CYBER ETHICS AND DIGITAL COMPLIANCE IN MALAYSIA: EMPOWERING ETHICAL DIGITAL CITIZENSHIP

Elisnorazmaliza Ab Hamid[1], Roshila Abdul Mutalib[2], Saifuddin Semail[3]

[1,2,3] Department of Information and Communication Technology, Politeknik Besut Terengganu, Malaysia

*Corresponding E-mail: elis@polibesut.edu.my

ABSTRACT

Objective: This study investigates the relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. It addresses a key research gap, as past studies have focused predominantly on students, with limited empirical evidence involving adult digital users across diverse backgrounds. The study further aligns with national digital-transformation agendas and global sustainability goals, particularly SDG 4 (Quality Education), SDG 9 (Industry, Innovation and Infrastructure), and SDG 16 (Peace, Justice and Strong Institutions).

Research Method: A quantitative survey design was employed using a structured online questionnaire distributed to 392 Malaysian digital users aged 18 and above. The instrument was developed based on the NIST Cybersecurity Framework and validated through expert review and pilot testing. Reliability analysis showed high internal consistency (overall Cronbach's alpha = 0.914). Descriptive statistics were used to assess construct levels, while Pearson's correlation analysis examined the relationship between cyber-ethics knowledge and digital-ethics compliance. The study tested both a null hypothesis (H_0: no significant relationship) and an alternative hypothesis (H_1: significant positive relationship).

Findings: Results indicated high levels of cyber-ethics knowledge (M = 4.187, SD = 0.715) and digital-ethics compliance (M = 4.205, SD = 0.613). A strong, positive, and statistically significant correlation was found between the two constructs ($r = 0.696$, $p < 0.001$). These findings confirm that individuals with higher ethical knowledge are more likely to demonstrate responsible online behaviour, thereby supporting H_1 and rejecting H_0. Minor gaps were identified in fact-checking and responsible content sharing, indicating the need for continuous ethical reinforcement through education and policy.

Originality: This study contributes new empirical evidence by focusing on adult digital users in Malaysia, extending existing literature beyond student-centred research. It strengthens theoretical understanding of digital citizenship by demonstrating that ethical literacy is a key determinant of ethical behaviour in online environments. Practically, the findings highlight the importance of integrating cyber-ethics education into national curricula, promoting ethics-by-design practices within organisations, and enhancing nationwide digital-ethics awareness campaigns. These implications directly support Malaysia's aspiration to build a value-driven digital society characterized by integrity, accountability, and respect.

Keywords: Cyber-ethics knowledge, digital-ethics compliance, cybersecurity awareness, digital citizenship, ethical literacy, SDG.

1. INTRODUCTION

The global wave of digitalization has reshaped how individuals interact, communicate and access information, and Malaysia is no exception to this transformation. The rapid rollout of digital technologies across sectors such as education, business, public administration and entertainment has accelerated national progress but has also heightened exposure to ethical vulnerabilities in

cyberspace. As reliance on digital platforms continues to intensify, the cultivation of responsible, ethical and sustainable online behavior becomes increasingly critical. This effort aligns closely with the aspirations of Sustainable Development Goal (SDG) 16, which emphasizes the importance of building peaceful, just and accountable institutions through secure and trustworthy access to information.

Cyber ethics encompasses the moral standards and behavioral norms that guide appropriate conduct within digital environments. It includes safeguarding privacy, respecting intellectual property, ensuring accuracy of information and upholding integrity in online communication. Previous research highlights the centrality of ethical knowledge in shaping responsible digital actions; for instance, Kshetri et al. (2023) and Bertino and Matei (2023) emphasize that cyber-ethics knowledge forms the conceptual foundation for sound digital judgement. Likewise, Johar et al. (2023) argue that the integration of Islamic ethical principles within digital behavior enhances moral accountability and cultural alignment, further contributing to ethical resilience among users. These insights support the broader agenda of SDG 4, which aims to ensure inclusive and value-driven quality education capable of nurturing digital citizens with strong ethical grounding.

Despite increasing awareness of ethical expectations in cyberspace, issues such as cyberbullying, misinformation, privacy breaches and data theft remain widespread. Research by Alsheala et al. (2023) and Shahrani et al. (2023) shows that many users have theoretical knowledge of cyber ethics but struggle to translate it into consistent behavioural practice, revealing a persistent gap between awareness and compliance. Understanding how cyber-ethics knowledge influences actual behaviour is therefore essential to designing interventions that strengthen discipline, accountability and responsible digital participation.

While cyber ethics and digital compliance have been widely studied, much of the existing research focuses primarily on student populations, resulting in limited empirical understanding of adult digital users in community and workplace contexts. In Malaysia, few studies examine how cyber-ethics knowledge influences adherence to ethical digital standards, nor do many consider how cultural and religious frameworks, particularly Islamic values, shape ethical digital behaviour. Addressing this gap is crucial in supporting national digital agendas such as MyDIGITAL and Malaysia MADANI, which aim to build a value-based digital society and correspond with SDG 9 through the promotion of ethical, innovative and sustainable digital infrastructure.

Prior research underscores the critical role of ethical education in fostering responsible online conduct. T and K (2024) and Raju et al. (2022) found that structured cyber-ethics instruction significantly enhances ethical compliance, while ENISA (2023) reported that users with higher ethical awareness are less prone to cyber threats. The ethics-by-design model introduced by Ibiricu and Van Der Made (2020), which embeds moral principles directly into digital systems, further reinforces the need to merge technical innovation with ethical considerations to ensure secure and inclusive digital participation.

Given these gaps, this study investigates the relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. The study aims to determine the level of cyber-ethics knowledge, assess the degree of digital-ethics compliance and analyse the relationship between these two constructs. The findings are expected to contribute empirical insights that will inform educational development, awareness campaigns and policy initiatives aimed at strengthening ethical digital citizenship on a national scale.

Grounded in the literature and theoretical framework, the study proposes the following hypotheses: H_0: There is no significant relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. H_1: There is a significant and positive relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. These hypotheses assume

that individuals equipped with higher levels of ethical knowledge are more likely to act responsibly and uphold moral standards in their online interactions.

In summary, this research contributes to the growing discourse on ethical digital citizenship by validating the role of cyber-ethics knowledge in shaping digital-ethics compliance. The study's results are anticipated to support policymakers, educators and digital communities in promoting ethical digital literacy and cultivating a digital ecosystem built on integrity, accountability and respect, thereby advancing the national vision for a digitally resilient society aligned with SDG 4, SDG 9 and SDG 16.

2. LITERATURE REVIEW

2.1 CYBER ETHICS KNOWLEDGE

Cyber-ethics knowledge refers to an individual's cognitive, moral, and behavioral understanding of safe, lawful, and responsible conduct within digital environments. It encompasses awareness of cybersecurity risks, personal data governance, adherence to digital regulations, and compliance with ethical principles during online interactions. This multidimensional construct serves as both the intellectual and moral foundation for responsible digital participation, empowering users to make informed and ethical decisions while navigating technological platforms.

Previous studies have consistently identified a gap between cyber-ethics knowledge and its application in practice. Fikry et al. (2023a, 2023b) attribute this discrepancy to user apathy and the absence of consistent cybersecurity education and training. Kshetri et al. (2023) emphasize that understanding cybersecurity threats such as malware, phishing, and data breaches is a key determinant influencing ethical conduct online. Individuals with greater threat awareness are more likely to exercise caution, responsibility, and integrity in digital environments.

Bertino and Matei (2023) argue that education grounded in systems thinking and ethical communication enhances the capacity to identify, evaluate, and mitigate ethical dilemmas, particularly in AI-driven or data-intensive contexts. The integration of cultural and moral frameworks also strengthens ethical behaviors. Johar et al. (2023) advocate embedding Islamic digital ethics to align user behaviors with societal and spiritual norms, while Wyman et al. (2021) suggest that moral education helps reduce unethical practices such as cyberbullying, hate speech, and online exploitation. Similarly, Panwar et al. (2022) highlight that awareness of cyber laws, including Malaysia's Personal Data Protection Act (PDPA), supports ethical decision-making among users.

Collectively, these studies conceptualize cyber-ethics knowledge as a synthesis of technical literacy, legal awareness, and moral reasoning. Nevertheless, while awareness provides an essential foundation, it does not necessarily ensure consistent ethical compliance. This underscores the importance of continuous digital-ethics education and sustained behavioral reinforcement to close the knowledge–practice gap.

2.2 COMPLIANCE WITH THE DIGITAL CODE OF ETHICS

Compliance with digital ethics refers to the degree to which individuals internalize and practice recognized ethical standards, cybersecurity protocols, and legal obligations when using technology. It includes behaviors such as safeguarding personal data, verifying information accuracy, communicating respectfully, and adhering to both national and international digital regulations.

Alsheala et al. (2023) found that participants who attended cybersecurity-awareness programs exhibited stronger ethical discipline, such as using complex passwords and enabling multi-factor authentication. Similarly, Shahrani et al. (2023) observed that ethical compliance is closely associated with information literacy, particularly in verifying sources to prevent misinformation. Ham and Macnish (2020)

emphasize that digital freedom must coexist with moral accountability, especially in research and professional contexts.

Manjikian (2022) relates compliance to observance of digital laws, including refraining from copyright infringement and unauthorized downloads. Wulandari et al. (2021) interpret respectful communication on social media as a manifestation of ethical responsibility, while Ibiricu and Van Der Made (2020) propose the *ethics-by-design* principle, which encourages both individuals and organizations to integrate moral considerations directly into technological systems and digital-governance frameworks.

Overall, digital-ethics compliance extends beyond technical awareness and requires the internalization of moral values that guide ethical decision-making in daily online activities. Fostering sustainable compliance, therefore, necessitates a balanced approach that combines knowledge acquisition, behavioral reinforcement, and the cultivation of ethical values.

2.3 THE ROLE OF CYBER-ETHICS EDUCATION

Cyber-ethics education serves as a transformative mechanism for shaping ethical awareness and behaviors in digital contexts. T and K (2024) found that formal instruction on cyber ethics significantly enhances compliance with digital regulations and encourages responsible online engagement. Likewise, Raju et al. (2022) report that structured educational interventions increase learners' understanding of ethical accountability in cyberspace.

Embedding ethical content within educational curricula has been widely supported by scholars. Zvereva (2023) asserts that integrating moral reasoning into communication and technology education fosters reflective judgement, while Denchev and Trencheva (2021) advocate incorporating transparency and integrity frameworks to strengthen moral discernment. Bilinga and Mfaume (2024) highlight the importance of sustained initiatives, including professional-development programs and community-based education, to reinforce ethical awareness among educators and the broader public.

Similarly, Skyrda et al. (2020) and Bertino and Matei (2023) recommend explicitly embedding cyber-ethics content within cybersecurity curricula to cultivate comprehensive competence that combines technical proficiency with ethical reasoning. Altogether, the literature suggests that cyber-ethics education extends beyond technical training; it aims to nurture value-driven digital citizens who uphold integrity, accountability, and respect within virtual environments.

2.4 RESEARCH GAP AND RATIONALE

Despite extensive academic discussion on cyber ethics and digital compliance, a significant empirical gap remains, particularly regarding adult digital users in Malaysia. Most prior studies have primarily targeted student populations, resulting in limited empirical evidence on ethical behaviors among the wider community.

Additionally, while international research has examined the relationship between ethical knowledge and behaviors, few studies have contextualized these relationships within Malaysia's cultural and moral frameworks, including Islamic ethical principles. Moreover, there is insufficient evidence on the long-term effectiveness of cyber-ethics education initiatives in sustaining behavioral change.

Consequently, this study endeavors to bridge the identified research gaps by empirically investigating the relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users representing diverse demographic and professional backgrounds. The research is designed to contribute both theoretically and practically by enriching the understanding of ethical digital behavior while offering insights that can strengthen cyber-ethics education, inform national digital policy frameworks, and cultivate ethical digital citizenship aligned with Malaysia's socio-cultural and moral context.

3 METHODOLOGY

3.1 RESEARCH DESIGN

This study employed a quantitative, correlational research design to empirically investigate the relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. This design was selected for its capacity to ascertain both the direction and magnitude of the association between the constructs through statistical means. A quantitative approach was deemed optimal for generating objective, generalizable evidence pertinent to the broader population. Data were collected via a structured online questionnaire, which enabled extensive geographic coverage and efficient dissemination across Malaysia.

3.2 POPULATION AND SAMPLING

The target population comprised Malaysian adults aged 18 years and above who actively utilize the internet for daily activities, including communication, social networking, e-commerce, and online learning. A simple random sampling technique was utilized for survey distribution, ensuring every eligible individual within the sampling frame had an equal probability of selection.

The study secured a final sample of 392 respondents. This sample size aligns with the sampling table proposed by Krejcie and Morgan (1970), which stipulates a minimum of 384 participants for a large population, thereby ensuring statistical power and reliability following data-cleaning procedures.

3.3 RESEARCH INSTRUMENT AND MEASUREMENT

A structured questionnaire was employed as the primary instrument, developed from an extensive literature review and guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014). The framework's five core functions are Identify, Protect, Detect, Respond, and Recover. It provided a solid theoretical basis that ensured the inclusion of both technical and psychosocial aspects of cybersecurity behavior. Insights from contemporary studies, such as Zulkifli et al. (2020), were incorporated to refine item formulation and bridge the gap between knowledge and practice.

For this study, data from three sections of the questionnaire were analyzed: Section A (Demographic Profile), Section E (Cyber-Ethics Knowledge), and Section F (Digital-Ethics Compliance). Each construct was assessed using ten items measured on a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). All items were adapted from validated instruments to ensure conceptual clarity, contextual relevance, and suitability within the Malaysian digital landscape.

Table 1: Measurement of Constructs

Section	Construct	Number of Items	Sample Item
A	Demographic Information	3	"Highest education level"
E	Cyber Ethics Knowledge	10	"I understand what constitutes cyber-ethics and its importance."
F	Digital Ethics Compliance	10	"I refrain from sharing my account passwords with others."

3.4 VALIDITY AND RELIABILITY

To ensure instrument quality, content validity was reviewed by a panel of experts specializing in cybersecurity and educational technology. Reliability testing was conducted through a pilot study involving 30 respondents. The results yielded Cronbach's alpha coefficients above 0.70 for all constructs, signifying satisfactory internal consistency and reliability (Koo & Li, 2016). Specifically, the reliability

coefficients were 0.882 for Cyber Ethics Knowledge and 0.896 for Digital Ethics Compliance, while the overall reliability of the instrument reached 0.914, indicating excellent measurement stability across all items.

Table 2: Reliability Analysis

Construct	Number of Items	Cronbach's Alpha (α)	Reliability Level
Cyber Ethics Knowledge	10	0.882	High
Digital Ethics Compliance	10	0.896	High
Overall Instrument	20	0.914	Very Good

3.5 RESEARCH HYPOTHESES

This study formulates and tests two hypotheses to examine the relationship between cyber-ethics knowledge and digital-ethics compliance among Malaysian digital users. The null hypothesis (H_0) posits that there is no significant relationship between cyber-ethics knowledge and digital-ethics compliance within the target population. Conversely, the alternative hypothesis (H_1) proposes that a significant and positive relationship exists between the two constructs. These hypotheses are grounded in the theoretical premise that individuals with higher levels of ethical awareness are more likely to demonstrate responsible, lawful, and accountable online behaviors. By empirically evaluating these hypotheses, the study aims to confirm whether enhanced cyber-ethics knowledge contributes meaningfully to ethical digital practices, thereby offering insights that support the development of value-driven digital citizenship in Malaysia.

3.6 DATA COLLECTION AND ANALYTICAL PROCEDURES

Data collection was executed over one month using an online survey hosted on the Google Forms platform. The questionnaire link was distributed across various channels, including social media platforms, professional email networks, and digital community forums, to obtain responses from a diverse range of participants. Prior to participation, all respondents were clearly informed of the study's purpose, assured of the confidentiality of their responses, and notified that their involvement was entirely voluntary.

The collected data were processed and analyzed using the Statistical Package for the Social Sciences (SPSS) Version 26. Descriptive statistics, including mean scores and standard deviations, were generated to address the first research objective related to the levels of cyber-ethics knowledge and digital-ethics compliance. To examine the research hypothesis, a Pearson's correlation test was employed to determine the strength and direction of the relationship between the two constructs. The level of significance was set at $p < .05$, and the interpretation of correlation coefficients followed the conventional thresholds proposed by Cohen (1988).

3.7 ETHICAL CONSIDERATIONS

The research adhered to the highest ethical standards. Participation was entirely voluntary and anonymous, with no personally identifiable information collected. Respondents retained the right to withdraw at any point without penalty. All data were stored securely on password-protected systems and are presented solely in aggregate form to uphold confidentiality and anonymity.

This methodological framework, combining a validated instrument, a statistically sound sampling strategy, and robust analytical techniques, ensures the reliability, validity, and generalizability of the study's findings.

4.0 RESULTS AND DISCUSSIONS

This section presents the empirical findings of the study for digital citizenship, describing the demographic profile of respondents, the level of assessment of cyber

ethics knowledge and digital ethics compliance, and an analysis of the relationships between these constructs.

4.1 DEMOGRAPHIC PROFILE OF RESPONDENTS

Table 3: Demographic Profile of Respondents (N=392)

Variable	Category	Frequency	Percentage (%)
Gender	Male	156	39.8
	Female	236	60.2
Age	18 – 25 years	142	36.2
	26 – 35 years	150	38.3
	Above 35 years	100	25.5
Education	Diploma	250	63.8
	Degree or higher	142	36.2

As illustrated in Table 3, the sample consisted of 392 participants. Most respondents were female (60.2 per cent) and aged between 26 and 35 years (38.3 per cent), while 36.2 per cent were aged 18–25 years, and 25.5 per cent were above 35 years. Most of them (63.8 per cent) held a diploma, followed by 36.2 per cent with a degree or higher qualification. These demographics indicate a balanced representation of adult digital users who possess adequate exposure to online environments, making them suitable for assessing cyber-ethics awareness and ethical compliance.

4.2 LEVELS OF CYBER-ETHICS KNOWLEDGE AND DIGITAL-ETHICS COMPLIANCE

Table 4: Descriptive Statistics for Cyber Ethics Knowledge

Item	Brief Statement	Mean	SD	Level
E37	Understanding the cyber ethics concept	4.20	0.69	High
E38	Aware that spreading false information is unethical	4.27	0.70	High
E39	Protecting personal data	4.32	0.65	High
E40	Using strong passwords	4.18	0.76	High
E41	Recognizing fake websites	4.06	0.72	High
E42	Aware of risks on social media	4.10	0.73	High
E43	Understanding phishing	4.12	0.71	High
E44	Avoiding pirated software	4.24	0.68	High
E45	Knowing copyright implications	4.11	0.70	High
E46	Understanding privacy in communication	4.16	0.74	High
Overall Mean		4.187	0.715	High

The descriptive analysis, summarized in Table 4, reveals a high aggregate level of cyber-ethics knowledge among respondents (M = 4.187, SD = 0.715). Awareness was most pronounced for protecting personal data (E39, M = 4.32), while the ability to recognize fake websites (E41, M = 4.06) represented the area with the lowest, though still high, mean score.

Table 5: Descriptive Statistics for Digital Ethics Compliance

Item	Brief Statement	Mean	SD	Level
F47	Use different passwords for accounts	4.30	0.67	High

F48	Do not share passwords	4.33	0.62	High
F49	Avoid offensive posts online	4.21	0.69	High
F50	Verify information before sharing	4.18	0.67	High
F51	Avoid suspicious emails	4.14	0.68	High
F52	Avoid disclosing personal data on unsafe sites	4.17	0.66	High
F53	Do not share confidential company data	4.20	0.61	High
F54	Activate antivirus	4.23	0.62	High
F55	Avoid downloading illegal files	4.09	0.65	High
F56	Avoid spreading false or offensive messages	4.19	0.67	High
Overall Mean		4.205	0.613	High

Similarly, as presented in Table 5, digital-ethics compliance was also high across all measured behaviors (M = 4.205, SD = 0.613). The strongest adherence was observed for not sharing passwords (F48, M = 4.33), while avoiding illegal downloads (F55, M = 4.09) was the least consistently practiced behaviors.

4.3 COMPARISON OF CONSTRUCT MEANS

To provide a clearer picture of respondents' ethical orientation in digital settings, the overall means and standard deviations for each construct were examined. This comparison highlights the extent to which Malaysian digital users possess cyber-ethics knowledge and the degree to which they report complying with ethical practices in their online behaviour.

Table 6: Overall Mean and Standard Deviation by Construct

Construct	Mean	SD	Level
Cyber Ethics Knowledge	4.187	0.715	High
Digital Ethics Compliance	4.205	0.613	High

The results consolidated in Table 6 show that both constructs, namely Cyber Ethical Knowledge and Digital Ethical Compliance, record high mean scores. This analysis revealed that respondents consistently demonstrated high levels of understanding and practice in both constructs. The mean scores for Cyber Ethical Knowledge were 4.187 (SD = 0.715) and for Digital Ethical Compliance 4.205 (SD = 0.613), indicating that Malaysian digital users generally have strong ethical awareness and apply it in their daily online behavior.

The highest scores were observed in personal data protection and password management, while lower means were found to recognize fake websites and avoid illegal downloads, although still in the "high" range. These findings reflect a mature digital ethics culture among respondents, echoing the emphasis by Kshetri et al. (2023) and Bertino and Matei (2023) that ethical knowledge forms the foundation of responsible online engagement. It also supports the argument that ethical knowledge forms the foundation for ethical behavior online (Wyman et al., 2021).

4.4 CORRELATION ANALYSIS

A Pearson correlation analysis was conducted to examine the relationship between Cyber Ethics Knowledge and Digital Ethics Compliance. The results revealed a strong, positive, and statistically significant correlation ($r = 0.696$, $p < 0.001$), indicating that higher levels of cyber-ethics knowledge correspond with greater compliance to ethical digital practices.

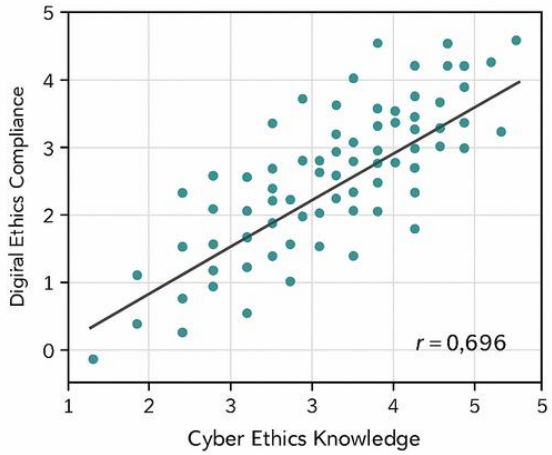

Figure 1: Correlation between Cyber Ethics Knowledge and Digital Ethics Compliance

The scatter plot depicts an upward-sloping linear trend, indicating that participants with higher cyber ethics knowledge scores also recorded higher levels of compliance. The dense clustering of data points around the regression line confirms a strong and consistent relationship between the two constructs.

4.5 DISCUSSION AND IMPLICATIONS

The results provide strong support for H_1: cyber-ethics knowledge significantly and positively predicts digital-ethics compliance among Malaysian digital users. The high correlation ($r = 0.696$, $p < 0.001$) indicates that stronger ethical understanding is associated with more responsible, rule-compliant online behavior, suggesting increasing ethical maturity and awareness of moral and social responsibilities in Malaysia's digital community.

Despite high mean scores for both constructs, small weaknesses emerged, especially in verifying online information and sharing content responsibly. These gaps imply that ethical awareness does not automatically translate into consistent practice, reinforcing the need for ongoing reinforcement through education and targeted interventions.

Several implications follow. Embedding cyber-ethics within the national curriculum and lifelong-learning programs would strengthen ethical digital literacy and directly advance SDG 4 (quality education and responsible citizenship). In parallel, organizations should implement ethics-by-design by integrating ethical principles into digital systems, cybersecurity frameworks, and technological infrastructure, supporting SDG 9 (resilient, responsible innovation). Finally, nationwide digital-ethics campaigns, delivered through government efforts, civil-society partnerships and media outreach, can broaden awareness across demographic groups and promote trustworthy digital engagement aligned with SDG 16 (just, accountable institutions).

Together, these actions can reinforce ethical practice, encourage responsible innovation, and improve digital safety, positioning Malaysia to sustain an integrity-centred digital ecosystem aligned with SDG 4, SDG 9 and SDG 16.

5. CONCLUSIONS

This study provides clear empirical evidence demonstrating the strong connection between Cyber-Ethics Knowledge and Digital-Ethics Compliance among Malaysian digital users. The consistently high mean scores for both constructs, together with the strong positive correlation obtained ($r = 0.696$, $p < 0.001$), indicate that individuals with higher levels of ethical knowledge are more likely to practice responsible and secure digital behavior. These results confirm that ethical literacy functions as the foundation of sustainable digital citizenship, supporting national aspirations under MyDIGITAL and Malaysia MADANI to build a value-driven, integrity-centered digital society.

Theoretically, the findings reinforce existing frameworks suggesting that ethical awareness and ethical behavior are mutually reinforcing. Practically, the study highlights several important implications: the need to embed cyber-ethics education within formal curricula and lifelong learning programs (supporting SDG 4: Quality Education); the importance of encouraging organizations to adopt ethics-by-design principles in their digital systems (supporting SDG 9: Industry, Innovation and Infrastructure); and the value of strengthening nationwide digital-ethics awareness initiatives to foster trustworthy and secure online participation for all age groups (supporting SDG 16: Peace, Justice and Strong Institutions). Together, these measures promote a safer, more ethical and more sustainable digital ecosystem characterized by integrity, accountability and respect.

To advance this field further, future studies are encouraged to employ mixed-methods or longitudinal research designs to explore behavioral, cultural and moral influences on ethical digital engagement. Such efforts will deepen understanding and enhance the development of effective strategies that can further strengthen ethical digital citizenship in Malaysia.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of Politeknik Besut Terengganu and the Department of Information and Communication Technology (JTMK). Appreciation is extended to the Cybersecurity and Digital Ethics students, colleagues from the Commercial Innovation Research Unit for their continuous support and technical assistance throughout the development of this project. The author would also like to thank all respondents for their valuable input during the preparation of this research and all participants whose contributions made this research possible.

REFERENCES

Ab Hamid, N. R., Yusoff, M. S., & Mat Ghani, N. A. (2025). Kesedaran dan amalan keselamatan siber pengguna digital di Malaysia: Implikasi terhadap literasi digital lestari. *Northern Journal of Innovation and Engineering Applications*, *1*, 193–202.

Alsheala, A., Rajagopal, K., & Abdulnabi, M. (2023). Balancing ubiquitous computing: Addressing ethical, privacy, and cybersecurity challenges for responsible and secure implementation in Malaysia. *Proceedings of the IEEE 21st Student Conference on Research and Development (SCOReD),* 111–118. IEEE. https://doi.org/10.1109/SCOReD60679.2023.10563463

Banerjee, S., & Vaish, A. (2022). Cyber ethics: An important concept to become a responsible cyber citizen. *International Journal of Technical Research & Science, 7*(2). https://doi.org/10.30780/ijtrs.v07.i02.001

Bertino, E., & Matei, S. (2023). Educating for AI cybersecurity work and research: Ethics, systems thinking, and communication requirements. *arXiv.* https://doi.org/10.48550/arXiv.2311.04326

Bilinga, M., & Mfaume, H. (2024). Promoting cyber ethics compliance among teachers in Tanzania: What should be done? *Journal of Learning for Development, 11*(3). https://doi.org/10.56059/jl4d.v11i3.980

Cohen J. (1988). *Statistical power analysis for the behavioral sciences (2nd ed.). Hillside, NJ: Lawrence Erlbaum Associates.*

Denchev, S., & Trencheva, T. (2021). Model for cyber ethical and transparency issues in education: A short overview. *Proceedings of INTED2021,* 7583–7588. https://doi.org/10.21125/INTED.2021.1527

ENISA. (2023). *The role of ethical awareness in mitigating cyber threats*. European Union Agency for Cybersecurity.

Fikry, M. F., Salleh, N. M., & Rosli, N. A. (2023a). Factors influencing cybersecurity behaviour among university students. *Malaysian Journal of Learning and Instruction*, *20*(1), 45–60. https://doi.org/10.32890/mjli2023.20.1.3

Fikry, M. F., Rosli, N. A., & Zainuddin, S. (2023b). Awareness vs practice: A case study on cybersecurity habits. *Journal of Information Security Research*, *12*(2), 88–100.

Ham, J., & Macnish, C. (2020). Ethics in cybersecurity research and practice. *Technology in Society, 63,* 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Ibiricu, B. M., & Van Der Made, R. (2020). Ethics by design: A code of ethics for the digital age. *Records Management Journal, 30*(3), 357–371. https://doi.org/10.1108/RMJ-08-2019-0044

Johar, M., Badhrulhisham, A., Mukhtar, M., Othman, K., Meerangani, K., & Ibrahim, A. (2023). Implementation of Islamic cyber ethics on digital platform use. *International Journal of Academic Research in Progressive Education and Development, 12*(1), 1–15. https://doi.org/10.6007/ijarped/v12-i1/14562

Kasang, F., Rahmawati, T., Sari, E., Sakti, A., & Priyanto, A. (2024). Sosialisasi cyber ethics dalam membangun budaya literasi digital di SMK Bina Harapan. *Journal of Community Development, 5*(2). https://doi.org/10.47134/comdev.v5i2.255

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Koo, T. K., & Li, M. Y. (2016). A guideline of selecting and reporting intraclass correlation coefficients for reliability research. *Journal of Chiropractic Medicine, 15*(2), 155–163. https://doi.org/10.1016/j.jcm.2016.02.012

Kshetri, N., Voas, J., & Budalakoti, S. (2023). KnowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students. *Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS),* 298–304. IEEE. https://doi.org/10.1109/ICCCIS60361.2023.10425385

Manjikian, M. (2022). *Cybersecurity ethics.* Routledge. https://doi.org/10.4324/9781003248828

Masrom, M., Zainon, O., Mahmood, N., Wan, H., & Jamal, N. (2012). Information and communication technology issues: A case of Malaysian primary school. *ARPN Journal of Science and Technology, 2*(1), 5–10.

Naaj, M., & Nachouki, M. (2021). Evaluating students' cyber ethics awareness in a gender-segregated environment under the impact of COVID-19 pandemic. *TEM Journal, 10*(3), 1210–1217. https://doi.org/10.18421/tem103-31

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity Version 1.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.02122014

Panwar, A., Baghel, S., Khattar, V., Kumari, S., Sharma, A., & Khattar, V. (2022). A brief study on cyber crime, laws and ethics. *Proceedings of the International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP),* 210–214. IEEE. https://doi.org/10.1109/ICFIRTP56122.2022.10059445

Raju, R., Ahmad, A., Rahman, A., & Hidayah, N. (2022). Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education, 18*(3), 303–316. https://doi.org/10.24191/ajue.v18i3.18967

Shahrani, S., Zainudin, S., & Ahmad, K. (2023). Interactive STEM in cyber awareness learning system. *Proceedings of the International Conference on Electrical Engineering and Informatics (ICEEI),* 1–5. IEEE. https://doi.org/10.1109/ICEEI59426.2023.10346823

Skyrda, A., Merkulova, K., Bychkov, O., & Adaryukova, L. (2020). The introduction of ethics into cybersecurity curricula. *Journal of Digital Learning, 12*(1), 13–24.

T, S., & K, M. (2024). Fostering responsible behavior online: Relevance of cyber ethics education. *Malaysian Online Journal of Educational Technology, 12*(1), 56–69. https://doi.org/10.52380/mojet.2024.12.1.428

Wulandari, E., Triyanto, T., & Winarno, W. (2021). The formation of digital citizenship ethics through Kampung Cyber Civic Community. *Proceedings of the 2nd International Conference on Progressive Education (ICOPE 2020), Universitas Lampung.* https://doi.org/10.4108/EAI.16-10-2020.2305233

Wyman, J., McConnell, R., Rodi, A., & Malcolm, I. (2021). Why should I behave? Addressing unethical cyber behavior through education. *Journal of Digital Ethics, 8*(2), 45–59.

Zulkifli, N. A., Razak, M. F., & Ismail, A. (2020). *Applying NIST cybersecurity framework for awareness education in Malaysian schools*. Journal of Cybersecurity Education, 10(1), 88–103.

Zvereva, E. (2023). Digital ethics in higher education: Modernising moral values for effective communication in cyberspace. *Online Journal of Communication and Media Technologies, 13*(1), 1–13. https://doi.org/10.30935/ojcmt/13033