A SYSTEMATIC REVIEW OF DATA PRIVACY AND SECURITY IN NIGERIA'S ONLINE EDUCATION: ETHICAL CONSIDERATION AND CHALLENGES

Anthony Etta Bisong
Department of Educational Technology
Faculty of Educational Foundation Studies
University of Calabar, Cross River State - Nigeria
https://orcid.org/0000-0002-2878-7007

Imoke John Eteng
Department of Educational Technology
Faculty of Educational Foundation Studies
University of Calabar, Cross River State - Nigeria

Mrs. Imoke John Mary
Department of Environmental Health
College of Health Technology, Calabar
Cross River State - Nigeria

Abstract
The rapid growth of online education in Nigeria raises ethical concerns about data privacy and security. This study explores these concerns in Nigeria's online education. This work provides an overview of online education's evolution, challenges, and data privacy issues. Key ethical considerations, including informed consent, user rights, data retention, transparency, accountability, and equitable access, were examined. The paper assessed current data privacy and security practices, identified challenges and gaps, and proposed recommendations. Recommendations covered policy and regulation, technological solutions, and education as well as awareness initiatives. In conclusion, this review highlights the ethical importance of data privacy and security in Nigeria's online education and offers strategies to enhance data ethics and safeguard individuals' information while supporting the growth of online learning platforms.

Keywords: *Online education, Data privacy, Data security, and Ethical consideration*

Introduction

The use of online education, often referred to as e-learning or distance learning, has witnessed a remarkable surge in recent years, transforming the educational landscape across the globe. In Nigeria, a country marked by its diverse population and unique educational challenges, online education has emerged as a promising solution to address issues related to access, quality, and flexibility in learning. This section delves into a comprehensive exploration of the background of online education in Nigeria, tracing its evolution, highlighting its importance, and elucidating the key challenges it faces, thus setting the stage for a profound analysis of the ethical considerations surrounding data privacy and security in this context.

The concept of online education has its historical roots in traditional correspondence courses and early forms of distance education, which allowed learners to access educational materials remotely, typically through printed materials and postal services (Okebukola & Jegede, 2019, Ayo, Odukoya, & Azeta, 2014). However, the advent of digital technologies,

particularly the internet, heralded a new era of online education in Nigeria. The proliferation of the internet in the late 20th century provided the foundation for the exponential growth of online education platforms. In Nigeria, the first significant wave of online education initiatives emerged in the early 2000s, with the objective of utilizing the internet's reach to expand access to education, particularly at the tertiary level (Onuoha, 2019, Abdullaev, Kendjaeva, & Xikmatullaev, 2019).

One remarkable milestone was the establishment of the National Open University of Nigeria (NOUN) in 2002. NOUN pioneered open and distance learning in the country, offering a broad spectrum of programs accessible to students from diverse geographical locations. By embracing online learning technologies, NOUN played a pivotal role in integrating technology into Nigeria's education system (National Open University of Nigeria, n.d., Pandey & Tiwari, 2014). Furthermore, several private and public universities in Nigeria have progressively integrated online components into their educational offerings. This integration enables students to access lectures, assignments, and learning resources through digital platforms, thus augmenting their learning experience (Okebukola & Jegede, 2019, Habila & Nachandiya, 2018).

Online education has assumed a pivotal role in Nigeria's educational landscape due to several compelling reasons:

Nigeria's vast geographic expanse poses substantial challenges when it comes to ensuring access to quality education. Online education transcends geographical boundaries, enabling students from remote and underserved areas to access educational content (Pandey & Tiwari, 2014;UNESCO, 2020 & Abdulmajeed, Joyner, & McManus, 2020).

The inherent flexibility of online education is particularly valuable in a country where many individuals need to juggle multiple responsibilities. Online learning allows students to balance their studies with work or family commitments (Ope-Davies, 2021; Habila & Nachandiya, 2018 & Onuoha, 2019). Online education can be a cost-effective solution for both students and educational institutions. It reduces the need for extensive physical infrastructure and can accommodate a larger number of students without the spatial constraints of traditional classrooms (Okebukola & Jegede, 2019; Abdulmajeed, Joyner, & McManus, 2020; Pandey & Tiwari, 2014).

In an era where technology permeates every facet of society, online education equips students with essential digital literacy skills. These skills are paramount for participation in the modern workforce and align with the goals of Nigeria's digital economy initiatives (UNESCO, 2020; Habila & Nachandiya, 2018 & Ope-Davies, 2021). Online education platforms offer students access to a vast array of digital resources, including multimedia content, research materials, and interactive learning tools. This wealth of resources enriches the educational experience and promotes self-directed learning (Onuoha, 2019, Abdulmajeed, Joyner, & McManus, 2020; Habila & Nachandiya, 2018). Despite the promising potential of online education, it faces several formidable challenges in the Nigerian context:

Nigeria grapples with a pronounced digital divide characterized by disparities in internet access and technology ownership between urban and rural areas (UNESCO, 2020). A study by the Nigerian Communications Commission (NCC) in 2020 revealed a significant disparity in internet access between urban and rural areas. The report indicated that internet penetration stood at 73.8% in urban centers compared to a mere 40.2% in rural regions (NCC, 2020. This digital divide can limit the reach of online education initiatives, leaving marginalized communities underserved.

Inadequate infrastructure, including unreliable electricity and inconsistent internet connectivity, poses a substantial hindrance to the effective delivery of online education (Okebukola & Jegede, 2019). A 2021 World Bank report titled "Nigeria Development Update" emphasizes the challenges posed by unreliable electricity supply in the country. The report states that only 47% of Nigerians have access to reliable electricity, which significantly impacts the

feasibility of online learning (World Bank, 2021). These infrastructure challenges affect both students and educational institutions, impacting the quality of the learning experience.

Ensuring the quality of online education programs is a pressing concern. Challenges related to accreditation, assessment, and the monitoring of course delivery can pose hurdles in maintaining and assuring educational standards (Onuoha, 2019). The lack of a robust quality assurance framework for online education programs in Nigeria is a concern raised by several experts. A 2015 article by Regha, discusses this issue, highlighting the need for clear accreditation guidelines and effective monitoring mechanisms for online courses (Regha, 2015) . Quality assurance mechanisms need to adapt to the unique features and challenges of online learning.

While smartphones have become increasingly ubiquitous, access to personal computers and stable internet connections remains a challenge for many Nigerians (UNESCO, 2020). A 2022 survey conducted by the National Bureau of Statistics (NBS) of Nigeria indicates that while smartphone ownership is on the rise, access to personal computers remains limited, particularly in low-income households. This disparity can disadvantage students in online learning environments (NBS, 2022). This limitation impacts students' ability to participate fully in online courses, particularly those that require specialized software or larger screens.

As online education platforms collect and store vast amounts of student data, concerns about data privacy and security have emerged as critical challenges (Abdulrazaq, Ndako., Emecheta., & Aliyu 2020). The increasing use of online education platforms in Nigeria has raised concerns about data privacy and security. A research paper by Okafor, Oparah & Okwudili, (2018) explores these concerns, emphasizing the need for robust data protection measures in online learning platforms (Okafor, Oparah & Okwudili 2018). This challenge forms the focal point of this systematic review.

In the digital age, the handling of personal data in online education platforms has assumed paramount importance. These platforms collect a wide range of data, encompassing student profiles, learning activities, assessment results, and communication logs (Okebukola & Jegede, 2019). This data is invaluable for personalizing learning experiences, monitoring progress, and improving educational outcomes. However, it also poses substantial ethical and practical challenges related to data privacy and security.

Data privacy pertains to the protection of individuals' personal information, ensuring that it is not misused or disclosed without proper consent. Data security, on the other hand, focuses on safeguarding data from unauthorized access, breaches, or loss (Abdulrazaq et al., 2020 & Yang, Xiong & Ren 2020). In the context of online education, the ethical handling of data is of paramount importance, as it involves the sensitive information of students, educators, and institutions.

The ethical considerations surrounding data privacy and security in online education platforms encompass issues related to informed consent, user rights, data retention, transparency, accountability, and equitable access (Bietz., Bloss., Calvert., Godino., Gregory., Claffey., & Patrick 2019 & Sheridan, 2022). These considerations are integral to upholding individuals' privacy rights, maintaining the integrity of educational data, and fostering trust among users of online education platforms.

Statement of Problem

The rapid proliferation of online education in Nigeria has introduced innovative learning opportunities, but it has also given rise to critical concerns regarding the data privacy and security of students and educators. As online education platforms collect and store extensive volumes of sensitive data, including personal information and learning activities, there is a pressing need to address the ethical dimensions of data privacy and security within this context.

Nigeria, with its diverse population and complex educational landscape, faces a multitude of challenges in balancing the benefits of online education with the safeguarding of individuals' personal information. These challenges include the digital divide, inadequate infrastructure, quality assurance, limited access to devices, and the evolving landscape of data protection laws and regulations. Moreover, ethical considerations within the realm of data privacy and security are multifaceted. Issues encompass informed consent, user rights, data retention, transparency, accountability, and equitable access. The potential consequences of mishandling data, including breaches, unauthorized access, or misuse, pose significant risks to both students and educators participating in online education platforms.

Research Objectives

This systematic review aims to achieve several key objectives:

1. To assess the current state of data privacy and security in online education platforms in Nigeria.
2. To identify ethical considerations related to data privacy and security in the Nigerian online education sector.
3. To identify challenges related to data privacy and security in the Nigerian online education sector.

Research Questions

The research questions to guide an investigation into data privacy and security in Nigerian online education platforms:

1. What are the existing data privacy and security measures implemented in online education platforms operating in Nigeria?
2. What ethical considerations are encountered concerning data privacy and security within the Nigerian online education sector?
3. What ethical challenges are encountered concerning data privacy and security within the Nigerian online education sector?

Methodology

Search Strategy: To conduct this systematic review, a comprehensive search strategy was employed to identify relevant literature. This strategy involved searching multiple academic databases, including PubMed, IEEE Xplore, and Google Scholar. The search was conducted using a combination of keywords and search terms relevant to the study, such as "online education," "data privacy," "security," and "Nigeria" (Munn, Peters, Stern, Tufanaru, McArthur & Aromataris 2018).

Inclusion and Exclusion Criteria: The inclusion and exclusion criteria were established to ensure that the identified studies were relevant to the research objectives. Studies considered for inclusion met the following criteria:

Publication Date: Studies published between 2018 and 2023 were considered to ensure the inclusion of recent research.

Study Types: Primary research articles, reviews, and gray literature were eligible for inclusion.
Geographic Focus: Studies focusing on online education platforms used in Nigeria were included in the review.

Data Extraction: Data extraction was carried out systematically to gather relevant information from the selected studies. This process involved recording data sources, study characteristics,

data privacy practices, security measures, ethical considerations, and challenges identified in each study (Higgins, Thomas, Chandler, Cumpston, Li, Page & Welch 2021).

Quality Assessment: The methodological quality of the included studies was assessed using standardized tools or checklists to ensure the reliability and validity of the findings (Higgins et al., 2021). The assessment considered factors such as study design, data collection methods, and potential sources of bias.

Data Synthesis: The data collected from the selected studies were subjected to thematic analysis to identify common themes and patterns related to data privacy and security in online education platforms in Nigeria (Thomas & Harden, 2008). This synthesis aimed to provide a comprehensive overview of the state of data ethics in online education in Nigeria.

Data Privacy and Security in Online Education Platforms in Nigeria

The proliferation of online education platforms in Nigeria, driven by advancements in technology and the necessity for remote learning during events such as the COVID-19 pandemic (UNESCO, 2020), has transformed the educational landscape. These platforms, including Learning Management Systems (LMS) and video conferencing tools, serve as vital tools for educators and students alike, providing access to a wide range of educational resources and facilitating remote instruction (Okebukola & Jegede, 2019).

Online education platforms collect and store significant amounts of personal data, including student information, academic records, and communication logs (Huang, 2023). These platforms typically outline their data privacy practices in their terms of service and privacy policies. However, the extent to which these practices are adhered to varies (Zeide, n.d). Data collection may encompass student demographics, learning progress, and even biometric data in some cases (Drachsler & Greller, 2016; Jones, Asher, Goben, Perry, Salo, Briney & Robertshaw 2020). However, ethical considerations regarding the collection and use of such data in the Nigerian context remain understudied (Amo, Fonseca, Alier, García-Peñalvo, Casañ, & Alsina 2019; Bala, 2022). Understanding the ethical implications of data privacy and security practices within online education platforms in Nigeria is crucial for safeguarding individuals' rights and ensuring accountability ((Williams, Ducoste & Rege 2020 n.d; Henningsen, Valde, Entzminger, Dick & Wilcher 2019; Abdulrazaq et al., 2020).

As online education platforms continue to expand, the collection, storage, and management of student data have become increasingly important considerations (Chen & Xu, 2020).Online education platforms often collect data on student behavior and performance (Yuan, Ruonan & Rongrong, 2017), including information such as time spent on tasks, quiz scores, and participation in discussion forums (Chen & Xu, 2020). This data is typically stored in secure servers, and access is restricted to authorized personnel only. The use of encrypted connections and secure protocols ensures the safety and confidentiality of the collected data (Office, 2020; Luan., Geczy., Lai., Gobert., Yang., Ogata & Tsai 2020).

In addition to collection and storage, the effective management of student data is crucial. Data management includes processes for organizing, analyzing, and utilizing the collected information to improve the educational experience for students (Luo, 2021; Shao, 2019). This may involve tracking student progress, identifying areas of improvement, and personalizing learning paths to cater to individual student needs(Chen & Xu, 2020; Zhao & Sun, 2014)

Ethical data practices require informed consent from users regarding data collection and usage. (Mislove & Wilson, 2018;Punchoojit & Hongwarittorrn, 2014). It's essential to prioritize user consent and permissions when it comes to ethical data practices. Obtaining informed consent from users is crucial for transparent data collection and usage (Mislove & Wilson, 2018). This not only ensures compliance with ethical guidelines but also fosters trust between

the users and the data collectors. When users are informed about how their data will be collected and used, it empowers them to make informed decisions about their privacy (Kreuter., Haas., Keusch., Bähr., & Trappmann 2020). This approach is fundamental in upholding ethical standards and promoting responsible data handling

Data security is a critical concern in the modern digital landscape, particularly when it comes to safeguarding sensitive student information (Derawi, 2014).. As technology continues to advance, the need for effective data encryption and security measures becomes increasingly imperative (Lai & Lv, 2012). One notable approach to addressing this concern is the implementation of end-to-end encryption, which ensures that data is securely transmitted and can only be accessed by authorized parties (Nabeel, 2017). Additionally, the use of multi-factor authentication can provide an extra layer of security by requiring multiple forms of verification before granting access to sensitive information (Lutkevich & Bacon, 2021). These measures are crucial in ensuring the protection of student data from unauthorized access and breaches (Ibrokhimov., Hui., Al-Absi., & Sain 2019; Ometov., Bezzateev., Mäkitalo., Andreev., Mikkonen., & Koucheryavy 2018).

As online education continues to evolve, the responsible collection, storage, management and encryption of student data will remain key factors in ensuring the success and security of online learning platforms.

Current Security Practices

Ensuring the security of online education platforms is paramount to protect the integrity and privacy of student data.

Protection Against Cyber Threats: Cybersecurity measures aim to protect these platforms from threats such as hacking, malware, and phishing attacks. However, the evolving nature of cyber threats poses an ongoing challenge to security (Abdulrazaq et al., 2020;Parthiban, Pandey & Pandey 2021).

Access Control and Authentication: Authentication mechanisms are employed to verify the identity of users accessing the platform. Robust access control measures are crucial for preventing unauthorized access (Onuoha, 2019; Marton & David, 2014).

Incident Response and Recovery: A robust incident response plan is essential for addressing data breaches and security incidents promptly. The effectiveness of response and recovery mechanisms varies across platforms (UNESCO, 2020; Maddox, 2021).

Ethical Concerns in Data Privacy and Security

In the context of online education platforms in Nigeria, obtaining informed consent from users regarding data collection and usage is a crucial ethical consideration (Abdulrazaq et al., 2020; Henze., Schwind., Wolf, Kocur & Schmidt 2020). Informed consent ensures that individuals are aware of how their data will be used and provides them with the opportunity to make informed decisions about sharing their information. However, achieving meaningful informed consent can be challenging in online education settings due to issues such as the length and complexity of privacy policies (Mulligan & Zuckerman, 2019; Grady., Cummings., Rowbotham., McConnell., Ashley., & Kang 2017).

Students have a right to control their personal data, including the ability to access, correct, and delete their information when necessary (Groom, 2019; (Sindhuri & Dongre, 2023). Ensuring that online education platforms in Nigeria respect these rights is an ethical imperative. Providing students with user-friendly tools to manage their data and privacy settings is essential to uphold these rights (Bietz., Bloss., Calvert., Godino., Gregory., Claffey & Patrick 2019; VanScoy., Jones., Bright., & Harding 2020)

Ethical data retention practices involve setting clear policies for how long student data will be stored and under what conditions it will be deleted. Transparent and ethical data retention policies contribute to the protection of student privacy (Mulligan & Zuckerman, 2019; Chiou., & Tucker 2017).

Respecting the "right to be forgotten," as outlined in data protection regulations, is vital in online education platforms (Groom, 2019). Students should have the ability to request the deletion of their data once it is no longer necessary for educational purposes or when they withdraw from a course or platform (Khalil & Ebner 2015). Online education platforms must be transparent about their data handling practices, including data collection, storage, sharing, and usage (Bietz et al., 2019; Laoutaris 2018). Transparency builds trust with users and helps them understand how their data is being used for educational purposes (Wiencierz & Luenich 2022).

Accountability is a cornerstone of ethical data handling. Online education platforms in Nigeria should have clear protocols for responding to data breaches and security incidents (Groom, 2019; Asgarinia., Chomczyk Penedo., Esteves., & Lewis 2023). Ethical accountability involves taking responsibility for breaches, notifying affected parties promptly, and implementing measures to prevent future incidents.

Equity and Access

Ensuring equitable access to online education platforms is an ethical imperative in a diverse country like Nigeria (UNESCO, 2020; Faturoti 2022). Ethical considerations include addressing disparities in internet access, device availability, and digital literacy. Online education should not exacerbate existing inequalities but instead work to bridge the digital divide. This can be achieved by identifying strategies to ensure equal access to online platforms and educational technology for all students, regardless of their socioeconomic background or geographical location (Cheng & Milikich, 2023). It is important for educational institutions to prioritize the development and implementation of policies and initiatives aimed at promoting diversity and inclusion. One way to achieve this is by actively engaging with community organizations and forming partnerships with public and private entities to address educational disparities. By collaborating with external stakeholders, educational institutions can leverage resources and expertise to create more equitable learning environments and opportunities for students.

Online education platforms should implement measures to ensure that students from underserved communities and marginalized groups have equal opportunities to access and benefit from online learning (Bietz et al., 2019). Ethical practices should focus on promoting inclusivity and reducing educational disparities. Promoting inclusivity and reducing educational disparities are crucial ethical practices in education (Idziorek et al., 2012). These practices should focus on creating a learning environment where diversity is celebrated and all students, regardless of their background or abilities, have equal access to educational opportunities.This includes addressing issues of discrimination, bias, and systemic barriers that may hinder certain students from achieving their full potential (Holmes et al., 2021). Looking beyond the classroom and into community organizations and other public or private partnerships can also reduce inequalities in educational achievement outcomes.

Challenges and Gaps

One significant challenge in the context of data privacy and security in online education platforms in Nigeria is the presence of legal and regulatory gaps (Okebukola & Jegede, 2019). Existing data protection laws may not adequately address the unique challenges posed by online education. Additionally, regulatory enforcement and compliance mechanisms may be lacking, creating vulnerabilities in data handling practices. Addressing legal and regulatory gaps related to data privacy and security is crucial to ensure the ethical and responsible use of technology in education (Understanding Data Privacy. The Objective and Scope of Nigeria Data…, 2021) (As

Number of Edtech Providers Grow, Some Say Student Privacy Needs a Reset, 2023). Collaborating with government agencies, industry experts, and legal professionals can help in developing and implementing robust policies and guidelines to safeguard the privacy and security of students and educators using online platforms (5 Policy Recommendations for Effective Implementation of AI in Education | by Deblina Pakhira | Medium, 2021; Technology can close achievement gaps, improve learning, 2014).

The rapid evolution of technology introduces challenges related to data security. Online education platforms must continually adapt to emerging threats such as cyberattacks and data breaches (Abdulrazaq et al., 2020). Technological limitations can hinder the implementation of robust security measures in online education. However, it is imperative that every effort is made to mitigate these limitations and ensure the privacy and security of student data (Heath, 2020). This may involve implementing secure data encryption protocols, conducting regular security audits, and providing comprehensive training for educators and administrators on data privacy best practices (Li & Peng, 2021). Additionally, it is crucial to engage in ongoing dialogue and collaboration with students, parents, and communities to ensure that their voices are heard and their unique needs are considered in the development and implementation of ethical practices in online education (Heath, 2020).

Another challenge is the lack of awareness and education among educators, students, and parents regarding data privacy and security issues in online education (Onuoha, 2019). This knowledge gap can lead to inadvertent breaches and compromises in ethical data practices. Efforts should be made to proactively educate and raise awareness about the importance of data privacy and security, as well as the potential risks and vulnerabilities associated with online learning (Heath, 2020). Promoting digital literacy and providing training programs for educators, students, and parents can empower them with the knowledge and skills necessary to navigate online educational platforms safely and responsibly (Li & Peng, 2021).

Addressing Research Gaps

Research in the field of data privacy and security in online education platforms in Nigeria remains relatively limited. Future investigations should explore the effectiveness of specific data protection measures and cybersecurity practices (UNESCO, 2020). By conducting thorough research and analysis, these investigations can provide valuable insights into the current state of data protection and cybersecurity practices in Nigeria's educational system. This can involve studying the implementation of encryption protocols, security audits, and the effectiveness of training programs for educators and administrators in safeguarding student data privacy.

Furthermore, future investigations should also assess the level of awareness and education among educators, students, and parents regarding data privacy and cybersecurity issues. Understanding the existing knowledge and practices related to data protection will be crucial in identifying areas for improvement and potential vulnerabilities in online educational platforms.

Future research should also focus on the development and evaluation of innovative technologies and practices to enhance data privacy and security in online education. In addition to exploring the current state of data protection and cybersecurity practices in Nigeria's educational system, future research should also focus on the development and evaluation of innovative technologies and practices to enhance data privacy and security in online education. This involves investigating emerging encryption protocols, authentication methods, and cybersecurity tools specifically tailored for online educational platforms. By assessing the effectiveness of these technologies in safeguarding student data and preventing unauthorized access, researchers can contribute to the advancement of secure online learning environments.

Moreover, the evaluation of privacy-enhancing technologies such as differential privacy and secure multi-party computation in the context of online education can provide valuable

insights into their applicability and effectiveness in safeguarding sensitive student information (Abdulrazaq et al., 2020). Additionally, research efforts should address the impact of regulatory reforms and policy changes on data ethics in the online education sector in Nigeria.

Recommendations

To address the legal and regulatory gaps, Nigerian authorities should consider enhancing and modernizing data protection laws (Okebukola & Jegede, 2019). These laws should explicitly address data privacy and security in the context of online education platforms. Comprehensive legislation can provide a robust framework for ethical data practices.

To address the legal and regulatory gaps, Nigerian authorities should consider enhancing and modernizing data protection laws and regulations to ensure that they are aligned with the evolving landscape of online education and encompass robust provisions for data privacy and security (Nigeria's New Data Protection Act, Explained, 2023; What you should know about education technology (edtech) models in Nigeria, 2020; NITDA is on a mission to safeguard the data privacy rights of Nigerians, 2019). Collaboration between governmental bodies, educational institutions, and industry experts can facilitate the development of comprehensive guidelines that protect the rights of students and educators while promoting responsible and ethical use of technology in education (Report: Specific Steps Needed for Student Data Privacy, 2023; As Number of Edtech Providers Grow, Some Say Student Privacy Needs a Reset, 2023). Additionally, establishing a certification or accreditation process for online educational platforms can help ensure that they adhere to stringent data privacy and security standards (Personal Data Security Technical Guide for Online Education Platforms, 2020; Zhang, 2020). This can involve creating a framework for assessing the privacy practices, security measures, and data handling procedures of online education providers, thereby enhancing transparency and accountability in the sector.(Liagkou, Stylios & Петунин 2019; Report: Specific Steps Needed for Student Data Privacy, 2023)

The Nigerian government should collaborate with educational institutions and industry stakeholders to develop and implement regulatory frameworks specific to online education (Sangoniran, 2023). This collaboration will ensure that online education in Nigeria meets high quality standards, promotes inclusivity and access for all students, and protects the rights and interests of learners and educators involved in online education (Bhushan & Verma, 2017).This collaboration will also address the challenges and opportunities presented by online education, such as ensuring data privacy and security, fostering innovation in online teaching methodologies, and establishing mechanisms for quality assurance and accreditation of online programs (Sangoniran, 2023). It is a theoretical description and procedural flow of face to face and web-based (Turmudi, 2020). This collaboration will also address the challenges and opportunities presented by online education, such as ensuring data privacy and security, fostering innovation in online teaching methodologies, and establishing mechanisms for quality assurance and accreditation of online programs (Felder, Brent & Prince 2011). These frameworks should outline minimum data security standards, compliance requirements, and mechanisms for oversight.

Online education platforms in Nigeria should invest in advanced encryption technologies and cybersecurity measures to protect student data from unauthorized access and potential cyber attacks (Idziorek, Rursch & Jacobson 2012). This includes end-to-end encryption for communications, robust access controls, and regular security audits and updates. Additionally, there should be transparent and comprehensive policies in place to address issues such as plagiarism, academic integrity, and intellectual property rights within the realm of online education. Given the evolving landscape of cyber security threats, it is important to provide our workforce with ongoing training in cyber security (LeClair, Abraham & Shih 2013).The protection of cyber assets requires a multipronged approach that requires the coordination of government, academia, and industry (Idziorek et al., 2012).This collaboration will ensure that

online education in Nigeria meets high quality standards, promotes inclusivity and access for all students, and protects the rights and interests of learners and educators involved in online education (Lim, 2018).

To empower users with control over their data, online education platforms should design user-friendly privacy settings (Bietz et al., 2019). These settings should allow students to easily manage data sharing preferences, access their data, and request data deletion when needed. Educational institutions should incorporate digital literacy and ethics education into their curricula to ensure that students, educators, and parents are well-informed about data privacy and security (8 Tech Skills Every Student Should Have, According to Educators, 2024 ; Importance of Digital Literacy, 2022). These programs should cover best practices, risks, and the importance of ethical data handling(Oducado & Estoque, 2021; Abdulmajeed, Joyner & McManus, 2020; Rasheed, n.d)Online education platforms should engage in awareness campaigns to educate their users about data privacy and security practices (Hassan, Wahi, Ismail & Awwad 2022; Siemens, Althaus & Stange 2013). These campaigns should emphasize the ethical responsibilities of all stakeholders in protecting sensitive data and maintaining a secure online learning environment.

By implementing these recommendations, Nigeria can enhance the ethical treatment of data in online education, safeguarding the privacy and security of individuals' information while promoting the continued growth and accessibility of online learning platforms.

Conclusion

In conclusion, the ethical considerations surrounding data privacy and security in online education platforms used in Nigeria are of paramount importance as these platforms become increasingly integral to the education landscape. This systematic review has shed light on the current state of data ethics in online education and identified several key findings and recommendations. The review revealed that while online education platforms offer numerous benefits, they also present ethical challenges. Data privacy practices vary, and issues such as informed consent, user rights, data retention, and transparency remain areas of concern. Security measures, though essential, need improvement to protect against evolving cyber threats.

To address these challenges and promote ethical data practices, we recommend a multifaceted approach:

- Strengthening data protection laws and establishing regulatory frameworks specific to online education will provide a legal foundation for ethical data handling.
- Investing in advanced encryption and cybersecurity measures, along with user-friendly privacy settings, will enhance data security and user control.
- Incorporating digital literacy and ethics education into curricula and conducting awareness campaigns will ensure that all stakeholders are well-informed about data privacy and security.
- It is crucial that Nigeria takes proactive steps to safeguard data privacy and security while fostering the growth and accessibility of online education platforms. By doing so, the country can provide a secure and ethical digital learning environment for its students and educators, contributing to the advancement of education in the digital age.
- In the rapidly evolving landscape of online education, continual research, regulation, and education will be essential to adapt to new challenges and ensure that ethical considerations remain at the forefront of digital learning.

References

Abdullaev, Z., Kendjaeva, D., & Xikmatullaev, S. (2019, November). Innovative approach of distance learning in the form of online courses. In *2019 International Conference on Information Science and Communications Technologies (ICISCT)* (pp. 1-3). IEEE.

Abdulmajeed, K., Joyner, D. A., & McManus, C. (2020, August). Challenges of online learning in Nigeria. In *Proceedings of the Seventh ACM Conference on Learning@ Scale* (pp. 417-420).

Abdulrazaq, A., Ndako, A. G., Emecheta, S. B., & Aliyu, H. (2020). Information security and privacy issues in e-learning: A review. International Journal of Engineering Research and Technology, 13(6), 1500-1506.

Amo, D., Fonseca, D., Alier, M., García-Peñalvo, F. J., Casañ, M. J., & Alsina, M. (2019). Personal data broker: A solution to assure data privacy in EdTech. In *Learning and Collaboration Technologies. Designing Learning Experiences: 6th International Conference, LCT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings, Part I 21* (pp. 3-14). Springer International Publishing.

As Number of Edtech Providers Grow, Some Say Student Privacy Needs a Reset. (2023). https://www.edsurge.com/news/2023-05-18-as-number-of-edtech-providers-grow-some-say-student-privacy-needs-a-reset

Asgarinia, H., Chomczyk Penedo, A., Esteves, B., & Lewis, D. (2023). "Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information*, *14*(7), 351.

Ayo, C. K., Odukoya, J. A., & Azeta, A. (2014). A Review of Open & Distance Education and Human Development in Nigeria. *International Journal of Emerging Technologies in Learning*, *9*(6).

Bala, R. (2022). Challenges and Ethical Issues in Data Privacy: Academic Perspective. *International Journal of Information Retrieval Research (IJIRR)*, *12*(2), 1-7.

Bhushan, S., & Verma, A. (2017). Quality Assurance in Higher Education—An Indian Experience. Elsevier BV, 51-66. https://doi.org/10.1016/b978-0-08-100553-8.00011-2

Bietz, M. J., Bloss, C. S., Calvert, S., Godino, J. G., Gregory, J., Claffey, M. P., & Patrick, K. (2019). Ethical considerations for research in the Internet of Things (IoT). Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1-14.

Chen, C., & Xu, W. (2020). Innovation and application of college students' education and management based on big data. In *Proceedings of the 2020 3rd International Conference on Big Data and Education* (pp. 5-9).

Cheng, Y., & Milikich, N. (2023, January 1). An Analysis of How COVID-19 Shaped the Realm of Online Gaming and Lesson Delivery. Cornell University. https://doi.org/10.48550/arxiv.2304.06102

Chiou, L., & Tucker, C. (2017). *Search engines and data retention: Implications for privacy and antitrust* (No. w23815). National Bureau of Economic Research.

Derawi, M. (2014). Securing e-learning platforms. In *2014 International Conference on Web and Open Access to Learning (ICWOAL)* (pp. 1-4). IEEE.

Drachsler, H., & Greller, W. (2016, April). Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In *Proceedings of the sixth international conference on learning analytics & knowledge* (pp. 89-98).

Eight Tech Skills Every Student Should Have, According to Educators. (2024, January 31). https://www.edweek.org/technology/8-tech-skills-every-student-should-have-according-to-educators/2024/01

Faturoti, B. (2022). Online learning during COVID19 and beyond: A human right based approach to internet access in Africa. *International Review of Law, Computers & Technology*, *36*(1), 68-90.

Felder, R M., Brent, R., & Prince, M J. (2011). Engineering Instructional Development: Programs, Best Practices, and Recommendations. Wiley-Blackwell, 100(1), 89-122. https://doi.org/10.1002/j.2168-9830.2011.tb00005.x

Five Policy Recommendations for Effective Implementation of AI in Education | by Deblina Pakhira | Medium. (2021). https://medium.com/@deblinapakhira/5-policy-recommendations-for-effective-implementation-of-ai-in-education-15c8dfc8ba6

Grady, C., Cummings, S R., Rowbotham, M C., McConnell, M V., Ashley, E A., & Kang, G. (2017). Informed Consent. https://www.nejm.org/doi/10.1056/NEJMra1603773

Groom, J. M. (2019). The need for better student data privacy and security in higher education. EDUCAUSE Review, 54(3), 39-52.

Habila, I., & Nachandiya, N. (2018). Development of an online learning management system (OLMS) a case study of Adamawa State University Mubi Nigeria. *International Journal of Computer Applications*, *975*, 8887.

Hassan, R., Wahi, W., Ismail, N H A., & Awwad, S A B. (2022). Data Security Awareness in Online Learning. https://doi.org/10.14569/ijacsa.2022.0130432 Nigeria's New Data Protection Act, Explained. https://fpf.org/blog/nigerias-new-data-protection-act-explained/

Heath, M K. (2020). Buried treasure or Ill-gotten spoils: the ethics of data mining and learning analytics in online instruction. Springer Science+Business Media, 69(1), 331-334. https://doi.org/10.1007/s11423-020-09841-x

Henningsen, M. L. M., Valde, K. S., Entzminger, M. J., Dick, D. T., & Wilcher, L. B. (2019). Student disclosures about academic information: Student privacy rules and boundaries. *Communication Reports*, *32*(1), 29-42.

Henze, N., Schwind, V., Wolf, K., Kocur, M., & Schmidt, A. (2020). Preparing an Online Lecture That We Wouldn't Hate to Attend. Institute of Electrical and Electronics Engineers, 19(3), 51-55. https://doi.org/10.1109/mprv.2020.2997614

Higgins, J. P., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M. J., & Welch, V. A. (2021). Cochrane Handbook for Systematic Reviews of Interventions (2nd ed.). John Wiley & Sons.

Hillman, V. (2022). Data privacy literacy as a subversive instrument to datafication. *International Journal of Communication*, *16*, 22.

Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T T., Shum, S B., Santos, O C., Rodrigo, M M T., Cukurova, M., Bittencourt, I I., & Koedinger, K R. (2021). Ethics of AI in Education: Towards a Community-Wide Framework.

Springer Science+Business Media, 32(3), 504-526. https://doi.org/10.1007/s40593-021-00239-1

Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers*, *16*(2), 2577-2587.

Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. (2019). Multi-factor authentication in cyber physical system: A state of art survey. In *2019 21st international conference on advanced communication technology (ICACT)* (pp. 279-284). IEEE.

Idziorek, J., Rursch, J A., & Jacobson, D. (2012). Security across the curriculum and beyond. https://doi.org/10.1109/fie.2012.6462297

Importance of Digital Literacy. (2022). https://www.ecoleglobale.com/blog/teaching-digital-literacy/

Jiugen, Y., Ruonan, X., & Rongrong, K. (2017). Research on interactive application of online education based on cloud computing and large data. In *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)* (pp. 593-596). IEEE.

Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology*, *71*(9), 1044-1059.

Khalil, M., & Ebner, M. (2015). Learning analytics: principles and constraints. In *Edmedia+ innovate learning* (pp. 1789-1799). Association for the Advancement of Computing in Education (AACE).

Kreuter, F., Haas, G. C., Keusch, F., Bähr, S., & Trappmann, M. (2020). Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review*, *38*(5), 533-549.

Lai, K., & Lv, X. (2012). Data Safety Policy Considerations in Educational Information Management Systems. In *2012 Sixth International Conference on Internet Computing for Science and Engineering* (pp. 235-238). IEEE.

Laoutaris, N. (2018). Data transparency: Concerns and prospects [point of view]. *Proceedings of the IEEE*, *106*(11), 1867-1871.

LeClair, J., Abraham, S., & Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. https://doi.org/10.1145/2528908.2528923

Li, W., & Peng, Y. (2021). An Intelligent Recommendation Strategy for Online Courses Based on Collaborative Filtering Algorithm for Educational Platforms. , 4(16). https://doi.org/10.25236/fer.2021.041605

Liagkou, V., Stylios, C., & Петунин, А А. (2019). Handling Privacy and Concurrency in an Online Educational Evaluation System. https://doi.org/10.22364/bjmc.2019.7.1.07

Lim, C P. (2018). Digital learning for development of Asian schools. Informa, 367-368. https://doi.org/10.4324/9781315694382-34

Luan, H., Geczy, P., Lai, H., Gobert, J., Yang, S. J., Ogata, H., ... & Tsai, C. C. (2020). Challenges and future directions of big data and artificial intelligence in education. *Frontiers in psychology*, *11*, 580820.

Luo, Y. (2021). Research on the methods of management of university students in the big data age. *Open Access Library Journal*, *8*(5), 1-6.

Maddox, I. (2021). Account authentication and password management best practices. https://cloud.google.com/blog/products/identity-security/account-authentication-and-password-management-best-practices

Marton, G., & David, A O. (2014). Security considerations and two-factor authentication opportunities in e-learning environments. https://doi.org/10.1109/iceta.2014.7107604

Mislove, A., & Wilson, C. (2018). A practitioner's guide to ethical web data collection.

Mulligan, D. K., & Zuckerman, E. (2019). A functional approach to data ethics. International Data Privacy Law, 9(4), 247-257.

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Medical Research Methodology, 18(1), 143.

Nabeel, M. (2017). The many faces of end-to-end encryption and their security analysis. In *2017 IEEE international conference on edge computing (EDGE)* (pp. 252-259). IEEE.

National Bureau of Statistics (NBS). (2022). *Report on Information and Communication Technology (ICT) in Nigeria*.

Nigerian Communications Commission (NCC). (2020). *Nigerian National Broadband Plan 2020-2025*. Retrieved from ncc.gov.ng/documents/880-nigerian-national-broadband-plan-2020-2025/file

NITDA is on a mission to safeguard the data privacy rights of Nigerians. (2019). https://techpoint.africa/2019/03/21/nitda-ndpr-data-privacy/

Nowicki, J. M. (2020). Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm. Report to the Republican Leader, Committee on Education and Labor, House of Representatives. GAO-20-644. *US Government Accountability Office*.

Oducado, R M F., & Estoque, H V. (2021). Online Learning in Nursing Education During the COVID-19 Pandemic: Stress, Satisfaction, and Academic Performance. https://doi.org/10.30994/jnp.v4i2.12

Ogunmola, O. F., & Oluwatobi, S. A. (2018). The role of digital economy in the development of Nigeria. *Journal of Applied Sciences and Environmental Management*, 22(6), 915-920.

Okafor, N. U., Oparah, C. C., & Okwudili, U. M. (2018). Security and Privacy in E-learning Education. *TETFUND SPONSORED*, 40.

Okebukola, P. A., & Jegede, O. J. (2019). E-learning in Nigeria: An overview of challenges and prospects. *International Journal of Information and Education Technology*, 9(4), 313-317.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.

Onuoha, U. D. (2019). Online education in Nigeria: A comparative analysis of attitudes and performance in university-level mathematics courses. Education Sciences, 9(1), 2.

Ope-Davies, T. (2021). Online remote language teaching during and beyond the pandemic: echoes from. *The world universities' response to COVID-19: remote online language teaching*, 63.

Pandey, S., & Tiwari, S (2014). Education and prosperity through technology–Case of virtual education limited, Nigeria. *Procedia-Social and Behavioral Sciences*, *157*, 55-62.

Parthiban, K., Pandey, D., & Pandey, B K. (2021). Impact of SARS-CoV-2 in Online Education, Predicting and Contrasting Mental Stress of Young Students: A Machine Learning Approach. Springer Science+Business Media, 6(1). https://doi.org/10.1007/s41133-021-00048-0

Personal Data Security Technical Guide for Online Education Platforms. (2020, May 18). https://iite.unesco.org/publications/personal-data-security-technical-guide-for-online-education-platforms/

Punchoojit, L., & Hongwarittorrn, N. (2014). The Ethics of computer research: A survey of user acceptance towards mobile HCI research practices and factor influencing the willingness to participate and to share information in research. In *2014 International Computer Science and Engineering Conference (ICSEC)* (pp. 383-388). IEEE.

Regha, I. O. (2015). Adoption of blended learning into the Nigerian education system: Prospects and challenges. *International Journal of Social Sciences*, *11*(3), 129-142.

Report: Specific Steps Needed for Student Data Privacy. (2023). https://www.govtech.com/education/higher-ed/report-specific-steps-needed-for-student-data-privacy

Sangoniran, A. (2023). What Factors Influence Students to Persist and Achieve on Science, Technology, Engineering and Mathematics (STEM) Courses in Nigerian Universities?. , 14(1), 4750-4759. https://doi.org/10.20533/ijcdse.2042.6364.2023.0585

Shao, C. (2019). Research and Analysis on Management Information Construction of College Students Based on Big Data Environment. In *2nd International Conference on Contemporary Education, Social Sciences and Ecological Studies (CESSES 2019)* (pp. 843-846). Atlantis Press.

Sheridan, P. M. (2022). Edtech in higher education: Protecting student data privacy in the classroom. NCJL & Tech., 24, 49.

Siemens, L., Althaus, C., & Stange, C. (2013). Balancing Students' Privacy Concerns While Increasing Student Engagement in E-learning Environments. https://doi.org/10.1108/s2044-9968(2013)000006g014

Sindhuri, R., & Dongre, A R. (2023). Challenges in Obtaining Informed Consent in Qualitative Research and Suggestions to Improve It- A Descriptive Qualitative Study. National *journal of community medicine*, 14(06), 386-390. https://doi.org/10.55489/njcm.140620232874

Technology can close achievement gaps, improve learning. (2014). https://ed.stanford.edu/news/technology-can-close-achievement-gaps-and-improve-learning-outcomes

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. BMC Medical Research Methodology, 8(1), 45.

Turmudi, D. (2020). Utilizing a web-based technology in blended EFL academic writing classes for university students. IOP Publishing, 1517(1), 012063-012063. https://doi.org/10.1088/1742-6596/1517/1/012063

Understanding Data Privacy. The Objective and Scope of Nigeria Data…. (2021). https://medium.com/@solomon.igori/understanding-data-privacy-3d1ca96cda23

UNESCO. (2020). COVID-19 educational disruption and response. Retrieved from https://en.unesco.org/covid19/educationresponse

VanScoy, A., Jones, K. M., Bright, K., & Harding, A. (2020). Instructors' understanding of and responses to student privacy in the datafied classroom. *Proceedings of the Association for Information Science and Technology*, *57*(1), e400.

What you should know about education technology (edtech) models in Nigeria. (2020). https://techpoint.africa/2020/03/09/edtech-models-nigeria/

Wiencierz, C., & Luenich, M. (2022). Trust in open data applications through transparency. *New media & society*, *24*(8), 1751-1770.

Williams, K., Ducoste, M. R., & Rege, A. (2020). Educating multidisciplinary undergraduates on security and privacy. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE.

World Bank. (2021). *Nigeria Development Update*. Retrieved from https://thedocs.worldbank.org/en/doc/88d5ed4248d7063eced528070a83173e-0360012023/original/NDU-december-2023-presentation.pdf

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *Ieee Access*, *8*, 131723-131740.

Zhang, H. (2020). Methods of Teachers' Personal Privacy Security Protection Based on Big Data Analysis. https://doi.org/10.1088/1757-899x/750/1/012231

Zhao, H. Y., & Sun, Q. (2014). Research on the Design and Implementation of Student Information Management System. *Applied Mechanics and Materials*, *687*, 2833-2836.