, 2022; Moro et al., 2021).

Published by Commonwealth of Learning, Canada

However, realising that the elastic benefits of the devices can be reaped through their ethical use, most governments have passed cyber-ethics laws and policies (Aderibigbe et al., 2022; Adeniyi et al., 2021). For example, South Africa enacted the *Electronic Communications and Transaction Act* in 2002, Nigeria passed *The Cybercrime Act* in 2015, and Ghana adopted *The Cyber Security Act* in 2020 (The Republic of South Africa, 2002; The Federal Republic of Nigeria, 2015; The Republic of Ghana, 2020), Uganda introduced *The Computer Misuse Act* in 2010, and, in 2018, Kenya adopted *The Computer Misuse and Cybercrime Act* (Republic of Uganda, 2010; Republic of Kenya, 2018). The major goal of these Acts was to sensitise citizens to the ethical use of technology and prevent cyber crimes (Sareen, 2020). Based on these promulgated national laws, some educational institutions have adopted cyber-ethics policies to guide the ethical use of technologies (Adeniyi et al., 2021; Aderibigbe et al., 2022). Cyber ethics refers to a system of standards that prescribe rules pertaining to ethical behaviour in using digital media in online environments (IkeepSafe, 2014; Rama, 2014). Teachers' adherence to cyber-ethics is mandatory, since they are key agents of education delivery and the transmission of societal norms and values (Mfaume, 2020). Their commitment to cyber ethics with a high sense of responsibility and honesty is critical to successfully integrating technology into modern society's teaching and learning (Kindu et al., 2023).

Despite the inauguration of cyber ethics and the ethical obligations for teachers to comply with them, there are alarming rates of violation reports across countries (Karanja, 2016; Porter et al., 2016; Mfaume, 2020; 2022). For example, in South Africa, Ghana, and Malawi, teachers use their smartphones to seduce and harass girl students, chat, and exchange pornographic materials with students (*The Daily News*, 2017; Porter et al., 2016). In Kenya and Nigeria teachers were found guilty of examination leaks through WhatsApp groups in 2015 and 2019, respectively (Erunke, 2019; Karanja, 2016).

In Tanzania, the government inaugurated *The Cyber Crimes Act of 2015,* providing standards of ethical conduct expected for users of information technology systems (United Republic of Tanzania [URT], 2015). The government also expects all citizens, including teachers, to be ethically responsible in using various technologies for national development. Although no national cyber ethics policy is specifically set for schools, the teachers' professional code of conduct requires that teachers abide by all state laws (Teachers' Service Commission [TSC], 2015). Thus, it is incumbent on teachers to comply with the cyber ethics set out in *The Cyber Crime Act* of 2015 when using ICT devices (TSC, 2015).

Despite the government's expectations, as in other Sub-Saharan African countries, cyber ethics violations by teachers are numerous in Tanzania (Kambo, 2023; Mfaume & Bilinga, 2017; Mfaume, 2020, 2022; Mwananchi, 2023; The National Examinations Council of Tanzania [NECTA], 2009; Ramadhan, 2018). Teachers use their devices to play games, listen to music, watch videos in examination rooms, leak examinations, and engage in cyberbullying, sexting, and falsification. Also, disclosure of confidential information, invasion of privacy, recording and posting of other peoples' photos without consent, and dissemination of pornographic materials are common among teachers (Kambo, 2023; Mfaume & Bilinga, 2022; Mfaume, 2020, 2022; Mwananchi, 2023; The National Examinations Council of Tanzania [NECTA], 2009; Ramadhan, 2018). If this seemingly alarming problem is taken for granted, it could be fatal to the government's enthusiasm to promote quality education through technology. Therefore, this study explored stakeholders' views on initiatives towards promoting teachers' compliance with cyber ethics for education excellence in Tanzania. The study tried to answer the following fundamental question:

1. What initiatives do the education stakeholders think are worth taking to curtail cyber ethics violations among teachers in Tanzania?

Literature Review

The issue of cyber ethics has garnered a great deal of interest from researchers in various countries of the world. Most existing studies have identified the level of awareness of cyber ethics and suggested ways to promote compliance among different education stakeholders, including students and teachers. A review of these studies is presented to gain an overview, in essence, of suggested ways to promote compliance with cyber ethics.

Langland (2009) examined graduates' compliance with evolving cyber ethics in the workplace. The results indicated that graduates had difficulty complying with the new rules regarding the use of technology in the workplace. The study proposed that all organisations should have specific policies guiding the use of electronic devices in the workplace, teaching workers about e-etiquette and that colleges should provide their students with training on e-etiquette. Iyadat et al. (2012) determined the level of students' awareness of computer technology and ethics at Hashemite University in Jordan. The researchers proposed that the university hold regular seminars and workshops to educate students, faculty members, and staff members about cyber ethics, preventing cyber crimes, exhibiting good ethical behaviour in cyberspace, and the university administration incorporating learning about cyber ethics into every university course.

Porter et al. (2016) thought establishing specific school policies could address the negative aspects of phone use and promote more positive usage among students and teachers. They also proposed the full involvement of ministries of education, schools, communities, and network providers in promoting digital education and associated safety programmes for the responsible use of mobile phones. Kritzinger et al. (2017) suggested that to improve ethical behaviour in cyberspace, cyber ethics must be anchored in all stages of education, not only for students but also for teachers. Omiunu (2017) proposed training and workshops for teachers on using ICT devices for education activities and incepting a specific policy to curtail cyber ethics violations. Adeniyi et al. (2021) drew insights into the cyber behaviour of undergraduate students at selected universities in Africa. The findings revealed that cyber ethics violations were high due to limited cyber ethical knowledge among students. The study recommended thorough and regular awareness, education, the development of policies dealing with cyber ethics, and the responsible use of cyber technologies.

Baysan and Çetin (2021) suggested that teachers need training on technological devices' pedagogical and ethical use to comply with cyber ethics. Owolabi et al. (2021) examined the cyber ethical behaviour of university students in South Africa and Nigeria. The findings showed that students had intermediate cyber technology skills. The study recommended that university management provide a working ICT policy that could be used to curtail negative uses. Milton et al. (2021) determined awareness and knowledge of cyber ethics among pre-service teachers in Norway, Malta, and Spain. The findings indicated a lack of understanding of how to behave in an exemplary manner online among most pre-service teachers. The study recommended that all Initial Teacher Education (ITE) programmes include digital competence and cyber ethics components in their curricula to promote awareness and compliance. Mfaume et al. (2022) examined why teachers in Tanzania use mobile phones unprofessionally. The researchers recommended that cyber ethics knowledge be taught in teacher education programmes, incorporated in the code of conduct, and have a formal policy to guide the ethical use of

technological devices in education settings. The present study has taken into account the above findings in formulating the research question and the research design.

Methods

The study used a qualitative research approach to explore respondents' views on initiatives to promote cyber ethics compliance among teachers (Creswell, 2014). The qualitative research approach was based on a multiple case study design. The design provided researchers with extensive and rich data from respondents in their natural environment in three public secondary schools in the Dar es Salaam region (Yin, 2011). Thus, the approach and the design made it possible to understand the possible strategies to promote compliance with cyber ethics among teachers in cyberspace (King & Horrocks, 2010).

Population and Sample

The study population was heterogeneous, involving Education Officers, School Quality Assurance Officers, and Teachers' Service Commission (TSC) Officers. Others were: heads of schools, teachers, and students in public secondary schools in Kinondoni Municipality in the Dar es Salaam region.

The sample involved three public secondary schools and twenty-seven (27) respondents in Kinondoni Municipality in the Dar es Salaam region. Specifically, the sample consisted of one School Quality Assurance Officer, one TSC officer, three heads of schools, one Municipal Education Officer for Secondary schools, 18 teachers (six selected from each sample school) and three student head prefects (one selected from each sample school). This sample size was determined due to data saturation (Patton, 2015; Yin, 2011). The names of the sampled schools and respondents were anonymised for ethical considerations.

The purposive sampling technique was used to select schools and study respondents. The method allowed the researchers to use their judgment to obtain the respondents (Magwa & Magwa, 2015). In this respect, the Kinondoni Municipality was chosen as the study area as it was a pilot area for integrating ICTs into schools in the region. Within the municipality, the researchers selected three public secondary schools with enabling ICT infrastructure and facilities such as wireless Internet connectivity and ICT labs. In addition, respondents were selected based on the positions they held in their respective schools and the education sector. The selected respondents were responsible for the overall management of education and discipline matters.

Instruments

The data were gathered through semi-structured interviews and document review (Mogalakwe, 2006; Willig, 2013). The researchers interviewed the respondents in relaxed and comfortable school premises within their respective offices. The semi-structured interviews allowed the interviewees to express their opinions fully, enabling the researchers to delve deeply into insider perspectives (Turner, 2010). All interviews were recorded with the respondents' consent. To complement the interview data, the researchers reviewed the Tanzanian *Cyber Crime Act*, *2015,* the teachers' professional code of conduct and the public servant code of conduct (Mogalakwe, 2006; TSC, 2015; URT, 1996, 2015). The review allowed researchers to familiarise themselves with the ethical obligations that guide teachers' practices as public servants in Tanzania.

Data Analysis

The data gathered were analysed manually through the five phases of thematic analysis proposed by Creswell (2013). In the first phase, the researchers transcribed the audio recording and reviewed the transcripts repeatedly to ensure the respondents' original meaning had been captured. In the second phase, each researcher conducted a separate analysis to code and produce themes and reported the identified themes during the data analysis meeting. The researchers then agreed on the appropriate themes, taking into account the availability of the evidence submitted. In the third phase, the researchers went back and forth through the previous steps and agreed on the format for presenting the data, and each researcher was given a section to write. In the fourth phase, the researchers met, compiled, conceptualised, and interpreted the data and provided adequate evidence for each theme before the conclusions were drawn. In the fifth and final phase, the researchers drafted the report to present the study findings and developed recommendations. Schools were named X, Y, and Z for anonymity in reporting the results.

Findings

This section presents the findings about the initiatives proposed for promoting teachers' compliance with cyber ethics in Tanzania. Based on the analysis of the data, the following major themes emerged:

The Training of Teachers on the Pedagogical uses of Technology

The respondents felt that for teachers to comply with cyber ethics, they should be provided with the skills and competencies needed to integrate digital technologies into pedagogical processes. They argued that teachers often engage in unethical practices due to their lack of digital skills and support to use their devices for educational purposes. The extracts below confirm the ideas presented so far:

> As far as I know, teachers violate cyber ethics because of their limited knowledge of the pedagogical use of technology… If they are properly trained to use them for teaching purposes, they will likely concentrate on more professional than unprofessional uses... (Head of School X).

The Education Officer concurred:

> The best way to combat cyber ethics violations is to educate teachers on using their devices for teaching and learning. I say that because most teachers who commit offenses have no such knowledge.

According to the results, it is more evident that teachers' knowledge of the pedagogical use of devices is a crucial step in tackling the problem. It can motivate teachers to cling to the professional use of devices rather than abuse.

Promoting Teachers' Awareness of the Cyber Crime Act, 2015

The respondents also expressed that teacher awareness and knowledge of the *Cyber Crime Act* is key to reducing unethical behaviours in cyberspace. They argued that though the government has passed legislation to guide the ethical use of technology, many teachers are blind to its existence and many others to its content. As a result, they are more likely to break the law without their knowledge and find themselves in a difficult situation. Thus, they suggested that the Teachers' Services Commission (TSC), a body responsible for teacher discipline, should provide teachers with copies and knowledge of the law. This would alert them to inappropriate practices and help

eliminate them when using their devices. This sentiment from the teacher from School "Y" elucidates:

> The Cyber Crime Act of 2015 sets out ethical and unethical practices regarding the use of technology, but most teachers are not familiar with its content. Others don't even know it exists, let alone have access to its copies. Therefore, if the TSC and the Ministry of Education provide teachers with copies of the Law and its knowledge, they will certainly comply.

The findings suggest that the lack of knowledge of the *Cyber Crime Act* and the unavailability of training contributes significantly to ethical violations among teachers. Of course, if the responsible authorities take concerted initiatives to educate teachers, the majority will act appropriately in cyberspace.

The Inception of a Specific National Policy for Responsible use of Technology in School Settings

The respondents, mostly heads of schools, recommended that the government establish a specific national policy to guide the acceptable and responsible use of emerging technologies in schools. They said that the absence of clear policy direction has made it extremely difficult for school leaders to monitor professional versus non-professional use of devices in schools. The policy would serve as a framework for heads of schools to address any violations instead of relying on inconsistent statements made by top government officials. Further, they expressed the reservation that, for the policy to be effective, it should highlight the expected ethical behaviour, reporting procedures, and penalties for each violation. The head of School "Y" reflected on this in the following manner:

> I think it's time to develop a specific national policy to guide the ethical use of emerging technologies in schools. It will enable us to understand desired behaviour in cyberspace and avoid abusing them...

The preceding findings suggest that clear policy direction is essential for appropriately using technological devices in schools. It will provide a clear path and help curb breaches of cyber ethics, as teachers and their leaders will be confident about expected behaviour and sanctions for violations.

Integrating Cyber Ethics into the Initial Teacher Education (ITE) Programmes

The respondents believed that integrating cyber ethics as a core subject in the ITE curriculum is paramount in promoting teachers' compliance. They said that currently, student teachers in Tanzania are not exposed to cyber ethics courses in colleges and are free to use their devices however they want. As a result, it is often difficult for them to adhere to a new set of rules governing the use of technology in a work environment that restricts their freedom. The respondents felt the subject would be relevant for equipping student teachers with ethical behaviour to transpire in their future careers. The school Quality Assurance Officer said:

> ITE is often the first place where a student teacher is initiated into professional knowledge and experience; I think that may also be the best place for them to learn more about the ethical rules governing the use of technology.

Arguably, teaching cyber ethics in the ITE is imperative, not only to curb unethical behaviour in cyberspace but also to instil and reinforce a sense of moral sensibility among tomorrow's teachers in the digital world.

The Integration of the Cyber Ethics Aspects in the Teachers' Code of Conduct

Most respondents suggested including cyber ethics aspects in the teachers' professional Code of Conduct. They said that since the Code of Conduct guides the teachers' everyday practices, the integration of ethical aspects regarding the use of technology would provide them with a point of reference that should guide them to ethical use. However, the respondents also expressed reservations that for the Code to be effective, it must be made known and available to teachers, students, and the wider public. Arguing about this, the head of School "Z" divulged:

> If we need to promote teachers' compliance with cyber ethics, the teachers' code of conduct should incorporate cyber ethical aspects so that teachers become aware of their ethical obligation and refrain from violations…

The findings suggest that because the Code of Professional Conduct is the benchmark for the daily conduct of teachers then, if cyber ethics is built into it and is effectively enforced, teachers will likely behave in an ethically acceptable way in cyberspace.

Providing Teachers with Counselling and Mentoring Support

The findings indicated that another way to address cyber ethics violations by teachers would be for schools to give the teachers counseling and mentorship support. It was admitted that some teachers indulged in unethical practices due to psychological problems such as addiction, frustrations, and emotional problems. Others, especially newly appointed teachers, were reported to lack proper guidance from more experienced teachers. Therefore, professional counseling and stringent mentorship support could enable teachers to meet their personal, emotional, and professional aspirations and avoid unethical practices. An experienced teacher at School "X" concurred:

> Education today is dominated by teachers born in the digital era who can hardly stay offline. As an experienced teacher, I see many unethical practices online from those teachers. Sometimes they share nude photos in the staff's WhatsApp group, and you are amazed, but I'm sure they will stop if they get systemic mentorship.

Based on the findings, it is evident that teachers, especially those who are newly appointed, should be attached to experienced mentors for appropriate induction and mentoring. Accordingly, teachers need psychological support from competent psychologists for behavioural and emotional therapy. Thus, systemic and sustainable mentorship and counseling support are likely desirable for curbing cyber ethical breaches.

To Establish a Clear and Secure System of Reporting Cyber Ethics Violations

Another suggested way to promote cyber ethics compliance is to have a well-established system of reporting the perpetrators of cyber ethics violations in schools. The respondents said that establishing a clear and well-known reporting procedure would allow different persons, including victims of unethical practices, to report the perpetrators of such practices for ethical measures. Some proposed systems include suggestion boxes, hotlines, and confidential assessment forms for evaluating teachers' behaviour. The words of a student at School "X" point to these respondents' suggestions:

> We see different unethical practices from our teachers online, but we do not know where to report them, and sometimes we fear their retaliation. If schools had good reporting systems, like a suggestion box, the problem would have been minimized or stopped once and for all ...

The findings imply the ineffective status of the reporting system for teachers' misconduct in schools. The implication is that if a clear and confidential reporting system is put forth and adhered to, schools would certainly become free from cyber ethical violations.

Improving Teachers' Conditions of Service

Another suggested way to curb cyber ethics violations is for the government to improve teachers' living and working conditions. The participants stated that teachers are deprived of their economic rights and freedom. This is because their current salaries are scant and other benefits are unavailable and associated with longstanding arrears. As a result, their morale and commitment to the workplace have diminished; they are frustrated and engage in unethical practices, such as online gambling, online business during working hours, forgery, and other forms of cyber ethics violations. Participants also said if the government draws attention to and attends to teachers' needs and claims, including claims for salary and allowance, and improves their living and working conditions, they will feel responsible for fulfilling their core roles and refrain from unethical practices. The TSC officer gave this suggestion:

> One possible way to promote teachers' compliance with cyber ethics is for the government to improve teachers' salaries and pay them allowances to survive in the alarmingly high inflation situation ... it should also pay the longstanding salary arrears and other claims. Once this is done, these abuses of technology will stop automatically.

Arguing in the same tone, a male teacher at School "Z" maintained:

> Teachers are among the low-income professional communities. Surprisingly, even their low income is coupled with longstanding arrears. This situation poses complicated life questions which compel them to breach professional ethics. If economic problems are addressed, they will comply with cyber and professional ethics generically.

The assertions affirm that teachers' economic and social satisfaction is critical for promoting their adherence to the established ethical guidelines in cyberspace.

Empowerment of the TSC

The study respondents suggested the TSC be empowered regarding fiscal and physical resources. The participants clarified their suggestion by saying that many teachers violate ethical obligations due to a lack of knowledge about their professional ethics. Thus, as the TSC is an autonomous authority in teachers' ethics and professional development, it should be empowered so that it fulfils its core mandate of equipping teachers with adequate professional knowledge. This will make them familiar with and adhere to the necessary moral and ethical requirements. Sharing this view, the TSC officer said:

> Most teachers lack knowledge about ethics. Our responsibility is to educate them, but this needs adequate funds and human resources. Yet, we do not have any source apart from relying on the central government… If we are adequately empowered, teachers will be educated and behave accordingly…

It is apparent from the preceding quotation that the TSC fails to educate teachers on their professional obligations due to the budget deficit and lack of workforce. Convincingly, it is apparent that if the TSC were empowered, it could likely succeed in equipping teachers with ethical knowledge and addressing unethical practices.

Discussion

The study results showed that teacher training in the educational use of technology could help reduce breaches of cyber ethics. The finding echoes the findings of Omiunu (2017), Baysan et al. (2021), and Mfaume (2022). It is undeniable that the training could reinforce teachers' positive attitudes and interest in the professional use of ICT devices. This, in turn, would reduce negative uses, improving the benefits that the technology could provide for education and national development. When speaking on the importance of training on cyber ethics compliance, Sinom (2017) claimed that equipping staff with the information required to recognise and react to cyber threats, would mitigate risk, enhance organisational resilience against cyber threats, and embed a culture of cyber security awareness.

As stated elsewhere, teachers were not aware of the Act. The need to educate teachers about the *Cybercrime Act of 2015* was therefore considered critical to improving compliance with cyber ethics. This suggestion has strengthened the findings of Adeniniyi et al. (2021), Owolabi et al. (2021), and Mfaume et al. (2022), who pointed out that a lack of awareness of cyber-ethics laws has exacerbated cyber-ethics problems. Lack of awareness regarding the Act can be explained in two ways. Firstly, implementers cannot implement it since they are unaware of its intentions. Secondly, those trying to implement it may do so incorrectly by promoting restricted content, thus going against the policy developers. Arguably, since the *Cyber Crime Act of 2015* is a benchmark for practice in cyberspace, knowledge of its existence and content should be provided to all citizens, including teachers. Knowledge can be disseminated by distributing and discussing the Act in all schools and the community and organising awareness sessions.
In addition, the study identified the need for a specific national policy for the responsible use of technology in educational contexts. This proposal has emerged from various studies (Langland, 2009; Porter et al., 2016; Adeniyi et al., 2021; Owolabi et al., 2021; Mfaume et al., 2022) showing that the ethical use of technology in educational institutions requires an accurate policy framework. With the rapid integration of technology into education, it is apparent that a clear and precise policy direction is needed for the ethical use of technology. It is a matter for the policymakers to formulate a policy and to ensure systemic and stringent mechanisms for its implementation.

It was also noted that, as part of a strategy to combat breaches of cyber ethics, the ITE curriculum should incorporate cyber ethics as a core subject. Cyber security awareness changes individual mindsets and behaviour toward information security, generating buy-in and commitment towards cyber security initiatives. In the same vein, Langland (2009), Iyadat et al. (2012), Kritzinger et al. (2017), Milton et al. (2021), and Mfaume et al. (2022), contend that colleges and universities should be the first place for teachers to learn about ICT use ethics. If teachers are exposed to cyber ethics during the ITE, they will be familiar with, knowledgeable about and will later conform to cyber ethics in workplaces.

It has been suggested that the Code of Conduct for teachers include cyber ethics. This finding sustains the recommendation made by Mfaume et al. (2022) that for teachers to use their mobile phones professionally, their Code of Conduct should be reviewed to consider the central contemporary aspects of professional accomplishment. Because the code serves as a guide to teachers' practices, it is appropriate to review it, include acceptable ethical behaviour, and highlight rigorous disciplinary measures against violators of cyber ethics. However, it is important to note that for teachers, learners, and the community to enforce the law successfully, they must have access to it and adequate knowledge of what the law is all about.

This study also proposed that cyber ethics can be prevented by providing counselling and mentoring services to teachers. Consistent with this finding, Magwa (2015) postulates that school psychologists are essential assets to provide teachers with a range of appropriate psychological assessments and counselling, and interventions. From a similar perspective, Langland (2009) argues that new employees need strong mentoring support to become familiar with the ethical principles governing the usage of ICT devices in the workplace. Teachers are coupled with several issues where they need support. In this respect, the role of counselling and mentoring should not be underestimated. If teachers obtain this support, there is a high probability of them settling in and focusing on technology's ethical and professional use.

The study's findings suggested a clear and confidential system for reporting violations is necessary. In most cases, the lack of a clear system to report unethical practices has fuelled misconduct in education settings (Poisson, 2009; Shumba, 2011; Mfaume, 2012). Hence, as suggested, having a clear and confidential system is critical as most violations will be reported. With the knowledge that they are reportable, offenders would use their devices more wisely.

The results also indicate that the promotion of cyber ethics among teachers can be achieved if the teachers' service conditions are improved. Better wages and decent working and living conditions are important in order for professionals to devote themselves fully to work and execute their duties effectively (Bennell & Akyeampong, 2007). However, as in many developing countries, most teachers in Tanzania are overwhelmed with work and have difficulty with living and travelling expenses, taking into account a starting salary of TGTSB1 of 479,000 Tanzanian shillings for a teacher with a grade IIIA certificate, TGTSC1 of 590,000 for a diploma holder, and TGTSD1 of 771,000 for a graduate. The government should draw attention to teachers' plight and create favourable living and working conditions so that teachers feel responsible for executing their professional duty and behaving accordingly.

Another suggested approach was to ensure the TSC had adequate financial and physical resources. This perspective also emerged from research by Mfaume et al. (2022). The TSC is an autonomous authority entrusted, among other things, with teachers' professional development and discipline. Thus, supporting it with sound financial and human resources would enable it to provide teachers with ethical guidelines, as well as training them regularly on related cyber ethics.

Conclusions and Recommendations

On the basis of the results, the most pertinent conclusions are: compliance with cyber ethics is possible if teachers receive training on the pedagogical uses of technology; teachers' awareness of the *Cyber Crimes Act of 2015* is promoted; a specific national policy for responsible use of technology in school settings is instituted; and cyber ethics aspects are integrated into the initial teacher education programmes and the teachers' Code of Conduct. Other ways to promote compliance included providing teachers with counselling and mentoring support, establishing a clear and secure system of reporting cyber ethics violations, improving teachers' service conditions, and empowering the TSC.

The study, therefore, recommends that policymakers and education authorities, including the Ministry of Education and TSC, examine how they can better work on suggested initiatives to address the problem and promote cyber ethics compliance among teachers for education excellence. Teachers should also consider compliance with cyber ethics and other ethical requirements as a matter of duty. They should therefore use the technology per the stated laws. This will develop good values and virtues that benefit them in work and society. Given that the study was confined to a limited category of stakeholders within a single region and municipality,

to get the most out of the study, it would be better to expand it to other educational institutions, such as colleges and universities, and to explore the views of different categories of stakeholders.

References

Aderibigbe, N.A., & Owolabi, K.A. (2021). Cyber ethical behaviour of university students: An overview of the University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Ogun state, Nigeria. *Journal of Applied Information Science and Technology, 13*, 87-106.

Aderibigbe, N., Ocholla, D., & Britz, J., (2021). Differences in the ethical cyber behavioural intention of Nigerian and South African students: A multi-group analysis based on the theory of planned behaviour. *Libri, 71*(4), 389-406. https://doi.org/10.1515/libri-2019- 0062

Angello, C. (2015). Exploring the use of ICTs in learning and disseminating livestock husbandry knowledge of urban and peri-urban communities in Tanzania. *International Journal of Education and Development Using Information and Technology*, *11*(1), 5-22.

Baysan, E., & Çetin, Ş. (2021). Determining the training needs of teachers in the ethical use of information technologies. *Journal of Theoretical Educational Science, 14*(3), 476-497.

Bennell, P., & Akyeampong, K. (2007). *Teacher motivation in Sub-Saharan Africa and South Asia*. Department for International Development.

Creswell, J.W. (2013). *Qualitative inquiry, research design: Choosing from five approaches* (3rd ed.). Sage.

Creswell, J.W. (2014). *Research design: Qualitative, quantitative and mixed methods approach* (4th ed.). Sage.

Daily News. (2017, October 24). *Sexiting Durban teacher gets R. 6000 bail.* Durban, South Africa. http://www.dailynews.co.tz

Erunke, J. (2019). *Police parade three teachers arrested over leaked WAC question papers.* http://www.newsexpressngr.com/news

International Telecommunications Union [ITU]. (2018). *Measuring the information society.* www.itu.int/en/ITU-D/Statistics/Documents/Publications

Iyadat, W., Iyadat, Y., Ashour, R., & Khasawneh, S. (2012). University students and ethics of computer technology usage: Human resource development. *E-Learning and Digital Media, 9*(1), 43-49.

Kambo, M. (2023). *Curbing teachers' professional misconduct associated with mobile phone use in public secondary schools in Tanzania.* [Masters of Arts in Education Dissertation, University of Dar es Salaam.]

Karanja, S. (2016). The report reveals how teachers and students used phones to cheat in KCSE. *Daily Nation*.

Kartal, B., & Çinar, C. (2018). Examining pre-service mathematics teachers' beliefs of TPACK during a method course and field experience. *Malaysian Online Journal of Educational Technology, 6*(3), 11-37.

Kindu, A.A., Muluke, A.G., Menber, E. Y., & Kindie, A.L. (2023). Causes of teachers' professional misconduct in Ethiopian secondary schools: Implications for policy and practice. *Cogent Education*, *10*(1), 2188754, DOI: 10.1080/2331186X.2023.2188754

King, N., & Horrocks, C. (2010). *Interviews in qualitative research.* Sage Publications.

Kritzinger, E., Bada, M., & Nurse, J.R.C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. *IFP WG 10th World Conference on Information Security Education (WISE 2017).*

Langland, M. (2009). Evolving e-etiquette in the workplace. *NACE's Journal, 3*, 37-40.

Magwa, S. (2015). *Child sexual abuse by teachers in secondary schools in the Masvingo district, Zimbabwe: Perceptions of selected stakeholders.* [Doctoral Thesis, The University of South Africa.]

Magwa, S., & Magwa, W. (2015). *A guide to conducting research: A student handbook.* Strategic Book Publishing Rights Co., LLC.

Mfaume, H. (2020). *Modern technology and teachers' professional ethics in Tanzania: An investigation into the use of mobile phones by teachers in secondary schools.* [Ph.D. Thesis, University of Dar es Salaam.]

Mfaume, H. (2022). Mobile pedagogical technologies and teachers' professional ethics in Tanzania: An inquiry into the use and abuse of mobile phones by teachers in secondary schools. *Journal of Learning for Development, 9*(2), 176-189.

Mfaume, H., & Bilinga, M. (2017). Prevalence of teachers' professional malpractices in Tanzanian public secondary schools: What ought to be done? *Journal of Education and Training Studies, 5*(2), 43-52.

Mfaume, H., & Bilinga, M. (2022). Why are teachers prompted to use their mobile phones unprofessionally? Experiences from Tanzania. *International Journal of Education and Development using Information and Communication Technology, 8*(2), 191-206.

Milton, J., Giæver, T.H., Mifsud, L., & Gassó, H.H. (2021). Awareness and knowledge of cyber ethics: A study of pre-service teachers in Malta, Norway, and Spain. *Nordic Journal of Comparative and International Education, 5*(4), 18-37.

Mogalakwe, M. (2006). The use of documentary research methods in social research. *African Sociological Review, 10*(1), 221-230.

Moro, C., Phelps, C., Redmond, P., & Stromberga, Z. (2021). Hololens and mobile augmented reality in medical and health science education. *British Journal of Educational Technology, 52*(2), 680-694. http://doi.org/10.111/bjet.13049

Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S. (2022). Cyber security awareness and education framework for Zimbabwe universities: A case of National University of Science and Technology. *Proceedings of the International Conference on Industrial Engineering and Operations Management,* Nsukka, Nigeria.

Mwananchi. (2023). *Homework za likizo chanzo cha ukatili huu [Holiday Homework the source of this brutality].* https://www.malunde.com/2023

National Examination Council of Tanzania [NECTA]. (2009). *Evaluation of the conduct of primary school leaving examination in Tanzania mainland.* http://www.unicef.org

Njiku, J., Mutarutinya, V., & Francois, J.M. (2022). Exploring mathematics teachers' technology integration self-efficacy and influencing factors. *Journal of Learning for Development, 9*(2), 279-290.

Omiunu, O. (2017). Paradoxical modelling of negative uses of ICT and their implication among secondary school students in Oyo State, Nigeria. *Library Philosophy and Practice, 14*(85), 1-32.

Oyewole, O. (2017). Awareness and perception of computer ethics by undergraduates of a Nigerian university. *Journal of Information Science Theory and Practice, 5*(4), 68-80.

Patton, M.Q. (2015). *Qualitative research and evaluation methods: Integrating theory and practice* (4th ed.). Sage Publications.

Poisson, M. (2009). *Guidelines for design and effective use of teacher codes of conduct*. IIEP-UNESCO.

Porter, G., Hampshire, K., Milner, J., Munthali, A., Robson, E., de Lannoy, A., & Abane, A. (2016). Mobile phones and education in Sub-Saharan Africa: From youth practice to public policy: Mobile phones and education in Africa. *Journal of International Development, 28*(1), 22-39.

Ramadhan, M. (2018, October 3). *Dangerous examination cheat network*. http://www.dailynews.co.tz

Sareen, M. (2020). Computer ethics and its related issues. *International Journal of Creative Research Thoughts, 8*(9), 1202-1207.

Shumba, A. (2011). Student teachers' perceptions of the nature, extent, and causes of child abuse by teachers in Zimbabwean schools. *Journal of Social Sciences, 28*(3), 169-179.

Teachers' Service Commission [TSC]. (2015). *Tanzania teachers' code of conduct*. Government Press

The Federal Republic of Nigeria (2015). *The Cyber Crime Act, 2015*. http://www.nigerialawguru.com.

The Republic of Ghana. (2020). *The Cyber Security Act, 2020*. http://www.csdsafrica.org

The Republic of Kenya. (2018). *The Computer Misuse and Cyber Crimes Act, 2018*. http://www.http://kenyalaw.org.

The Republic of South Africa. (2002). *The Electronic Communications and Transaction Act, 2002*. http://www.saflii.org

The Republic of Uganda. (2010). *The Computer Misuse Act, 2010*. http://www.parliament.go.ug.

United Republic of Tanzania [URT]. (1996). *Code of Ethics and conduct for the public service Tanzania.* The Government Printer.

UNESCO. (2017). *Supporting teachers with mobile technology.* UNESCO.

URT. (2015). *Cybercrimes Act, 2015*. The Government Printer.

Willig, C. (2013). *Introducing qualitative research in psychology*. McGraw-Hill.

Wright, B., & Akgunduz, D. (2018). The relationship between technological pedagogical content knowledge (TPACK) self-efficacy belief levels and the usage of Web 2.0 applications of pre-service science teachers. *World Journal of Educational Technology: Current Issues, 10*(1), 52-69. https://eric.ed.gov/?id=EJ1196042

Yin, R.K. (2011). *Qualitative research from start to finish*. The Guilford Press.

Author Notes

Dr Hamisi Mfaume is a Lecturer in the Department of Educational Foundations Management and Life Long Learning, Dar es Salaam University College of Education a constituent college of the University of Dar es Salaam. Email: mfaumeham@gmail.com (https://orcid.org/0000-0002-4596-2188)

Dr Margareth Bilinga is a Senior Lecturer in the Department of Educational Foundations Management and Life Long Learning, Dar Es Salaam University College of Education a constituent college of the University of Dar es Salaam. Email: margarethbilinga33@gmail.com (https://orcid.org/0000-0002-5885-7539)

Cite as: Mfaume, H., & Bilinga, M. (2024). Promoting cyber ethics compliance among teachers in Tanzania: What should be done? *Journal of Learning for Development*, *11*(3), 540-552.