Journal of Computing, Science &Technology
https://focjournal.unidel.edu.ng/
editorjcst@unidel.edu.ng
ISSN: 3043-6818 Print
https://focjournal.unidel.edu.ng

Addressing Ethical Challenges in Educational Research: Data Privacy, Informed Consent, and AI Bias in Cybersecurity Studies

John Oji[1] & Caroline Ochuko Alordiah[2]
[1]Department of Educational Foundations, Faculty of Educations, University of Delta, Agbor, Delta State
[2]Department of Science Education, Faculty of Education, University of Delta Agbor, Delta State, Nigeria
john.oji@unidel.edu.ng[1], caroline.alordiah@unidel.edu.ng[2]
Corresponding Author's Email: *caroline.alordiah@unidel.edu.ng*

ABSTRACT

Article Info

Date Received: 14-01-2024
Date Accepted: 12-04-2024

Keywords:

Artificial Intelligence, Educational Research, Data Privacy, Informed Consent, AI Bias, Ethical Frameworks

This article explores the ethical challenges posed by the integration of artificial intelligence (AI) in educational research, focusing on critical issues such as data privacy, informed consent, and AI bias. As educational institutions increasingly adopt AI technologies for assessment, personalized learning, and administrative efficiencies, the protection of student data becomes paramount. Ensuring robust data privacy measures is essential to prevent breaches that could jeopardize personal information. Furthermore, informed consent is vital, as participants must fully understand the implications of their involvement in AI-driven initiatives. This comprehension promotes trust and guarantees that research procedures adhere to ethical standards. The bias ingrained in AI algorithms is a serious issue as well since it has the potential to exacerbate already-existing disparities and produce unfair results in educational settings. The paper proposes the creation of thorough ethical frameworks that give responsible AI implementation techniques top priority in order to address these ethical issues. Ethical frameworks are proposed to address these issues, including guidelines for safeguarding data, promoting transparency in AI processes, and ensuring informed consent practices that reflect the complexities of AI technology. These kinds of frameworks would improve the integrity of educational research while helping scholars navigate the intricacies of AI technologies. The essay finishes with a call to action for researchers and educational institutions to engage in continuous research and the creation of best practices that decrease ethical issues. The call-to-action urges researchers and institutions to develop ethical frameworks addressing data privacy, informed consent, and AI bias. It calls for further research to establish best practices for fair and transparent AI-driven studies. Working together is essential to advancing moral principles in AI-driven education and fostering an atmosphere that is just, open, and courteous of all participants. In the end, putting ethics first in educational research is both a moral and a legal requirement that supports the integrity and sustainability of AI applications in education.

1.0 INTRODUCTION

In recent years, there has been a noticeable increase in the use of artificial intelligence (AI) in educational research, especially in the cybersecurity arena. AI is being used more and more by academics and educational institutions to analyse massive volumes of data, streamline administrative tasks, and improve learning experiences [1]. Artificial intelligence (AI) is now widely used in cybersecurity research to identify threats, automate security procedures, and forecast potential vulnerabilities. These technologies are used to protect research data, student records, and educational networks from cyberattacks, but their use also raises difficult moral questions [2].

Because artificial intelligence (AI) can handle data more quickly and correctly than traditional methods, it is becoming more and more prevalent in educational and scientific settings. For example, researchers might go through massive datasets using AI-driven techniques to find patterns that would not be immediately apparent through manual examination [3].

This increases the efficiency of identifying security breaches in cybersecurity but also raises the possibility of sensitive student data being misused. Because AI is controversial in educational research, especially in cybersecurity, it is important to critically analyse the ethical issues that arise with its extensive use [4].

This work attempts to investigate the ethical issues that come up in AI-based educational research, especially in cybersecurity settings where student and institutional data are involved. Research approaches are being influenced by AI systems, and using them has ethical ramifications that should not be disregarded. Researchers must consider how emerging technologies impact individuals' rights to privacy and general well-being, from the gathering and storage of sensitive data to guaranteeing fairness in AI-driven processes.

Data privacy preservation is a major ethical challenge in AI-driven educational research. The potential for breaches and misuse increases as student information and personal data are increasingly collected and analysed by AI systems. The idea of informed consent is equally significant and is more intricate when it comes to AI research. It's possible that participants are unaware of the full ramifications of participating in an AI-driven study or how their data will be used. Moreover, AI bias is a problem, especially in cybersecurity research where algorithms could unintentionally reinforce discrimination or distort study findings [2, 5].

In order to preserve the integrity of the research and safeguard the rights of all parties concerned, this paper will emphasise how crucial it is to address these ethical issues. This study centres on three primary ethical issues in educational research powered by artificial intelligence: privacy of data, informed permission, and bias in AI. The use of AI in educational cybersecurity research necessitates close examination in each of these crucial areas. Whereas informed consent focusses on making sure participants are fully aware of and consent to the use of their data, data privacy is concerned with protecting institutional and personal information during the study process. AI bias casts doubt on the impartiality and fairness of the algorithms utilised in research, which is especially pertinent in the field of cybersecurity. These ethical issues will be discussed in this study together with a theoretical framework that will help readers comprehend how they relate to research in education. The paper attempts to provide ways for dealing with these challenges by examining recent literature, ethical guidelines, and case studies. The intention is not only to draw attention to the dangers but also to offer remedies that guarantee ethical, equitable, and transparent research in education that makes use of AI.

1.2 Ethical Considerations in Data Privacy

Defining Data Privacy in the Context of Educational Research:

In the context of educational research, "data privacy" refers to safeguarding private and sensitive information that is gathered from students, teachers, and organisations. This involves making certain that the rights and privacy of participants are respected in the way that such data is utilised, shared, and preserved. Legal frameworks that have created explicit criteria to secure data in educational contexts recently include the Family Educational Rights and Privacy Act (FERPA) in the United States and the General Data Protection Regulation (GDPR) in Europe [6]. These frameworks place strict limitations on the ways in which researchers gather, preserve, and disseminate student data, emphasising the significance of getting express consent, guaranteeing data security, and enabling people to view or have their personal data deleted.

Data privacy is a major concern in educational research incorporating AI, especially in cybersecurity. Researchers must take extra precautions to safeguard critical cybersecurity data, such as student login credentials, network traffic patterns, and personally identifiable information (PII). Access to systems and data that, if compromised, could have major repercussions, including identity theft, unauthorised access to educational records, or financial crime, is frequently required for cybersecurity research. Because of these hazards, researchers must implement strict ethical guidelines and procedures for handling cybersecurity data in learning environments [7,1].

1.1 Protecting Student and Participant Information:

Safeguarding participant and student data is one of the most important ethical issues in educational research integrating AI and cybersecurity. Individuals may suffer serious consequences from unauthorised access to sensitive data, notably when their personal information is used maliciously. The risks of data breaches or misuse rise dramatically in AI-driven educational research because large volumes of data are collected and analysed. The possibility of data exposure through hacking, insider threats, or vulnerabilities in data storage systems is a major worry [8].

Researchers need to put in place comprehensive procedures for data security in order to reduce these dangers. Data protection safeguards should be incorporated into the research process from the beginning, according to theoretical models like the "Privacy by Design" method. This model places a heavy emphasis on taking preventative measures to protect data, like using robust encryption, updating security procedures often, and restricting access to sensitive data [9].

In order to lower the danger of exposure, research involving AI and cybersecurity should also follow the data minimisation principle, which calls for gathering only the information required for the current study. Maintaining access controls, encryption, and routine audits further safeguards participant and student data, bringing research procedures into compliance with ethical and legal requirements for data privacy [8].

1.3 Balancing Access to Data and Privacy:

Finding a balance between the need to access and analyse big datasets and the need to safeguard individual privacy is one of the main challenges in educational research utilising AI. Large data sets are needed for AI-driven analytics to produce forecasts and insights. However, privacy hazards increase with the amount of data collected and processed. For instance, in order to detect any security breaches, AI algorithms may need access to real-time network data in cybersecurity research. Although this can increase the security of educational institutions, it also raises moral concerns regarding how much faculty or student data can be used without jeopardising their privacy [10].

Numerous ways have been put out to deal with this anxiety. Data anonymisation, or the removal or masking of personally identifiable information, enables researchers to use the required data without disclosing participant identities. Data minimisation, which restricts the amount of data collected to that which is absolutely required for the study's goals, is another useful strategy that lowers the risk of privacy violations [11]. Data security during transmission and storage is greatly aided by encryption, which makes sure that the information is safe even in the event of unauthorised access. By using these techniques, researchers can strike a balance between data access and ethical responsibility, protecting participant privacy and upholding the quality of AI-driven educational research [12].

1.4 Informed Consent in AI-Driven Educational Research

Definition and Importance of Informed Consent:

A fundamental tenet of educational research is informed consent, which guarantees that subjects willingly accept to take part in a study after being fully informed of its goals, methods, possible dangers, and rewards. Typically, obtaining informed permission from participants entails giving them a comprehensive explanation of the study, including its goals, the data that will be gathered, and its intended purpose. Additionally, participants are informed of their rights, such as the freedom to discontinue participation in the study at any moment. Informed consent is rather simple in the context of traditional educational research: participants ask questions, researchers explain the study in easily understood words, and they provide their assent once satisfied [13].

However, informed consent becomes much more complicated in AI-driven educational research, especially when cybersecurity is involved. This is due to the fact that AI systems frequently function in ways that are challenging for the typical participant—and perhaps even the researchers themselves—to completely understand. Artificial Intelligence (AI) systems, particularly in cybersecurity, are capable of analysing large volumes of data, making decisions on their own, and changing over time in response to new inputs or learning algorithms. Participants may therefore find it difficult to completely understand how their data is being utilised, which presents significant ethical questions regarding the suitability of informed consent in these kinds of studies [14].

1.5 Challenges in Obtaining Informed Consent for AI and Cybersecurity Studies:

Getting participants to understand and accurately describe the technology is one of the biggest obstacles to obtaining informed consent in AI-driven research. Artificial intelligence (AI) systems are extremely sophisticated; they frequently involve machine learning models, algorithms, and automated decision-making processes that might function in ways that are unclear even to the people who created them. This brings up the moral dilemma of how researchers can adequately teach participants on the workings of the AI without overloading them with technical terms or, on the other hand, reducing the explanation to the point where it becomes inaccurate in reflecting the risks involved [15,16].

A further layer of complexity is added by the dynamic nature of AI systems, especially in cybersecurity. Artificial Intelligence algorithms in cybersecurity have the capacity to evolve and adapt over time, surpassing the original explanations provided to participants during the permission process. This may lead to circumstances where the research takes unexpected turns that were not anticipated when consent was granted. As it gains knowledge, an AI system intended to identify security flaws in school networks, for instance, may be able to analyse more data than was initially disclosed in the consent form. Researchers may find it challenging to fully inform participants about the potential uses of their data due to this unpredictability, which raises questions about whether or not participants are really giving "informed" consent [1].

1.6 Ensuring Transparency and Understanding:

In order to tackle these obstacles, scholars need to embrace novel theoretical frameworks and approaches that guarantee clarity and foster authentic comprehension throughout the authorisation procedure. A paradigm that allows for this is "dynamic consent," which lets participants change or revoke their consent as the study progresses. In AI-driven research, where the algorithms used may vary over time, this method is especially helpful. By providing dynamic consent, participants can modify their level of participation in response to new study findings and stay informed about how their data is being used [17].

Making sure that participants have access to clear and understandable information on AI systems is another crucial tactic. This entails simplifying intricate AI ideas while retaining the subtlety required to effectively communicate the dangers and consequences of the study. In addition to avoiding using too much technical jargon, researchers should resist the urge to simplify the technology. Alternatively, they can utilise interactive demos, analogies, and visual aids to help participants understand how AI systems function and how their data will be used in the study [18].

Researchers can provide thorough, understandable descriptions of how AI algorithms work, the types of data they will handle, and any possible concerns in order to improve understanding even further. Crucially, participants ought to have the chance to enquire and seek clarification as needed until they are satisfied that they comprehend the research in its entirety. Sustaining participants during the research process can be achieved by offering continuous assistance, such as additional materials or follow-up sessions [19].

1.7 AI Bias and Its Impact on Educational Research Understanding AI Bias:

The term "artificial intelligence bias" describes the deliberate and frequently inadvertent bias that develops in artificial intelligence algorithms as a result of the environments in which they are used, the data they are trained on, or their design. Bias, for instance, might appear in cybersecurity solutions when algorithms mistakenly highlight some user profiles or data types as security risks more frequently than others due to systemic flaws [20]. For example, if the training data contained more samples from a given demographic group, then an AI system meant to identify malicious activities might be biassed towards that group. This might result in biassed outcomes and unfair treatment.

AI bias has important ramifications for educational research. Biassed algorithms have the potential to skew study findings when AI systems are employed to evaluate student data or forecast results. For instance, biassed algorithms may erroneously assign higher or poorer academic potential to particular demographic groups, such as those based on race, gender, or socioeconomic background, in a research evaluating students' performance or behaviour using AI techniques. This could result in study findings that support current disparities or preconceptions, eroding the research's credibility and sustaining systematic injustice [1].

1.8 AI Bias in Educational Settings:

Artificial intelligence (AI) systems are not impervious to social biases found in the real world, particularly those employed in educational research. In actuality, prejudices pertaining to socioeconomic class, gender, and race are frequently reinforced by these institutions. An AI system may generate biassed insights, for instance, if it is used to examine student involvement in cybersecurity programs and the training data for that system is disproportionately biassed towards students from a specific socioeconomic or ethnic background. As a result, preconceptions may be strengthened, such as the idea that pupils from marginalised or under-represented groups should be held to lesser standards. Additionally, students from particular communities may be disproportionately targeted by AI technologies used for cybersecurity research, exacerbating already-existing discrepancies in how security threats are managed or perceived [21].

Making sure that AI-driven educational research is equitable and inclusive is an ethical dilemma. Artificial intelligence (AI) bias has the potential to unfairly disadvantage or exclude some students, which is in direct opposition to the main objectives of educational research, which are to establish inclusive and equal learning environments. The quality and impartiality of educational research, as well as the educational systems it aims to enhance, are at risk when it makes use of AI techniques that unintentionally reinforce and reflect societal biases [22].

1.9 Theoretical Solutions to AI Bias:

There are ethical as well as technical solutions needed to address AI bias in educational research. Technically speaking, making sure AI systems are trained on a variety of datasets that fairly represent the populations they will be applied to is one efficient way to mitigate bias. Researchers can lessen the possibility of biassed results by using data from a variety of demographic categories, including those related to race, gender, socioeconomic position, and other factors. But in order to guarantee diversity, this strategy necessitates careful consideration when choosing data and ongoing oversight [23].

Regular algorithm auditing is another important remedy. This entails methodically checking artificial intelligence (AI) systems for biases and errors. Through auditing, researchers can find out how and where biases enter the system and modify their algorithms or procedures accordingly. In order to address this difficulty in a more reliable and scalable manner, frameworks for detecting biases in AI systems are currently being created [24].

Researchers have an ethical obligation to use models that put diversity and fairness first. Fairness-aware machine learning is one such paradigm that incorporates fairness restrictions into AI algorithm development to guarantee equitable treatment across all demographic groups. With the aid of this method, researchers can intentionally create AI systems that reduce discrimination and respect moral principles. Another crucial ethical factor is transparency. Researchers must make sure that all relevant parties, such as participants and educators, are informed of the dangers associated with their use of AI tools and be upfront about any potential limits or biases [2].

1.10 The Intersection of Cybersecurity and AI Ethics in Education

Cybersecurity's Role in Safeguarding Educational AI Systems:

AI technologies are becoming essential to education in the current digital era, improving research, data analysis, and learning. AI is becoming more and more integrated into educational environments, but it also makes it more susceptible to cyberattacks. Researchers, stakeholders, and educational institutions must understand that hackers are aiming to take advantage of data vulnerabilities in these AI systems because they process sensitive student data or produce insights from large datasets [16].

There is a serious ethical conundrum with AI systems in education being vulnerable to cyberattacks. The moral obligation to secure these systems goes beyond data protection; it also entails maintaining the confidence of educators, students, and organisations that depend on these AI tools for better decision-making and instruction. In the event of a breach, the stolen data may cause permanent harm to both students and teachers, such as identity theft, discrimination, and privacy violations. Therefore, in order to fulfil their ethical duties, academic institutions and researchers must not only use cutting-edge AI technologies but also put strong cybersecurity measures in place to guard against illegal access, data corruption, and AI algorithm manipulation [25].

The significance of ethical data management and cybersecurity procedures in educational research must be emphasised in this context. Any institution using AI for education must adhere to ethical standards by protecting user privacy, enforcing encryption protocols, and improving AI system defences on a regular basis. Cybersecurity breaches are bad for the reputation of the organisation as well as the personal and professional integrity of the researchers. Because of this, cybersecurity and ethical issues in educational AI research are linked, necessitating ongoing vigilance on the part of researchers and organisations to safeguard the systems they utilise [11].

1.11 Ensuring Ethical AI Deployment in Cybersecurity Education:

The interaction between AI and cybersecurity in education concerns not just safeguarding AI systems but also the ethical use of these two domains. When combined with AI in education, cybersecurity is an ethical field that needs to be carefully considered to make sure these technologies are responsible and safe. Because artificial intelligence (AI) is becoming more and more prevalent in educational research, cybersecurity experts are responsible for protecting these systems from outside threats and handling any ethical concerns that may arise [26].

Here, there are two roles to play: one is to defend AI systems from cybersecurity attacks, and the other is to make sure these systems are developed and used in an ethical and just way. Researchers and educational institutions need to develop and apply AI tools that adhere to ethical principles like responsibility, transparency, and justice in addition to being safe. This duty entails making assured that AI-driven cybersecurity tools do not reinforce prejudice or unfairly target particular populations, as well as ensuring that AI systems are intelligible and explicable to the researchers who employ them [25].

Furthermore, it is imperative to incorporate ethical issues into the development and instruction of AI systems as AI becomes more prevalent in cybersecurity education. Fairness, inclusivity, and privacy should be the top priorities when developing AI tools to prevent unintentionally harming certain researchers or students. For instance, an AI tool used in cybersecurity education needs to evaluate students' skills fairly across backgrounds, and cybersecurity researchers need to be aware of how AI systems affect student privacy or reinforce prejudice [26].

1.12 Theoretical Frameworks for Ethical Decision-Making

Ethical Theories Applicable to AI and Cybersecurity Research:

Making ethical decisions is crucial in the quickly changing fields of artificial intelligence (AI) and cybersecurity research in educational settings. The complicated moral terrain around AI technologies and its consequences for data privacy, informed consent, and algorithmic bias can be navigated by using a number of fundamental ethical ideas. Utilitarianism, deontology, and virtue ethics are a few of these that provide distinctive viewpoints that might help scholars make moral decisions [27].

A consequentialist theory called utilitarianism was established by philosophers such as Jeremy Bentham and John Stuart Mill. It places a strong emphasis on the significance of maximising happiness or well-being for all. Utilitarianism encourages academics to assess the possible advantages and disadvantages of AI applications in the context of cybersecurity and artificial intelligence. When applying artificial intelligence (AI) to education, for example, researchers need to think about how best to use the technology to improve learning results for most students while minimising detrimental effects on individuals, especially those from marginalised areas. This method prioritises the larger good and calls for a thorough evaluation of the trade-offs associated with implementing AI technologies in educational research [8].

Conversely, deontology is based on the idea that some behaviours are intrinsically good or bad, independent of the results. A key role in deontological ethics, Immanuel Kant highlighted the significance of obligation and obedience to moral laws. This viewpoint emphasises the significance of maintaining ethical standards, such as respect for people's rights, informed permission, and privacy, in educational research incorporating AI. Thus, it is the responsibility of researchers to guarantee that participants are treated with dignity and that their autonomy is maintained at all times during the research process. This framework requires educational institutions, independent of the research's possible benefits, to develop and implement ethical norms that protect participants' rights [10].

Aristotle is credited with creating virtue ethics, which places more emphasis on the moral agent's qualities and character than on the laws or results of their deeds. When working with AI technology, this method encourages researchers to develop moral qualities like honesty, integrity, and compassion. Specifically, to educational research, virtue ethics emphasises the significance of cultivating a study culture that places a high value on moral behaviour and gives participants' welfare first priority. Scholars are urged to consider their intentions and the moral consequences of their deeds, advancing a comprehensive understanding of ethics that includes both individual morality and professional accountability [5].

Through the integration of utilitarianism, deontology, and virtue ethics, researchers are able to effectively navigate the intricate fields of artificial intelligence and cybersecurity. Educational institutions are able to strike a balance between innovation and ethical integrity because each framework provides unique insights and tools that when combined, enable ethical decision-making.

1.13 Developing an Ethical AI Framework for Educational Research

Creating a thorough ethical AI framework is crucial to addressing the moral dilemmas raised using AI in educational cybersecurity research. In addition to assisting researchers in reaching moral conclusions, this framework should guarantee that the application of AI technology complies with accepted moral standards. A framework of that kind might be built around a number of essential elements.

First, the ethical theories listed above should be incorporated into the suggested ethical AI framework. For instance, it might stress the significance of protecting participants' rights and privacy (deontology), optimising benefits while minimising damage (utilitarianism), and promoting a culture of moral research practices (virtue ethics). Researchers would be encouraged to evaluate the ethical consequences of their work thoroughly and from a variety of angles by using this multifaceted method.

Second, to guarantee that participants are fully aware of the implications of AI technologies employed in research, the framework should contain explicit rules for getting informed consent. This involves being open and honest about the nature of the data gathered, how AI algorithms work, and any possible hazards. Informed consent is given priority in the framework, which upholds the moral duty to respect people's agency and autonomy.

The ethical AI framework also needs to take ethical responsibility and technological progress into account. Researchers may come under pressure to use cutting-edge instruments that promise increased efficacy and efficiency as AI technologies advance. Nonetheless, the approach ought also to serve as a reminder to researchers of their moral obligations to rigorously assess the wider ramifications of such discoveries. This entails taking into account the possibility of biases in AI algorithms, the repercussions on disadvantaged populations, and the long-term implications on educational justice and equity.

Lastly, the framework need to encourage continuous ethical instruction and discussion between stakeholders and researchers in academic contexts. Research on AI and cybersecurity will continue to prioritise ethical considerations if ethical issues are not consistently engaged with. Workshops, seminars, and group discussions with the goal of establishing an ethical practice community within educational research could be examples of this.

1.14 Ethical Framework for Artificial Intelligence in Educational Research

Table 1: Ethical Framework for Artificial Intelligence in Educational Research

Element	Description	Considerations
Purpose of Research	Clearly define the research objectives	Ensure alignment with educational

	and goals.	values and societal benefit.
Informed Consent	Obtain voluntary and informed consent from participants before involvement.	Provide clear information about the study's purpose, risks, and benefits.
Confidentiality	Maintain the privacy and confidentiality of participant data.	Implement measures to protect sensitive information and ensure data security.
Data Integrity	Ensure the accuracy and honesty of data collection and reporting.	Avoid fabrication, falsification, or misrepresentation of data.
Ethical Review	Subject research proposals to an ethics review process for evaluation and approval.	Utilize established ethical guidelines and frameworks for review [2].
Respect for Participants	Treat all participants with dignity and respect throughout the research process.	Acknowledge cultural, social, and personal differences among participants.
Beneficence	Ensure that the research contributes positively to the educational field and the participants involved.	Minimize potential risks and maximize benefits for participants and society.
Justice	Promote fairness in the selection of participants and the distribution of benefits and burdens of research.	Avoid exploitation of vulnerable populations and ensure equitable access to benefits.
Reporting and Dissemination	Share research findings responsibly, ensuring accurate representation of results.	Engage in transparent practices to communicate findings to the wider community.
Continuous Ethical Reflection	Regularly assess ethical considerations throughout the research process and be open to feedback.	Create a culture of ethical awareness and responsiveness in research practices.

Ethical Principles: Ethical behaviour in research is guided by these fundamental notions. Respect for people is one of the common values (informed consent), beneficence (maximizing benefits while minimizing harm), and justice (fair distribution of research benefits and burdens).

Research Design Considerations: Researchers need to make sure that their designs adhere to ethical standards and include safeguards for the welfare, rights, and dignity of participants. This entails taking participant safety into account when designing the methodology, sampling strategies, and data gathering approaches.

Informed Consent: In order for potential volunteers to make an informed decision about participating in the study, researchers must give them thorough information on the study's goals, risks, and rewards.

Data Privacy and Security: Researchers need to put plans in place to safeguard private information from prying eyes, maintain confidentiality, and adhere to applicable data protection regulations. This is especially crucial in educational environments when students' personal information is at stake.

AI and Cybersecurity Considerations: Given the increasing use of AI in education, the framework addresses ethical concerns related to AI, such as algorithmic bias, transparency, and the ethical use of AI tools in assessments and data analysis.

Assessment of Ethical Compliance: The framework should include mechanisms for ongoing assessment of ethical compliance throughout the research process, ensuring that researchers remain accountable for their ethical responsibilities.

Stakeholder Engagement: It is imperative to involve many stakeholders, such as educators, students, and community members, in order to recognise and tackle ethical issues pertaining to the research. The research process is made more inclusive and trustworthy by this cooperative approach.

1.15 Recommendations for Ethical Practices

Recommendations for Researchers

Gaining informed permission should be a top priority for researchers, who should do this by outlining the goals, methods, possible dangers, and advantages of the study. It should be possible for participants to leave at any moment and not incur any fees. Create studies with the intention of reducing damage and maximising benefits. This may entail carrying out risk analyses and offering assistance to research participants who might feel distressed. Make sure that hiring procedures are equitable and represent the variety of the community. The costs and rewards of research should be divided equally, and participation should be equitable for all. Protect personal information by putting strong data protection mechanisms in place, such as secure data storage and anonymisation. It is crucial to abide by applicable data protection laws, such as the GDPR. Researchers should be open and honest about the algorithms they use, the data they use to train their models, and any potential biases in these technologies when they use AI tools. Frequent audits of AI systems can aid in minimising bias and ensuring fairness. In order to ensure that the study represents the needs and viewpoints of many communities, involve a variety of stakeholder groups in the research design phase to gain feedback and insights.

Institutions, especially those involved in cybersecurity and artificial intelligence (AI), should create and uphold thorough ethical norms that mirror best practices in research. These policies ought to be examined and revised on a regular basis. Institutions ought to give researchers access to ethical training courses, equipment for carrying out moral research, and advice on moral conundrums, among other resources and assistance. Institutions should have explicit policies that cover ethical issues in AI-based educational research, together with procedures for reporting and resolving ethical transgressions. Form ethics committees to examine research proposals, evaluate adherence to ethical standards, and offer suggestions for reducing ethical hazards. These committees ought to be made up of a varied group of people with backgrounds in law, research ethics, and related fields. Establish mandated ethics education programs for researchers, with an emphasis on cybersecurity and artificial intelligence-specific concerns. The significance of data protection, informed consent, and ethical frameworks for making decisions should all be covered in this training.

2.0 CONCLUSION

To protect the interests of both students and educators, the integration of artificial intelligence (AI) in educational settings poses a number of significant ethical concerns. The most important concern is data privacy, which includes safeguarding personal data gathered by AI systems. Responsible handling of student data is essential since security breaches have the potential to cause serious harm. Furthermore, participants must completely comprehend the ramifications of their involvement in AI-driven research and technology, which makes informed consent an essential component. This comprehension is necessary to promote confidence between researchers and participants as well as to adhere to ethical standards. Another significant issue is the bias present in AI algorithms; machine learning models have the potential to reinforce and magnify preexisting biases in historical data, producing unfair and discriminating results in educational settings.

It is crucial to create strong ethical frameworks that give these concerns top priority in AI-driven educational research because of these ethical considerations. These frameworks will offer standards for moral behaviour, guiding researchers through the challenges of using AI technologies in a responsible manner. In the end, adhering to ethical principles is a moral requirement that upholds the integrity of educational research rather than merely being a legal requirement.

Both academic institutions and researchers need to issue a call to action in order to successfully solve these ethical issues. The development and application of AI technologies in education must adhere to the highest ethical standards, thus it is crucial to support continued research into best practices that reduce the ethical hazards connected with AI. Researcher, institutional, and policymaker collaboration will be essential to improving ethical AI practices and creating an inclusive, transparent, and equitable learning environment for all.

3.0 REFERENCES

[1]. L. Huang (2023): Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. *Science Insights Education Frontiers*, *16*(2), 2577–2587. https://doi.org/10.15354/sief.23.re202

[2]. M. Ashok Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for Artificial Intelligence and Digital technologies. *International Journal of Information Management*, *62*, 102433–102433. https://doi.org/10.1016/j.ijinfomgt.2021.102433

[3]. Yu, L., & Yu, Z. (2023). Qualitative and quantitative analyses of artificial intelligence ethics in education using VOSviewer and CitNetExplorer. *Frontiers in Psychology*, *14*. https://doi.org/10.3389/fpsyg.2023.1061778

[4]. Jeyaraman, M., Ramasubramanian, S., Balaji, S., Jeyaraman, N., Nallakumarasamy, A., & Sharma, S. (2023). ChatGPT in action: Harnessing artificial intelligence potential and addressing ethical challenges in medicine, education, and scientific research. *World Journal of Methodology*, *13*(4), 170–178. https://doi.org/10.5662/wjm.v13.i4.170

[5]. Akgün, S., & Greenhow, C. (2021). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, *2*(3), 431–440. https://doi.org/10.1007/s43681-021-00096-7

[6]. Cormack, A. (2016). A Data Protection Framework for Learning Analytics. *Journal of Learning Analytics*, *3*(1). https://doi.org/10.18608/jla.2016.31.6

[7]. Oji, J., & Alordiah, C. O. (2024). Navigating Ethical Quandaries in Nigerian Academia: A Conceptual Framework for Establishing Effective Research Ethics Boards and Ensuring Compliance. *NIU Journal of Educational Research*, *10*(1), 83-93. https://doi.org/10.58709/niujed.v10i1.1939

[8]. Nguyen, A., Ngo, H. N., Hong, Y., Dang, B., & Nguyen, B.-P. T. (2022). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, *28*(4), 4221–4241. https://doi.org/10.1007/s10639-022-11316-w

[9]. Siau, K., & Wang, W. (2020). Artificial Intelligence (AI) Ethics. *Journal of Database Management*, *31*(2), 74–87. https://doi.org/10.4018/jdm.2020040105

[10]. Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T. T., Shum, S. B., Santos, O. C., Rodrigo, Ma. M. T., Cukurova, M., Bittencourt, I. I., & Koedinger, K. R. (2021). Ethics of AI in Education: Towards a Community-Wide Framework. *International Journal of Artificial Intelligence in Education*, *32*(3), 504–526. https://doi.org/10.1007/s40593-021-00239-1

[11]. Klímová, B., Pikhart, M., & Kacetl, J. (2023). Ethical issues of the use of AI-driven mobile apps for education. *Frontiers in Public Health*, *10*. https://doi.org/10.3389/fpubh.2022.1118116

[12]. Akgün, S., & Greenhow, C. (2021). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, *2*(3), 431–440. https://doi.org/10.1007/s43681-021-00096-7

[13]. Busch, F., Adams, L. C., & Bressem, K. K. (2023). Biomedical Ethical Aspects Towards the Implementation of Artificial Intelligence in Medical

Education. *Medical Science Educator*, *33*(4), 1007–1012. https://doi.org/10.1007/s40670-023-01815-x

[14]. Jeyaraman, M., Ramasubramanian, S., Balaji, S., Jeyaraman, N., Nallakumarasamy, A., & Sharma, S. (2023). ChatGPT in action: Harnessing artificial intelligence potential and addressing ethical challenges in medicine, education, and scientific research. *World Journal of Methodology*, *13*(4), 170–178. https://doi.org/10.5662/wjm.v13.i4.170

[15]. Alordiah, C. O. (2023). Appreciating the AI revolution: Empowering educational researchers through AI tools for writing research articles. Zamfara International Journal of Humanities (ZAMFARA IJOH), 2(1), 178-191. https://doi.org/zamijoh.2023.v02i01.013

[16]. Kooli, C. (2023). Chatbots in Education and Research: A Critical Examination of Ethical Implications and Solutions. *Sustainability*, *15*(7), 5614–5614. https://doi.org/10.3390/su15075614

[17]. Ferrer, X., van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and Discrimination in AI: A Cross-Disciplinary Perspective. *IEEE Technology and Society Magazine*, *40*(2), 72–80. https://doi.org/10.1109/mts.2021.3056293

[18]. Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Jones, P., Chłosta, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers in Surgery*, *9*. https://doi.org/10.3389/fsurg.2022.862322

[19]. Morley, J., Elhalal, A., Garcia, F., Kinsey, L., Mökander, J., & Floridi, L. (2021). Ethics as a Service: A Pragmatic Operationalisation of AI Ethics. *Minds and Machines*, *31*(2), 239–256. https://doi.org/10.1007/s11023-021-09563-w

[20]. Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. *Journal of Business Research*, *129*, 961–974. https://doi.org/10.1016/j.jbusres.2020.08.024

[21]. Alasadi, E. A., & Baiz, C. R. (2023). Generative AI in Education and Research: Opportunities, Concerns, and Solutions. *Journal of Chemical Education*, *100*(8), 2965–2971. https://doi.org/10.1021/acs.jchemed.3c00323

[22]. Brown, S., Davidovic, J., & Hasan, A. (2021). The algorithm audit: Scoring the algorithms that score us. *Big Data & Society*, *8*(1), 205395172098386–205395172098386. https://doi.org/10.1177/2053951720983865

[23]. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera–Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896–101896. https://doi.org/10.1016/j.inffus.2023.101896

[24]. Masters, K. (2023). Ethical use of Artificial Intelligence in Health Professions Education: AMEE Guide No. 158. *Medical Teacher*, *45*(6), 574–584. https://doi.org/10.1080/0142159x.2023.2186203

[25]. Slimi, Z., & Villarejo-Carballido, B. (2023). Navigating the Ethical Challenges of Artificial Intelligence in Higher Education: An Analysis of Seven Global AI Ethics Policies. *TEM Journal*, 590–602. https://doi.org/10.18421/tem122-02

[26]. Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). Ethical principles for artificial intelligence in K-12 education. *Computers and Education Artificial Intelligence*, *4*, 100131–100131. https://doi.org/10.1016/j.caeai.2023.100131

[27]. Saylam, S., Duman, N., Yildirim, Y., & Satsevich, K. (2023). Empowering education with AI: Addressing ethical concerns. *London Journal of Social Sciences*, *6*, 39–48. https://doi.org/10.31039/ljss.2023.6.103