

Ethical Issues in Computer as an Instrument of Technology Growth

¹Onoja E. Oche. ²Suleiman M. Nasir, Adegboye, ³Y. Kazeem

¹Department of Cyber Security, Federal University of Technology, Minna

^{2 & 3}Computer Science Department, Federal Polytechnic Nasarawa

Corresponding Author: onoskiss@gmail.com

Abstract

The recent technological advancement in digital technology has provided more robust computer-based operations in modern industrial society and its numerous applications in all facets of life is faced with known and unknown threats which have created one or more ethical issues for the computer profession. This research therefore; investigates some of the fundamental aspects of ethical issues in computers, evaluates the influence of computer ethics, and proposes solutions to ethical issues in computers. Adopting the descriptive research design based on cluster sampling through the use of Microsoft Excel tool for data analysis on questionnaires targeted at the population of Computer Professionals at Abuja Metropolis with a sample size of 120, this research observed that software piracy, computer crimes, data breach, privacy, and poor computer ethics awareness limit the growth of digital technology. The study recommends the enforcement of computer ethics at all stages of system development life cycle and organisations.

Keywords: Computer Professionals, Computer Ethics, Privacy, Computer Crime, Software Piracy

Introduction

Recent advances in computing have provided more robust computer-based operations in modern industrial society, including manufacturing, transport and distribution, government, the military, health services, education, and research. This has resulted in unlimited opportunities and increasing acceptability in the general working approach, storage, and sharing of data, which may be abused and used unethically. (Li et al., 2023).

The idea of having advanced technologies in parallel with technological development is prevalent in most developing countries. The adoption of computers and the internet in all facets of society has not come with complementing policies that will safeguard cyberspace, which have created problems such as computer crime, software theft, hacking, viruses, and invasions of privacy. Each of these threats has created one or more ethical issues for the computer profession (Sargolzaei & Huang, 2021).

To avoid this mishap, there is an urgent need for computer users and learner to be conscious of the ethical issues associated with the computer profession, as it will go a long way in optimising the usage and bailing computer users from errors of commission and omission, besides freeing them from offending others and harming themselves (Ioannis et al., 2021).

This research therefore aimed to determine ethical issues in computers as an instrument of technological growth. Specifically, the study investigates: (i) the level of compliance and observance of computer ethics among computer professionals; (ii) the rate at which computer ethics can minimise

computer crime; (iii) the rate at which computer crime ethics can promote technology growth; (iv) the influence of computer ethics on software development and services; (v) the rate at which computer ethics has enhanced security against data breaches and software piracy; (vi) the level of computer ethics implementation among organisations; and (vii) the influence of computer ethics on software piracy and other counterfeit.

Fundamental Aspects of Computing Ethics

Computer ethics encompass personal morals and other legal rules that computer users will apply while using the computer in its various forms, such as software and hardware, for various purposes such as the transmission and usage of information and access to data. It describes various crimes in cyberspace (Li et al., 2023). These crimes may include access to data and information beyond users' privilege level, software plagiarism, hacking, social engineering, and espionage (MacIntyre et al., 2020).

In computing technology, ethics is the analysis of the nature and social impact of computer technology and the formulation of policies to handle computer technology. Computer ethics arises because of a policy vacuum about how technology should be used. Technology is capable of many things. A conceptual vacuum exists, inhibiting policy development. Policymakers are ignorant of the capabilities of new technologies. Individual preferences override sound legal reasoning for a policy (Kim & Routledge, 2018).

Ethical issues in computer science discuss the relationships among facts, conceptualizations, policies, and values with respect to trends in computer technology. This dynamism in technology calls for various policy controls in some areas, such as the ubiquitous use of electronic mail, electronics transfer, reservation systems, the World Wide Web, artificial intelligence, computer security, smart card applications, and information security (Kirsten et al., 2019).

The phrase "emerging technology" refers to the notion of a technology's life cycle, which includes technological innovation or discovery, technological emergence, adoption, technological sublime, and technological surplus. Emerging technologies include, affective computing, ambient intelligence, artificial intelligence, bioelectronics, cloud computing, the future internet, human-machine symbiosis, neuro-electronics, quantum computing, robots, and virtual or augmented reality (Grose et al., 2019).

This recent advancement in information technology has brought a wide acceptance and implementation of smart cards as an ideal device for many transactions such as healthcare, telecommunications, banking, and many other applications, making the world a smarter place. These technological paradigm shifts call for a clear specification of norms and ethics in the cyber domain in order to deter breaches of privacy and other security-related issues (MacIntyre et al., 2020).

The primary goal of computer ethics is to serve as a policy of deterrence for all classes of computer users; besides, it detects what is a computer crime, describes possible factors responsible for computer failure, shows how to protect the computer and software, and helps formulate the boundaries of individual and company privacy policies (Starke et al., 2021). Computer ethics also tries to resolve some issues in cyberspace, such as; the unauthorised use of hardware, the theft of software, disputed rights to products, the use of computers to commit fraud, the phenomenon of hacking and data theft, sabotage in the form of viruses, responsibility for the reliability of output, making false claims for computers, and the degradation of work (Li et al., 2023).

Historical Milestones of Computer Ethics

In the mid-1970s, Walter Maner coined the phrase "computer ethics" to refer to the field of study concerned with ethical issues. He taught an experimental course on the subject at several colleges, as well as workshops and talks at computer science and

philosophy conferences around the United States of America. In 1980, a slew of social and ethical ramifications of information technology were becoming public concerns throughout the world, ranging from computer-enabled criminality to disasters caused by computer breakdowns, breaches of privacy via computer databases, and big litigation challenges over software ownership (Kirsten et al., 2019).

Throughout the 1990s, computer ethics received a lot of attention through many academic mediums. This period introduced a new chapter in computer ethics that focused on security. The critical task in this period is to think that future advances in information technology will make computer ethics more lively and essential than ever before (Kirsten et al., 2019).

Ethical Issues in Computer

The four ethical concerns of the information age are Privacy, Accuracy, Property, and Accessibility (PAPA) (Li et al., 2023). Other studies identified the most urgent ethical problems with computer technology as concerns with secrecy, privacy, access rights, fraud and abuse, patents, copyright, and piracy (Kim & Routledge, 2018).

The development of information technologies and their capacity for processing, storing, and retrieving information and the increased importance of information in decision-making may encourage unauthorised individuals to get personal information by violating privacy (Li et al., 2023).

With the rapid growth of technology, the problem of access rights has become a top concern for IT and the internet. This problem was made more serious for numerous business organisations and governmental organisations by the development of e-commerce and electronic payment systems on the Internet. Unauthorised access to a network on the internet cannot be prevented. Intrusion detection systems are often used to assess whether a user is a legitimate user or an invader (Sargolzaei & Huang, 2021).

According to Kim and Routledge (2018), important ethical problems in computers also include destructive behaviour, piracy, and patents. In the context of computer ethics, harmful behaviour refers to harmful or unfavourable effects on information technology, such as the loss of crucial data, the loss of possessions, the loss of ownership, the destruction of property, and unfavourable significant effects. This code of ethics prohibits anyone from using information

technology in a way that causes harm to any users, employees, employers, or members of the public.

In order to secure computer software before and immediately after a security breach, copyright law offers a very important legal weapon (Kim and Routledge, 2018).

Formulated Rules of Computing Ethics

As computer technology and innovations advance, computer ethics may need to develop. With the introduction of the internet, a wealth of etiquette became available to us. The Net: Use Guidelines and Netiquette (Hess & Fore, 2018) is a well-known collection of online etiquette rules written by Arlene R. Some of this internet etiquette includes, but is not limited to, refraining from responding to phishing (a new scam that asks for personal information about computer users), checking the authenticity of any message requesting you to do something dubious, and avoiding flaming (i.e., sending messages that provoke). Typing in all capital letters is considered shouting and is therefore impolite.

Because of this, several professional organisations in the field of computers, like the Association of Computer Machinery (ACM), the Computer Ethics Institute (CEI), the Management Information Technology (MIT), and others, have created codes of ethics to engage in problematic behaviour, refrain from flaming (i.e., sending provocative remarks), and respond to phishing (a new fraud that requests information about computer users) (Ioannis et al., 2021).

In order to stop some of the aforementioned ethical problems in computing, several rules known as "commandments of computer ethics" have been developed by computer experts. Among them is (i) Do not use a computer to hurt others. (ii) Do not obstruct anyone else's computer work. (iii) Avoid looking into other people's files. (iv) Avoid using a computer to commit theft. (v) Do not fabricate evidence using a computer. (vi). Software that you haven't paid for should not be used or copied. (vii) Never use another person's computer without their permission. (viii) Avoid using the creative work of others for your own purposes. (ix) Do consider how the programme you develop will affect society. (x) Always treat computers with respect and attention (ACM, 2018).

Impact of Computing Ethics

The ethics of computers have had a beneficial impact on the advancement of technology in all areas of

life. It prevents dangerous and unlawful use of computing technology and offers guidelines for concept creation, implementation, application, usage, and protection of computers. (Lester & Dalat-Ward, 2019). Software engineers benefit from computing ethics because it ensures that their efforts will be focused on excellent, ethical development and a respectable profession. This has produced advancements in robotic engineering, data mining, and smart gadgets (Starke et al., 2021).

The founder of the Free Software Foundation, Richard Stallman, thinks that software ownership should never be permitted (Besnard & Arief, 2020). He argues that everyone should have access to free knowledge and that all programmes should be open for everyone to copy, study, and alter. This philosophy gave rise to open-source software, which has generated significant technical advancement (Besnard & Arief, 2020). A similar idea underlies the Android operating system.

According to Ioannis et al. (2021), by enacting users' privacy rules that will foster user confidence and encourage technology adoption, computing ethics, according to Kirsten et al. (2019), has been able to reduce the misuse of personal information generated from social media platforms, smart devices, e-banking (credit and debit cards), e-commerce platforms, and e-health systems.

In Tadayoshi et al. (2023), by discouraging software users from downloading and using software illegally, computing ethics safeguards computer professionals at all levels against the loss of numerous employment opportunities, particularly in the field of software development. By establishing rules that prevent computer users and experts from acting unethically, computer ethics has aided in the advancement of technology. Such standards reduce the frequency of cybercrime, cyberespionage, and other dangerous activity, which in turn fosters technological innovation and improves the security of the computing environment. Computer ethics, therefore, prohibits the theft of intellectual property, including data, software, hardware designs, discoveries, and other material stored online and in the cloud.

Summary Related Literature

The most helpful examples of information technology and computer (IT) growth include current security policies, smart card applications, and information security ethics. To assure the successful effect of information technology, many controls and procedures are adopted (Aderibigbe & Ocholla, 2020).

Emphasising computer ethics, Grosz et al. (2019) stated that the influence of computing ethics on society and human welfare has guaranteed a high standard of living for all, affirmed a responsibility to defend fundamental human rights and respect the diversity of all cultures, and minimised unfavourable effects of computing systems, such as risks to health and safety. This concept forbids the use of computing technology in a manner that endangers users, the public at large, employees, and employers.

Kirsten et al. (2019), discussing confidentiality and privacy issues, observed that computers enable users to access servers that are connected to each other and to users over a network even though they have their own hardware, operating systems, and software tools. Due to the network's extensive distribution, there is a high volume of data or information transmission, which increases the potential for information leaks and privacy violations against specific people or groups. The preservation of data integrity and privacy is a significant concern for IT society and organisations. The privacy problem also includes procedures to preserve the accuracy of data and prevent accidental exposure to improper parties.

Methodology

This research adopted a critical literature review for the knowledge gap and utilised a descriptive research design. A quantitative data analysis approach was adopted using the questionnaire method for data collection through cluster sampling. The data was statistically analysed using Microsoft Excel for maximum accuracy in all calculations and graphical representation. The population was composed of computer professionals in Abuja Metropolis, with a sample size of one hundred and twenty (120), respondents of one hundred and ten (110) and unfilled questionnaires of ten (10). During and after the process of administering questionnaire and other data gathering processes, this research ensured optimal compliance with ethical considerations such as voluntary participation, informed consent, anonymity, and confidentiality.

Results and Discussion

This section presents the analysis of ethical issues in computer based on the research questions/objectives guiding the study.

1. As a computer professional, do you observe most of the ethical principles in your profession, including not

using pirated software, not hurting people with computers, not using computers to commit theft, and not accessing unauthorised data on computers?

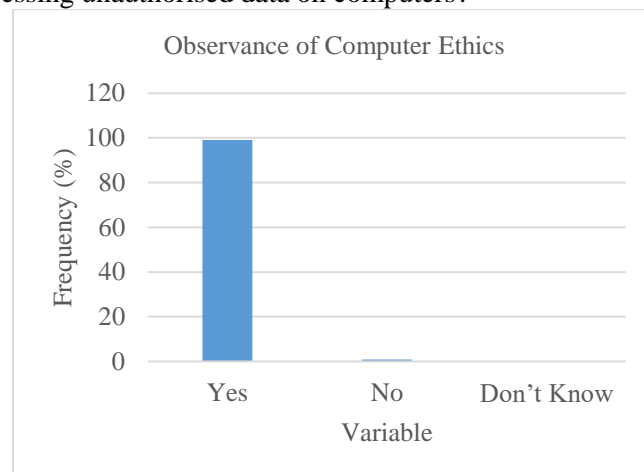


Figure 2.1 Observance of Computer Ethics

Figure 2.1 shows that 99.1% of computer professionals in Abuja metropolis agreed to be guided by ethical principles guiding the computer profession, with just 0.9% disagreeing.

2. Can awareness of computer ethics minimise major computer and technology crimes in the country?

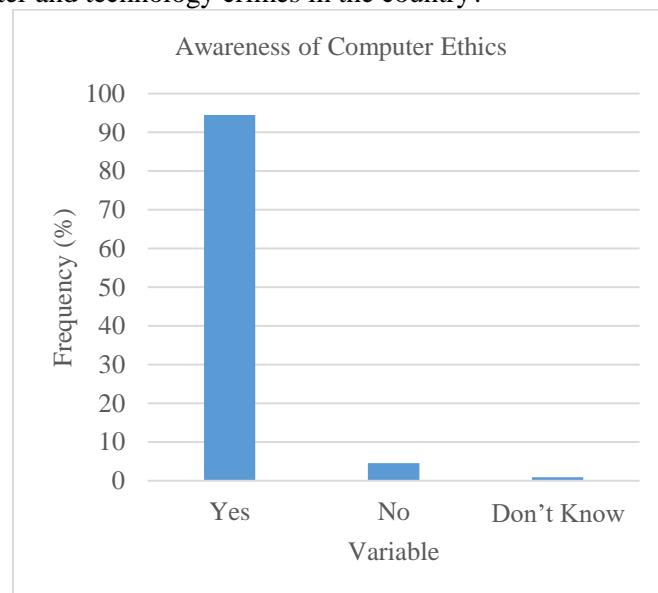


Figure 2.2 Awareness of Computer Ethics

Figure 2.2 shows that 94.5% of computer technology-related professionals agreed that awareness of computer ethics can minimise computer and technology-related crimes in the country, 4.5% disagreed, and 0.9% had no opinion. This agrees with the observation in Aderibigbe and Ocholla (2020).

3. To what extent does computer ethics promote technological growth?

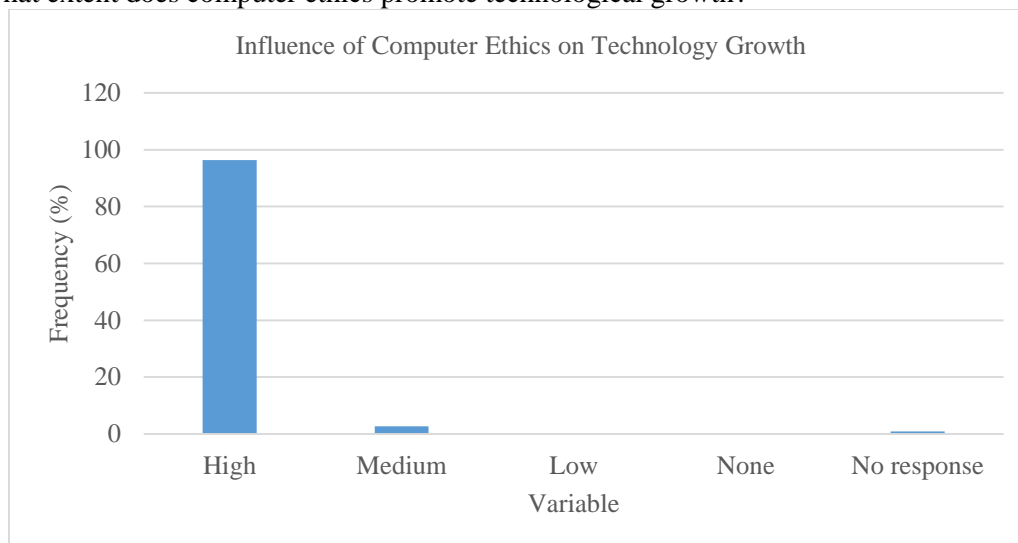


Figure 2.3 Influence of Computer Ethics on Technology Growth

Figure 2.3 show that 96.4% of computer professionals agreed that computer ethics highly promotes technology growth whereas 2.7% agreed that computer ethics has a medium influence on technology growth.

4. To what extent do computer ethics promote standard software development and services?

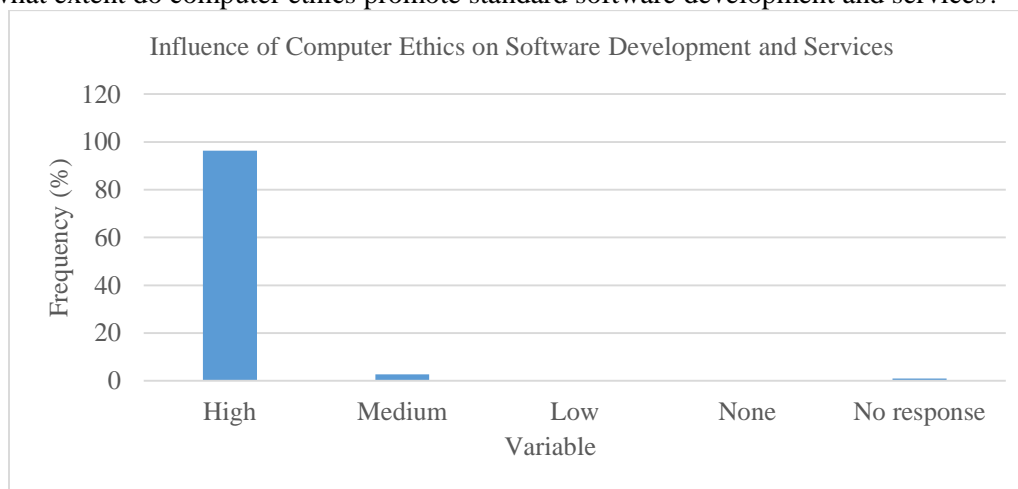


Figure 2.4 Influence of Computer Ethics on Software Development and Services

Figure 2.4 shows that computer ethics has a high, 96.4% positive influence on software development and services, as also stated in Aderibigbe and Ocholla (2020). This implies that there are better software services and designs due to compliance with computer ethics.

5. To what extent have computer ethics enhanced security features against data breaches and privacy in modern technology?

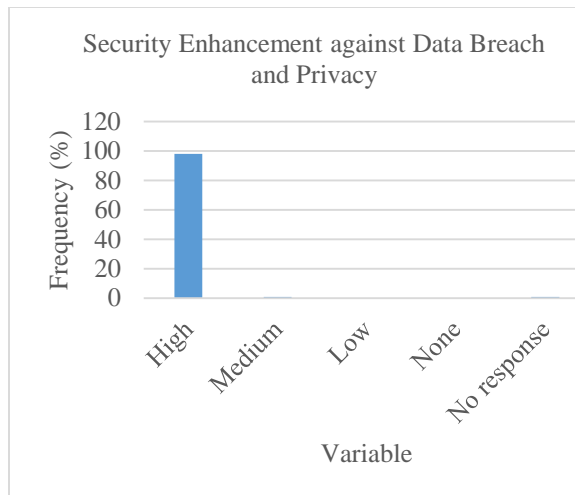


Figure 2.5 Security Enhancement Against Data Breach and Privacy

Figure 2.5 shows that the availability of computer ethics in computer technology has enhanced data and privacy security in modern technology by about

98.2%. Aderibigbe and Ocholla, (2020) observed that compliance with computer ethics has resolved some of the security issues faced by some organisations.

6. What is the level of implementation of computer ethics in your organisation?

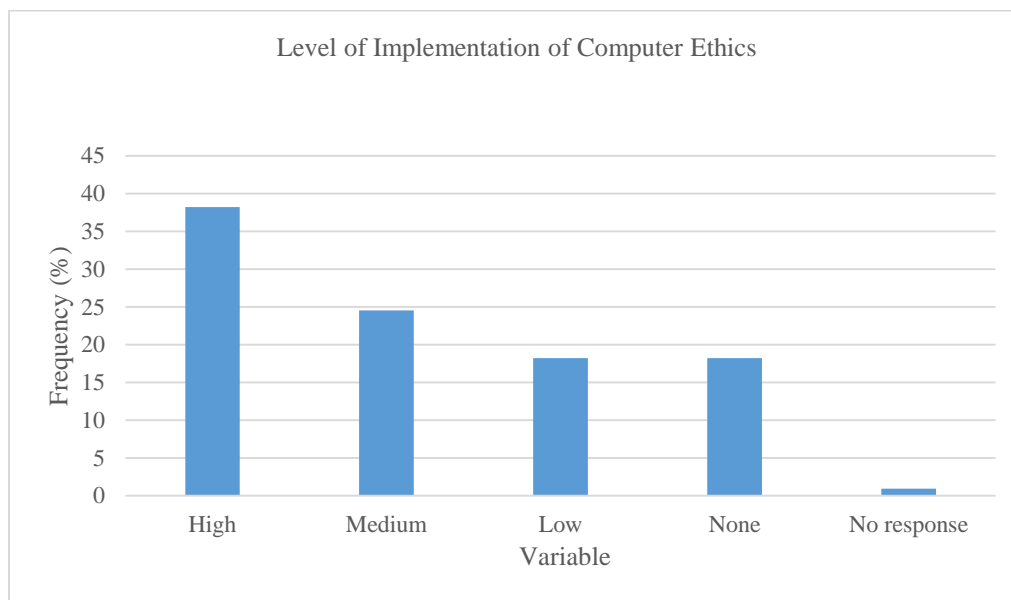


Figure 2.6 Level of Implementation of Computer Ethics

Though computer ethics has a high impact on technology, its implementation in some ICT organisations is 38.2% high, 24.5% medium, and 18.2% low, as shown in Figure 2.6 above.

7. Do you agree that computer ethics have greatly reduced software piracy and other counterfeit technology?

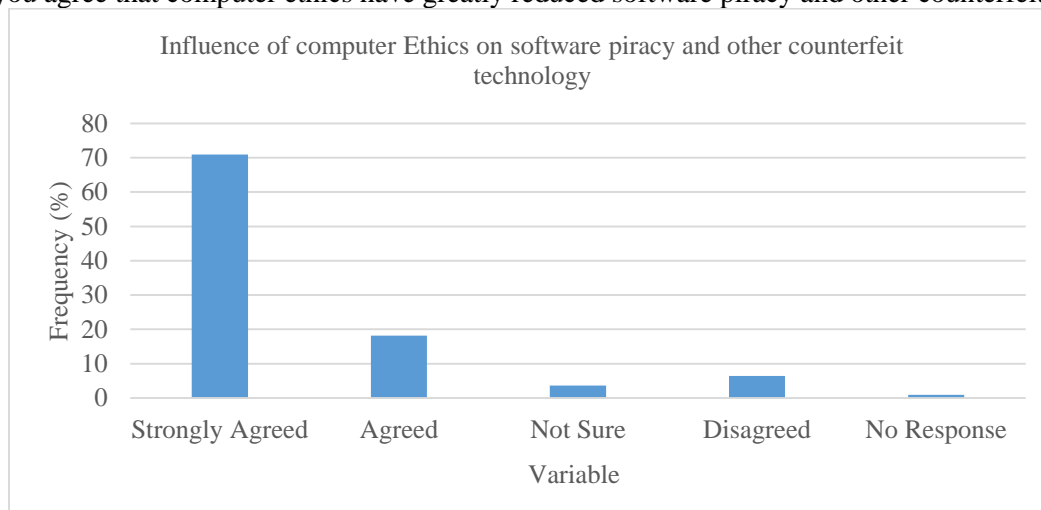


Figure 2.7 Influence of computer Ethics on software piracy and other counterfeit technology

Figure 2.7 shows that computer ethics have reduced software piracy and other counterfeit technology by 70.9%, as also presented in Aderibigbe and Ocholla, (2020).

Conclusion

The paper investigates ethical issues in computers as an instrument of technological growth by highlighting basic concepts, common examples, and various applications of computer ethics. The need for ethical standards among computer professionals was discussed as a major tool for good software development and services.

A survey of opinions from computer and other technology-related fields showed that computer ethics has really contributed to advancement in all spheres of technology.

Recommendation

This study therefore recommends that laws be put in place to enforce the compliance of (i) all the stages of the system development lifecycle, (ii) all organisations that apply digital technology in service delivery, and (iii) the school curriculum with modern computer ethics. Preference should be given to computer ethics awareness creation in order to maximise the rate of adoption.

References

- Kirsten, M., Katie, S., & Jeffery, S. (2019) Business and the ethical implications of technology: Introduction to the symposium, *Journal of Business Ethics*, 160(1), 307–317. <https://doi.org/10.1007/s10551-019-04213-9>
- Sargolzaei, M., W., & Huang, C. (2021). Ethical issues associated with computer as an instrument to technological growth in China. *Journal of Information and Technology*, 5 (1), 1-14. <https://doi.org/10.53819/81018102t5028>
- MacIntyre, J., Medsker, L., & Moriarty, R. (2020). Past the tipping point? AI and Ethics, *Springer*, 2, 65-77, <https://www.researchgate.net/publication/369995486> <https://doi.org/10.1007/s43681-020-00016-1>
- Tadayoshi, K., Yasemin, A., & Wulf, L. (2023). Ethical frameworks and computer security trolley problems: foundations for conversations, Available online at <https://securityethics.cs.washington.edu>.
- Hess, J.L., & Fore, G. (2018). A systematic literature review of US engineering ethics interventions. *Science and Engineering Ethics Journal*, 24 (2), 551–583.
- Aderibigbe, N. A., & Ocholla, D. N. (2020). Insight into ethical cyber behaviour of undergraduate students at selected African universities. *South African Journal of Information Management*, 22(1), 1-8.
- Li, F., Ruijs, N., & Lu, Y. (2023). Ethics and AI: A systematic review on ethical concerns and related strategies for designing with AI in



- healthcare. 4, 28–53.
<https://doi.org/10.3390/ai4010003>
- Besnard, D., & Arief, B. (2020). Computer security impaired by legitimate users. *Journal of Computers & Security*, 23(3), 253-264.
<https://doi.org/10.1016/j.cose.2003.09.002>
- Kim, T. W., & Routledge, B. R. (2018). Informational privacy, a right to explanation and interpretable AI. *2018 IEEE Symposium on Privacy-Aware Computing*.
<https://doi.org/10.1109/pac.2018.00013>
- Starke, G., De Clercq, E., Borgwardt, S., & Elger, B.S. (2021). Computing schizophrenia: Ethical challenges for machine learning in psychiatry. *Psychol. Med.* 51, 2515–2521. [CrossRef] [PubMed]
- Ioannis, S., Damian, G., Brendan, T., Anna, B., & Emma, M. (2021). The teaching of computer ethics on computer science and related degree programmes: An European survey. *International Journal of Ethics Education*, 7 (1), 101-129. <https://doi.org/10.1007/s40889-021-00135-1>
- Lester, L. J.Y., & Dalat-Ward, Y. (2019). Teaching professionalism and ethics in information technology by deliberative dialogue. *Information Systems Education Journal*, 17 (1), 1- 4.
- Grosz, B.J., Grant, D.G., Vredenburg, K., Behrends, J., Hu, L., Simmons, A., & Waldo, J. (2019). Embedded ethics: Integrating ethics across CS education. *Communications of the ACM* 62 (8): 54–61. <https://doi.org/10.1145/3330794>.
- ACM-Association for Computing Machinery, (2018) Code of ethics and professional conduct. <https://www.acm.org/code-of-ethics>