Journal of Education and Learning (EduLearn)
Vol. 20, No. 2, May 2026, pp. 791~800
ISSN: 2089-9823, DOI: 10.11591/edulearn.v20i2.22747

Impact of cyber safety and security literacy program on cyber etiquette of prospective teachers

Santhosh Thangan[1], Thiyagu Kaliappan[2], Vrinda Vijayan[3], Venukanti Sai Abhnav[2], Mandala Chandrashekhargoud[2], Suresh Anuganti[2]
[1]Department of Education, National Institute of Technology, Calicut, India
[2]Department of Education, School of Education & Training, Central University of Karnataka, Kalaburagi, India
[3]Department of Edcuation, School of Education, Integrated Teacher Education Program (ITEP), Central University of Kerala, Kasaragod, India

Article Info

Article history:

Received Jul 11, 2024
Revised Jun 26, 2025
Accepted Jul 19, 2025

Keywords:

ADDIE model
Cyber etiquette
Cyber safety and security literacy program
Digital behavior
Privacy and honesty

ABSTRACT

This research aims to evaluate the effectiveness of a module-based intervention program called cyber safety and security literacy program (CSLP) on cyber etiquette among prospective teachers. The entire study was divided into two major sections, namely: i) design and development of the CSLP; and ii) assessing the impact of the program. For the design, the research and development (R&D) method was used. To assess the impact of the program a quasi-experimental design was followed. Pre-experimental research with a one group pre-test and post-test design was adopted to measure the impact. The convenience sampling method was adopted for the selection of the sample. 50 prospective teachers from various training colleges in India participated in the study. The cyber etiquette scale with 50 items (Cronbach's α=0.889) and valid (Kaiser-Meyer-Olkin (KMO) value=0.804) used for this purpose. The study's findings highlight the effectiveness of the intervention in promoting responsible digital behavior, evidenced by the substantial improvements in participants' pre-test and post-test scores. The strong positive correlation (r=0.74) and large effect size (Cohen's d=5.16) confirm the program's success in fostering higher levels of cyber safety awareness and ethical online conduct.

Corresponding Author:

Santhosh Thangan
Department of Education, National Institute of Technology
Calicut, Kerala, India
Email: santhoshelappully@gmail.com

1. INTRODUCTION

As internet technologies become increasingly consumed in everyday life, users are exposed to a growing number of digital risks. Despite the rising complexity of these risks, the corresponding awareness and preparedness to manage them have not developed proportionately. While digital platforms offer immense educational, social, and professional opportunities, they also pose challenges such as data breaches, cyberbullying, misinformation, and unethical conduct. The central challenge today is not to restrict digital engagement but to empower users especially children and youth to navigate the digital world safely and responsibly. Studies have shown that society lack awareness of how to respond to cyber threats due to lowrisk perception, outdated knowledge, and the mistaken belief that they are unlikely to become victims [1].

In this context, cyber ethics emerges as a crucial framework for ensuring responsible behavior and promoting safety in digital spaces. Cyber ethics refers to the principles and norms that guide acceptable conduct, responsible interaction, and digital citizenship online [2], [3]. Although cyber ethics is frequently discussed in relation to social media use, online communication, and digital commerce, there is limited exploration of how these ethical principles can be systematically instilled through education. With the steady rise in cybercrime and unethical online behavior, the need to integrate cyber ethics into formal learning environments has become increasingly urgent [4].

While general awareness campaigns on digital risks are widespread, a substantial gap persists in targeted educational interventions, particularly those focused on teacher preparation [5]. Teachers play a pivotal role in shaping students' digital behavior and fostering an ethical culture within classrooms by applying their pedagogical competence to model, guide, and reinforce responsible online conduct [6]. However, most educators have not received adequate training to confidently address issues related to cyber safety, security, and ethics in their teaching [7]. Hence strengthening teacher education in this domain is essential, not only to enhance educators' digital competence but also to enable them to cultivate responsible online behavior among students [8].

To address these gaps, the present study introduces and evaluates a structured, module-based intervention: the cyber safety and security literacy program (CSLP). This program is designed specifically for prospective teachers and aims to enhance their understanding and practice of cyber etiquette. The novelty of this study lies in the development and evaluation of a pedagogically grounded CSLP that integrates the C3 matrix cyber ethics, cyber safety, and cyber security within the framework of teacher education [9]. Distinct from prior initiatives that predominantly emphasize general awareness or technical competencies, this program uniquely focuses on fostering behavioral transformation through the development of cyber etiquette.

2. REVIEW OF RELATED LITERATURE

The growing recognition of cyber ethics as a crucial component in addressing online risks has been well-documented in contemporary research. While rapid technological advancements have significantly transformed digital communication and learning environments, ethical guidelines and user awareness have not progressed at the same pace, leaving individuals especially young generation who are vulnerable to various forms of digital misconduct [10]. In this regard, teachers are in a key position to model younger generations' digital behavior and promote values of ethical online interaction. Therefore, encouraging a culture of digital responsibility in schools requires providing teachers, especially aspiring teachers, with a solid basis of cyber ethics in their courses. In line with this argument, comparative studies conducted among pre-service teachers in Malta, Norway, and Spain revealed important insights into the current state of cyber ethics awareness in teacher education. Pre-service teachers in Malta and Norway showed a minimum degree of competency in areas like copyright and privacy, according to these researches, but they lacked a deeper comprehension of the wider consequences of online activity for their professional positions. On the other hand, Spanish pre-service instructors demonstrated a more general awareness of cyber ethics [11], [12]. These findings emphasize the urgent need to systematically integrate cyber ethics into teacher education curricula with the goal of enhancing ethical consciousness and professional responsibility of prospective teachers while also preparing them to guide students towards safe, respectful, and ethical digital practices in today's complex online environments.

In addition, research has also examined instructional methods like case-based learning, which have shown potential in developing a basic understanding of information and communication technology (ICT) ethics. However, such methods alone may not be adequate unless they are supplemented with well-structured and comprehensive training programs specifically designed to meet the needs of pre-service teachers [13], [14]. A few studies indicated that pre-service teachers who have a better understanding of digital data security are more aware of online harassment issues, which further links cyber ethics education to the prevention of cyberbullying. This highlights the potential of integrated cyber ethics and security education in reducing harmful online behavior through enhanced awareness and proactive intervention [15]. Moreover, studies examining the interconnectedness of cyber ethics, cyber safety, and cyber security collectively referred to as the C3 matrix-has provided valuable understandings into how these elements influences digital competence. The findings revealed that understanding cyber ethics positively influences awareness of security and safety, which in turn strengthens overall digital competence. However, it was also found that pre-service teachers may not be adequately prepared for responsible digital involvement if ethical awareness is not accompanied by practical skills and contextual knowledge [9]. Addressing these knowledge and skill gaps through well-designed teacher education programs is essential because prospective teachers who receive comprehensive training in cyber safety, ethics, and security are better equipped to lead students toward being morally upright and responsible digital citizens. Therefore, it is argued that establishing cyber etiquette as a major component of professional development, teacher education programs can play a transforming role in creating safer and more ethical online settings for future generations [16].

3. METHOD

This study investigates the effects of a CSLP on cyber etiquette of prospective teachers. The research is structured into two sections. The first section focuses on the design and development of the literacy program, including its components and implementation. The second section measures the impact of the program, using pre- and post-intervention evaluations to analyze the changes in participants' cyber etiquette after experiencing the intervention.

3.1. Design and development of CSLP

The CSLP was developed as a proactive initiative to promote awareness and responsible behavior in the digital space. The program adopts a broader, lifelong learning perspective drawing from established security awareness frameworks and primarily concerned with developing foundational knowledge to bridge the gap between general awareness and skill-based training [17]. The program stresses key ideas in cyber safety and security through promotional activities, videos, and posters, preparing individuals with the knowledge and competences required for responsible digital interaction. To ensure systematic implementation and methodological development, the study employed a research and development (R&D) approach and adopted analysis, design, development, implementation, and evaluation (ADDIE) model instructional design framework. The procedure followed in the study is outlined as follows:

3.1.1. Phase 1: identification and selection of cyber safety and security literacy topics

The effectiveness of any educational program depends on clearly defined objectives and sound assumptions. The CSLP was designed with the primary purpose of promoting cyber etiquette among prospective teachers, based on the belief that online interaction plays a vital role in building digital literacy [18]. It also assumed that existing safety campaigns often lack the depth needed to address modern cyber safety issues. To ensure the program's relevance, a comprehensive review of literature was conducted to identify key focus areas, including communication security, information decency, online interpersonal safety, and safe use of digital tools, all perceived as necessary to equip educators to create a safe and responsible online learning environment [19], [20].

3.1.2. Phase 2: structuring the lesson transcript and implementation of the program

The lesson transcripts for CSLP for prospective teachers were structured using Bloom's evaluation approach by ensuring alignment with clear learning. The program covers 12 themes, divided into 44 sub modules. The contents of each module are carefully organized to achieve its specific goals. For consistency, all modules follow a similar structure, with lesson transcripts emphasizing discussion and activities as core components, recognizing that the complexity of cyber dangers warrants thorough debate. To enhance the program's effectiveness and maintain objectivity, additional resources were prepared by the investigators. The implementation plan was carefully developed by focusing on two key aspects: obtaining prior approval from academic stakeholders and ensuring a supportive institutional climate. These considerations were essential to ensure smooth execution and effective engagement with the program. The detailed outline of the modules and corresponding lesson transcript structure is presented as follows.

The Table 1 shows the general outline of the modules included in the CSLP. There are altogether 12 modules were in the programs with its corresponding sub themes which are closely related to educational environment. Based on the topics concerned, a precise structure for the lesson transcript was prepared in advance.

The Table 2 shows the components of lesson transcripts. The entire contents of each module are presented on the basis of components mentioned in the lesson transcripts. Each lesson transcript has similar sections, and the contents are presented in specific manner based on the objectives. All lesson transcripts consist of discussion and activity as a core section because all kinds of cyber dangers deserve broad debate.

3.1.3. Phase 3: evaluation of the program

To evaluate the efficacy of CSLP modules for prospective teachers a validity analysis carried out from the various stakeholders of this area. Computer science teachers, training college teacher's cyber security professionals were in the expert group. For this two data analysis techniques were used: quantitative and qualitative descriptive. Qualitative data was analyzed by collecting comments and suggestions from expert validators. Quantitative data was analyzed by calculating the percentage score from filling out the validation questionnaire sheet. Further to evaluate validity response of the different expert groups, a systematic approach is used involving the calculation of average scores and setting a benchmark for comparison. First, the scores from each validator for a particular group of experts are collected. These scores are then summed up and divided by the number of scores to calculate the average score for each group. A benchmark score of 3.30 is established to categorize the performance: if the average score meets or exceeds this benchmark, the validity is deemed "good"; otherwise, it would be considered "needs improvement". The validation criteria include: i) understanding of cyber safety concepts; ii) application of cyber safety practices; iii) creative thinking strategies; iv) learner's initiation; v) orientation towards expected outcome of CSLP, and vi) organization and structure of the program. The validity results are in Table 3.

The expert validation results of CSLP module, as presented in Table 3, reveal a commendable level of agreement among various experts. Computer science teachers, cyber security professionals, and training college teachers all contributed their evaluations, resulting in an overall positive assessment. Computer science teachers provided an average score of 3.33, while cyber security professionals offered a slightly higher average of 3.41. Notably, training college teachers rated the module the highest, with an average score of 3.40. Each group's scores were categorized as "good", reflecting a high degree of satisfaction. These results not only affirm the module's efficacy but also demonstrate its broad applicability in providing awareness on cyber etiquette. Finally, the exposure the entire intervention program was conducted online for 100 selected prospective teachers. Google Classroom served as the preferred learning management system (LMS), while Google Meet was used for video conferencing.

Table 1. Outline of modules

Module No.	Module title and topics	Module No.	Module title and topics
Module 1	Social networking security	Module 7	Online privacy
	Introduction to social networking		Introduction to the concept online privacy
	Platforms of social networking		Online privacy related risks
	Risks in social networking		General guidelines for what to share and what not to share
	Safe practices of social networking		Safe practices for online privacy
Module 2	Dealing with fake information	Module 8	Apps safety and security
	The concept of fake information		An introductory note on apps and major kinds of apps
	General formats and platforms of fake information		Major security risks in apps
	Reasons behind creation and consumption of fake information		Safe practices while using apps
	General tips to combat fake information	Module 9	Wi-Fi safety and security
Module 3	Mobile phone safety and security		The conceptual difference between public Wi-Fi and private Wi-Fi
	Introduction to mobile phone safety and security		Major security risks in public Wi-Fi
	Major risks and threats in mobile phone usage		Rules for public Wi-Fi safety
	Areas of mobile phone safety and security	Module 10	Web conferencing safety
	Safety concerns in mobile phone safety and security		Web conferencing
Module 4	Email safety and security		Major web conferencing platforms
	Introducing emails and email security		Major risks in web conferencing
	Forms of email threats		Web conferencing safety
	Safe practices for email security	Module 11	Digital learning resource safety
Module 5	Password safety and security		Digital learning resource
	Introduction to password security		Major dangers in digital learning resource
	Characteristics of strong password		Evaluation and safe practices for digital learning resources
	Major password cracking techniques	Module 12	Plagiarism and copyright infringement
	Safe practices for password security		Plagiarism and its examples
Module 6	Digital footprint or effective online presence		Safe practices for avoiding plagiarism
	Introduction to the concept digital footprint		Copyright infringement
	Major types of digital footprint		Safe practices to avoid copyright infringement
	Ways to create effective online presence		
	Ways to create effective online		

Table 2. Structure of the lesson transcript

Learning outcome	Goal of learning the topic
Content overview	General description of the topic.
Resources	Learning materials related to the topic.
Reference	Supporting documents of references.
Let's discuss	Provides thought-provoking questions. It helps to familiarize the content in advance.
Activity (offline/online)	Each Activity-Offline/online section includes directions to complete a directed, worksheet activity or an online activity to support learning. It prepares the audience to practice certain awareness knowledge and safety skills.
Summary	Consolidation and validation of the learned topic.
Self-reflection/evaluation	A quick review to be sure you understand the concepts just presented and for reflective evaluation.

Table 3. Results of validation

Experts	Score from validator					Average scores	Remarks
	I	II	III	IV	V		
Computer science teachers	3.25	3.46	3.25	3.32	3.36	3.33	Good
Cyber security professionals	3.11	3.42	3.69	3.32	3.53	3.41	Good
Training college teachers	3.44	3.22	3.43	3.25	3.67	3.40	Good

3.2. Assessing the impact of the program

The second section of the study focuses on evaluating the impact of the CSLP by analyzing pre- and post-intervention data to assess changes in participants' cyber etiquette. For this the employed a quasi-experimental design, measuring the experimental group twice before and after the intervention, without a control group for comparison. The intervention involved 50 prospective teachers from various training colleges in Kerala, a state in India, selected through convenience sampling. The primary tool used was a cyber etiquette scale. The following dimensions of cyber etiquette were taken into account when preparing cyber etiquette scale.

The primary tool used for data collection was a comprehensive cyber-etiquette scale, specifically designed to evaluate participants' etiquettes in the digital environment. The scale covers three key dimensions namely: privacy and confidentiality, piracy and plagiarism, and integrity and honesty.

- Privacy and confidentiality: privacy involves individual rights to access and use information, anonymity to protect identity, and confidentiality to maintain data security and confidentiality.
- Piracy and plagiarism: piracy is the unauthorized distribution of copyrighted intellectual property, while
- plagiarism involves using someone else's work without proper credit, a serious academic dishonesty.
- Integrity and honesty: integrity and honesty are concerned with moral uprightness, truthfulness, and trustworthiness in online environment

The final version of the scale includes 50 items, rated on a 4-point Likert scale ranging from "strongly disagree" to "strongly agree". This tool was validated through statistical analysis, showing high reliability with a Cronbach's α value of 0.889 and strong constructs validity with a Kaiser-Meyer-Olkin (KMO) value of 0.804. The scale was administered both before and after the intervention program through an online data collection process, allowing for a robust comparison of participants' cyber etiquette across the intervention period. The Table 4 presents the distribution of items across the key dimensions in the final scale. Out of 50 items, 21 positive statements address privacy and confidentiality, while 21 negative statements represent piracy and plagiarism. The dimension of integrity and honesty is measured by 8 positive items, resulting in a total of 29 positive and 21 negative items in the scale.

Table 4. Item distribution to the key dimensions

Name of the factors	List of items belonging to the factors		Total No. of items
	Positive statements	Negative statements	
Privacy and confidentiality	7, 17, 18, 19, 20, 21, 22, 23, 25, 27, 29, 30, 31, 32, 33, 37, 40, 41, 46, 49, 50	0	21
Piracy and plagiarism	0	10, 11, 12, 13, 14, 15, 16, 24, 26, 28, 34, 35, 36, 38, 39, 42, 43, 44, 45, 47, 48	21
Integrity and honesty	1, 2, 3, 4, 5, 6, 8, 9	0	8
Total	29	21	50

3.2.1. Experimental procedure

The exposure towards the whole intervention program is carried out in online/virtual mode. A separate time schedule was prepared in advance. A total of 60 days program (including 30 hours of instruction) for all selected topics of CSLP were allotted for the treatment. On the completion of each topic, immediate feedback and regular quizzes were implemented to reinforce learning, and responses from the target audience were systematically documented for future assessment. For each topic, various resources, including concept notes, tip sheets, posters, PowerPoint presentations, feedback forms, and attendance sheets, were shared via Google Classroom. To evaluate the program's impact, the cyber etiquette scale was administered again, and scores were recorded for analysis.

4. RESULTS AND DISCUSSION

In this study, the effectiveness of the CSLP was evaluated through statistical analysis using SPSS software. A paired-sample t-test was employed to compare the pre-test and post-test scores from the cyber etiquette scale, allowing for an assessment of the program’s impact on participants’ cyber etiquette. This method assisted in identifying any statistically significant differences in mean scores, indicating whether there was a meaningful improvement in cyber etiquette after the intervention. The analysis showed a significant increase in the posttest scores, indicating the program’s positive influence in improving the cyber etiquette of prospective teachers. The following Table 5 presents the data and results of the test of significance of difference between the mean pre-test scores and post test scores of cyber etiquette and its components among the total sample.

Table 5. Mean comparison of CE and its components

Variables	Pre-test		Post-test		t(49)	p	r	Cohen’s d
	M_1	SD_1	M_2	SD_2				
Cyber etiquette total	127.44	11.92	168.64	9.58	36.49	.00	.74**	5.16
Privacy and confidentiality	53.24	11.97	66.56	7.89	11.90	.00	.75**	1.68
Piracy and plagiarism	53.60	4.71	75.36	3.51	33.38	.00	.40**	4.72
Integrity and honesty	20.60	2.98	26.72	2.60	13.50	.00	.35**	1.91

Note: N=50; **Significant at 0.01 level

Table 5 reveals the mean comparison of pre-test and post-test scores of cyber etiquette in total. The finding indicated the significant mean difference in cyber etiquette with t(49)=36.49, $p<0.01$. Results shows that the mean pre-test score of cyber etiquette (M_1=127.44, SD_1=11.92) subsequently augmented in the post test scores of cyber etiquette (M_2=168.64, SD_2=9.58). Two sets of scores were significantly correlated (r=0.74, $p<0.01$). The value of Cohen’s d for pre-test and post-test scores of cyber etiquette was 5.16(>0.80) which indicates large effect size. For the component privacy and confidentiality of cyber etiquette the results specify the significant mean difference in privacy and confidentiality with t(49)=11.90, $p<0.01$. The findings shows that the mean pre-test score of privacy and confidentiality (M_1=53.24, SD_1=11.97) subsequently augmented in the post test scores of privacy and confidentiality (M_2=66.56, SD_2=7.89). Two sets of scores were significantly correlated (r=0.75, $p<0.01$). The value of Cohen’s d for pre-test and post-test scores of privacy and confidentiality was 1.68 (>0.80) which indicates large effect size.

With respect to the component piracy and plagiarism of cyber etiquette the results indicated significant difference in mean t(49)=33.38, $p<0.01$. Here the mean pre-test scores of piracy and plagiarism (M_1=53.60, SD_1=4.71) revealed a consequent progress in the post test scores (M_2=75.36, SD_2=3.51) of piracy and plagiarism. Further the two sets of values are correlated (r=0.40, $p<0.01$). The calculated Cohen’s value for the pre-test and post-test scores of piracy and plagiarism was 4.72 (>0.80) which indicates the effect size as large. With regard to the component integrity and honesty the finding indicated the significant mean difference in integrity and honesty with t(49)=13.50, $p<0.01$. Results shows that the mean pre-test score of integrity and honesty (M_1=20.60, SD_1=2.98) subsequently augmented in the post test scores of integrity and honesty (M_2=26.72, SD_2=2.60). Two sets of scores were significantly correlated (r=0.35, $p<0.01$). The value of Cohen’s d for pre-test and post-test scores of integrity and honesty was 1.91 (>0.80) which indicates large effect size.

The statistical analysis of the effectiveness of the CSLP revealed significant improvements in cyber etiquette scores among prospective teachers. Specifically, our findings indicate a substantial increase in the total cyber etiquette score, with a mean pre-test score of 127.44 (SD=11.92) rising to 168.64 (SD=9.58) in the post-test, yielding a t-value of 36.49 ($p<0.01$) and a large effect size (Cohen’s d=5.16). This supports earlier findings of the research suggesting that structured educational interventions can enhance learners’ understanding of cyber safety [21]. Furthermore, the components of privacy and confidentiality, piracy and plagiarism, and integrity and honesty also showed significant improvements, reinforcing the notion that targeted educational methods can effectively promote responsible digital behavior. For instance, the increase in privacy and confidentiality scores (from 53.24 to 66.56, t(49)=11.90, $p<0.01$, Cohen’s d=1.68) reflects a growing awareness among participants regarding the importance of maintaining privacy online, which is essential in the current digital landscape. According to the current study, improving one’s understanding of these topics is not only advantageous but may also improve participants’ general digital literacy without having a negative effect on their academic achievement in other areas. This emphasises the potential of integrating cyber etiquette education into teacher training programs, paving the way for more responsible digital citizenship in future educators.

The primary objective of this research is to measure the impact of CSLP on cyber etiquette of prospective teachers. After designing the intervention program CSLP and experimental study was carried out to measure its effectiveness. For this single group (pre-test and post-test) quasi experimental design was used. With the help of a standardized scale on cyber etiquette considerable difference was observed before and after the intervention of the program, which ultimately signified higher level of cyber safety awareness was connected to higher level of cyber etiquette. This enhancement underscores the effectiveness of the intervention in promoting responsible digital behavior among the participants. The strong positive correlation (r=0.74) between the pre-test and post-test scores underscores the consistency and reliability of the results. The very large effect size (Cohen's d=5.16) indicates that the intervention had a profound impact on the participants' overall cyber etiquette. Furthermore, these results highlight the importance of continued focus on cyber etiquette practices to foster responsible and ethical online behavior [22]. The significant advancements across all components namely privacy and confidentiality, piracy and plagiarism, integrity and honesty indicate that such educational interventions are not only effective but necessary in today's digital age [23]. As individuals spend more time online, understanding the fundamentals of cyber etiquette becomes crucial in preventing negative behaviors such as privacy breaches, piracy, plagiarism, and dishonesty [24]. To raise user awareness and encourage the implementation of preventive cyber safety techniques in everyday life, continuous education and targeted interventions are indispensable. These efforts not only equip individuals with the necessary skills to navigate the digital world safely but also foster a culture of proactive cyber safety practices [25]. This holistic approach guarantees that individuals are not only informed but also empowered to protect themselves and others in the digital environment.

5. CONCLUSION

In conclusion, this research demonstrates the significant impact of the CSLP on improving the cyber etiquette of prospective teachers. The results revealed that the intervention effectively promotes responsible digital behavior, with substantial improvements in participants' pre-test and post-test scores. However, while this study explored a comprehensive assessment of the CSLP's effectiveness, further and in-depth studies may be needed to confirm its long-term effects, particularly regarding sustainability across various educational contexts and demographic groups. The improvements showed in areas such as privacy and confidentiality, piracy and plagiarism, and integrity and honesty highlight the necessity of integrating comprehensive cyber etiquette programs into educational curricula and professional development.

Future research should examine the efficacy of various intervention methods, investigating how continuous education can help maintain and reinforce cyber etiquette among diverse populations. Moreover, investigating the role of advanced technologies, such as artificial intelligence and interactive learning platforms, in cyber etiquette education could provide innovative solutions for raising the knowledge of cyber safety awareness. Recent observations suggest that such educational interventions significantly enhance digital citizenship among teachers, and our findings provide conclusive evidence that this proposed learning method is associated with meaningful improvements in online behavior, rather than being merely a result of increased participant numbers. The ultimate goal of these initiatives is to make the internet a safer place by giving people the knowledge and abilities to safely traverse it and by promoting a proactive culture of cyber safety measures.

FUNDING INFORMATION

No funding source is involved in this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Santhosh Thangan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Thiyagu Kaliappan	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	
Vrinda Vijayan					✓		✓		✓	✓		✓	✓	
Venukanti Sai Abhnav				✓	✓				✓	✓		✓	✓	
Mandala Chandrashekhargoud				✓	✓				✓	✓		✓	✓	
Suresh Anuganti				✓	✓				✓	✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors have no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [ST], upon reasonable request.

REFERENCES

[1] S. Mhlongo, K. Mbatha, B. Ramatsetse, and R. Dlamini, “Challenges, opportunities, and prospects of adopting and using smart digital technologies in learning environments: an iterative review,” *Heliyon*, vol. 9, no. 6, pp. 1–20, Jun. 2023, doi: 10.1016/j.heliyon.2023.e16348.

[2] T. Sayjari and R. M. Silveira, “Ethics of privacy in cybersecurity: protecting individual autonomy through technology,” *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 10, pp. 1940–1951, Oct. 2024, doi: 10.56726/irjmets62448.

[3] T. Santhosh and K. Thiyagu, “Fostering responsible behavior online-relevance of cyber ethics education,” *Malaysian Online Journal of Educational Technology*, vol. 12, no. 1, pp. 32–38, Jan. 2024, doi: 10.52380/mojet.2024.12.1.428.

[4] W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: state of the art, challenges and future directions,” *Cyber Security and Applications*, vol. 2, pp. 1–9, 2024, doi: 10.1016/j.csa.2023.100031.

[5] R. Ravichandran, S. Singh, and P. Sasikala, “Exploring school teachers’ cyber security awareness, experiences, and practices in the digital age,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2025, no. 1, pp. 1–7, Jan. 2025, doi: 10.62915/2472-2707.1214.

[6] T. D. Dang, T. T. Phan, T. N. Q. Vu, T. D. La, and V. K. Pham, “Digital competence of lecturers and its impact on student learning value in higher education,” *Heliyon*, vol. 10, no. 17, pp. 1–12, Sep. 2024, doi: 10.1016/j.heliyon.2024.e37318.

[7] S. Rautela, N. Panackal, and A. Sharma, “Modeling and analysis of barriers to ethics in online assessment by TISM and fuzzy MICMAC analysis,” *Asian Journal of Business Ethics*, vol. 11, no. S1, pp. 111–138, Dec. 2022, doi: 10.1007/s13520-022-00158-x.

[8] W. H. Prasetiyo, B. Sumardjoko, A. Muhibbin, N. B. M. Naidu, and A. Muthali’in, “Promoting digital citizenship among student-teachers: the role of project-based learning in improving appropriate online behaviors,” *Participatory Educational Research*, vol. 10, no. 1, pp. 389–407, Jan. 2023, doi: 10.17275/per.23.21.10.1.

[9] D. Wuyun, “Exploring English preservice teachers’ digital competence perceptions regarding the C3 matrix-cyber ethics, cyber security and cyber safety: an empirical study executed in China,” *International Journal of New Developments in Education*, vol. 5, no. 1, pp. 31–41, 2023, doi: 10.25236/IJNDE.2023.050106.

[10] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, “Ethical dilemmas and privacy issues in emerging technologies: a review,” *Sensors*, vol. 23, no. 3, pp. 1–18, Jan. 2023, doi: 10.3390/s23031151.

[11] J. Milton, T. H. Giæver, L. Mifsud, and H. H. Gassó, “Awareness and knowledge of cyberethics: a study of pre-service teachers in Malta, Norway, and Spain,” *Nordic Journal of Comparative and International Education*, vol. 5, no. 4, pp. 18–37, Nov. 2021, doi: 10.7577/njcie.4257.

[12] V. I. Marín, J. P. Carpenter, G. Tur, and S. Williamson-Leadley, “Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers,” *Journal of Computers in Education*, vol. 10, no. 4, pp. 769–795, Dec. 2023, doi: 10.1007/s40692-022-00243-x.

[13] I. Stavrakakis *et al.*, “The teaching of computer ethics on computer science and related degree programmes. A European survey,” *International Journal of Ethics Education*, vol. 7, no. 1, pp. 101–129, Apr. 2022, doi: 10.1007/s40889-021-00135-1.

[14] K. Richard and N. Julian, “Ethical dimensions of ICT integration in higher education: a comprehensive review,” *Newport International Journal of Engineering and Physical Sciences*, vol. 4, no. 2, pp. 1–9, Apr. 2024, doi: 10.59298/nijep/2024/421922.2.2200.

[15] M. M. Gümüş, R. Çakır, and Ö. Korkmaz, “Investigation of pre-service teachers’ sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security,” *Education and Information Technologies*, vol. 28, no. 11, pp. 14399–14421, Nov. 2023, doi: 10.1007/s10639-023-11785-7.

[16] K. Walsh *et al.*, “Best practice framework for online safety education: results from a rapid review of the international literature, expert review, and stakeholder consultation,” *International Journal of Child-Computer Interaction*, vol. 33, pp. 1–12, Sep. 2022, doi: 10.1016/j.ijcci.2022.100474.

[17] M. Mukherjee, N. T. Le, Y.-W. Chow, and W. Susilo, “Strategic approaches to cybersecurity learning: a study of educational models and outcomes,” *Information*, vol. 15, no. 2, pp. 1–23, Feb. 2024, doi: 10.3390/info15020117.

[18] H. C. Lo, T. H. Wang, and R. S. Chen, “Enhancing critical digital literacy of preservice preschool teachers through service learning: the moderator of online social capital,” *Sustainability (Switzerland)*, vol. 16, no. 6, pp. 1–17, Mar. 2024, doi: 10.3390/su16062253.

[19] D. M. Zulqadri, A. Mustadi, and H. Retnawati, “Digital safety during online learning: what we do to protect our student?” *Jurnal Iqra’ : Kajian Ilmu Pendidikan*, vol. 7, no. 1, pp. 178–191, Jun. 2022, doi: 10.25217/ji.v7i1.1746.

[20] Y. Zheng *et al.*, “Effects of digital game-based learning on students’ digital etiquette literacy, learning motivations, and engagement,” *Heliyon*, vol. 10, no. 1, pp. 1–18, Jan. 2024, doi: 10.1016/j.heliyon.2023.e23490.

[21] R. Pirta-Dreimane *et al.*, “Application of intervention mapping in cybersecurity education design,” *Frontiers in Education*, vol. 7, pp. 3–12, Nov. 2022, doi: 10.3389/feduc.2022.998335.

[22] A. Assad, A. Kaleel, I. Zainal, and R. Wadood, “Practicing netiquette in online communication between students and professors in higher education: a systematic review,” *Studies in Media and Communication*, vol. 12, no. 4, pp. 65–78, Sep. 2024, doi: 10.11114/smc.v12i4.6903.

[23] W. Wulandari, “Ethical use of information technology in higher education: edited by Liliana Mâtă, Singapore, Springer, 2022, 217 Pp., ISBN: 978-981-16-1953-3 (Paperback) ISBN: 978-981-16-1951-9 (eBook),” *Open Learning: The Journal of Open, Distance and e-Learning,* vol. 38, no. 3, 2023, doi: 10.1080/02680513.2023.2213267.

[24] N. A. Aderibigbe, “Synopsis on cyberethics behaviour: a literature review,” *Inkanyiso: Journal of Humanities and Social Sciences*, vol. 13, no. 2, pp. 273–290, Dec. 2021, doi: 10.4102/ink.v13i2.8.

[25] A. A. Arishia, N. H. Kamarudinb, K. A. A. Bakarc, Z. B. Shukurd, and M. K. Hasan, “Cybersecurity awareness in schools: a systematic review of practices, challenges, and target audiences,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 12, pp. 467–478, 2024, doi: 10.14569/IJACSA.2024.0151249.

BIOGRAPHIES OF AUTHORS

Santhosh Thangan presently serving as an ad-hoc faculty in the Department of Education, National Institute of Technology, Calicut, Kerala, India. He has obtained his PhD in Education from Department of Education, Central University of Kerala. He holds Master’s degree in both Econmics and Education. He was a recipient of University Grants Commission (UGC) Junior Research Fellowship (JRF) in education and has qualified UGC National Eligibility Test (NET) for lectureship in economics. His areas of interest are education technology, teacher training, cyber safety and security, and economics of education. He has attended several workshops and conferences in the field of education and also presented and published articles in reputed journals. He has authored two books and two manuals in the field of cyber safety and security. He can be contacted at email: santhoshelappully@gmail.com.

Thiyagu Kaliappan is an associate professor in the Department of Education, School of Education and Training, Central University of Karnataka, Kalaburagi, India. His research interests include educational technology, pedagogy of mathematics, and research methods in education, with specializations in digital pedagogy, cyber safety, AI-powered Education, and augmented reality in education. He has authored four books and published more than fifty-five research papers in reputed journals and conference proceedings. His academic work focuses on integrating emerging technologies to enhance teaching and learning, fostering innovation in education, and promoting digital competence among educators. He actively engages in academic collaborations, seminars, and workshops. He can be contacted at email: thiyagusuri@gmail.com.

Vrinda Vijayan is an assistant professor (mathematics) and former ICSSR post-doctoral fellow as well as UGC research scholar in the Department of Education, Central University of Kerala. She has Master’s degree in both Education and Mathematics. She has published several articles in peer-reviewed, UGC-CARE listed, and SCOPUS-indexed journals. She has actively partcicpated and presented papers in many national and international seminars. Her areas of expertise include mathematics education, instructional technology, and research statistics. She can be contacted at email: drvrindarun@gmail.com.

Venukanti Sai Abhnav is working as an assistant professor in the Department of Education, School of Education and Training Central University of Karnataka, India. He has PhD in Physical Education and M.P.Ed. He has 7 years of experience in teaching and coaching, proficient in sports sciences and physical education. He has published articles in many peers reviewed journals. His areas of expertise are innovative teaching methods, research in sports training and health education, fitness and wellbeing, and sports sciences. He can be contacted at email: saiabhinav@cuk.ac.in.

Mandala Chandrashekhargoud is currently working as an assistant professor in the Department of Education at the Central University of Karnataka, Kalaburagi, Karnataka, India. He is having the qualifications of an M.A. in psychology, M.Ed., and PhD. His primary research areas are Indian knowledge systems, cognitive development, technology in education, comparative education, career guidance and counselling. He has presented 18 papers at various national and international conferences, chaired sessions, and published 21 research papers and articles. He can be contacted at email: man_chandu@yahoo.com.

Suresh Anuganti is currently working as an assistant professor in the Department of Education at the Central University of Karnataka, Kalaburgi, Karnataka, India. He holds M.A. (Political Science), M.A. (Sociology), and PhD. His main research thrust areas are foundational learning and numeracy, ICT in education, Indian knowledge system, and educational socio-cultural context. Related to his research areas he has written and published 8 books, over 24 articles in reputed national and international journals and proceedings of conference. He can be contacted at email: surihcuhyderabad@gmail.com.