INMRJ
International Nexus Multidisciplinary Research Journal
April-May, 2025: https://journals.classicmultilinks.com
Impact Factor: 5.0. Vol: 1 Issue:2

SAFEGUARDING STUDENT DATA: CYBERSECURITY POLICIES AND PRACTICES BY PRINCIPALS IN SECONDARY SCHOOLS IN ANAMBRA STATE

Dr. Nnenna Winifred Chukwu and Dr. Ezemba Edith Uzoamaka
Department of Educational Management and Policy; Faculty of Education
Nnamdi Azikiwe University Awka, Anambra State

ABSTRACT

The increasing digitalization of educational systems necessitates effective safeguarding of student data to protect privacy and ensure data integrity. This study investigates the cybersecurity policies and practices adopted by principals in secondary schools in Anambra State, Nigeria. The primary aim is to assess the extent of cybersecurity awareness, the implementation of data protection policies, and the challenges faced by school leaders in safeguarding student information. Employing a descriptive survey design, data were collected from a sample of principals across both urban and rural secondary schools through structured questionnaires and interviews. The findings reveal that while most principals recognize the importance of data security, their awareness of comprehensive cybersecurity policies remains limited, and the implementation of structured data protection practices is inconsistent. Key challenges identified include inadequate infrastructural resources, insufficient training, and low awareness of national and international data protection standards. The study emphasizes the urgent need for school leadership to prioritize cybersecurity education, establish clear policies, and invest in secure information systems. Strengthening principals' capacity and fostering a culture of cybersecurity within schools are critical for protecting student data in an increasingly digital educational landscape. The insights provided aim to inform policymakers, educational authorities, and school administrators in developing robust cybersecurity frameworks that safeguard students' personal information while promoting safe digital learning environments in Anambra State and beyond.

Keywords: Cybersecurity, Student Data Protection, Principal Practices and Secondary Schools,

Introduction

In the digital age, the reliance on technology and digital platforms in educational institutions has significantly increased, transforming traditional teaching and administrative practices. Nigerian secondary schools, like their counterparts worldwide, are increasingly utilizing electronic systems to manage student information, attendance, examination results, and other critical data. While these advances enhance operational efficiency and data accessibility, they also expose students' sensitive information to cybersecurity threats such as hacking, data breaches, and unauthorized access (Okafor & Nwachukwu, 2020). Safeguarding student data has thus become a crucial concern, necessitating the development and implementation of robust cybersecurity policies and practices. However, many

Nigerian secondary schools face challenges including inadequate security awareness, limited resources, and a lack of comprehensive policies, which hinder effective protection of student information (Adebayo, 2021). This paper explores the current state of cybersecurity strategies in Nigerian secondary schools, emphasizing the importance of establishing effective safeguarding measures to ensure data confidentiality, integrity, and privacy. By analyzing existing policies and recommending best practices, the study aims to support policymakers and school administrators in strengthening cybersecurity frameworks to protect students from emerging digital threats effectively.

The proliferation of digital technologies in educational institutions across Nigeria has brought about significant improvements in teaching, learning, and administrative processes. Particularly in secondary schools, the integration of information and communication technology (ICT) systems enables efficient management of student data, including academic records, attendance, examination results, and personal information (Eke & Nwachukwu, 2019). However, this increased dependence on digital platforms also exposes student data to a myriad of cybersecurity threats, such as data breaches, hacking, malware attacks, and unauthorized access, which compromise students' privacy and the integrity of educational records (Ojo & Akinwale, 2020).

In Nigeria, the importance of safeguarding student data is underscored by the increasing digitalization of school administration and the growing sophistication of cybercriminals. Despite this, many secondary schools still lack comprehensive cybersecurity policies and effective practices to protect sensitive information (Uche & Nwali, 2021). Several factors contribute to this gap, including limited awareness about cyber threats among school staff, inadequate infrastructural resources, and the absence of nationwide standardized cybersecurity frameworks. Consequently, student data in many Nigerian secondary schools remains vulnerable, exposing students to risks such as identity theft, extortion, and privacy violations.

Anambra State, located in Southeastern Nigeria, has witnessed a steady progression toward digital school management. The state government has made concerted efforts to adopt e-learning platforms and digital record-keeping systems in public secondary schools (Anambra State Ministry of Education, 2020). While these initiatives aim to improve educational delivery, they also heighten concerns about data security. It is crucial for these schools to establish robust cybersecurity policies that delineate responsibilities, establish standards for data protection, and promote best practices among stakeholders (Okorie & Chukwuma, 2021).

Research indicates that effective cybersecurity in schools relies on multiple factors, including policy formulation, staff training, regular software updates, and the deployment of security tools such as firewalls, encryption, and access controls (Ikechukwu & Udeh, 2018). Moreover, policies should address issues like data ownership, breach response protocols, and user authentication to create a comprehensive framework that guides safe data handling. In Nigeria, the National Data Protection Regulation (NDPR), which aligns with global data protection standards such as GDPR, provides a legal backdrop for safeguarding personal data (National Information Technology Development Agency [NITDA], 2019).

However, awareness and implementation at the school level remain inconsistent, particularly in secondary schools within Anambra State.

Furthermore, cultivating a cybersecurity culture among students and staff is vital. Training programs and awareness campaigns equip individuals with knowledge about potential threats and safe online practices. Schools that foster a data protection-aware environment tend to have fewer incidents and stronger resilience against cyberattacks (Obinna & Nwabueze, 2020). Nonetheless, resource constraints and the rapid evolution of cyber threats pose ongoing challenges. Improving cybersecurity practices in Anambra State secondary schools requires a multifaceted approach involving policy development, capacity building, infrastructural investment, and stakeholder engagement.

Therefore, safeguarding student data in Nigerian secondary schools in Anambra State is a pressing issue that demands urgent attention. While progress has been made with the adoption of digital tools, gaps in policies and practices threaten data security. They can have far-reaching consequences on students' privacy rights and the credibility of the educational system. To address these challenges, comprehensive cybersecurity policies aligned with national and international standards must be developed and effectively implemented. Equally important is fostering a culture of cybersecurity awareness among all stakeholders to build a resilient educational environment that protects student data from the evolving landscape of cyber threats.

Statement of the Problem

In the digital era, Nigerian secondary schools are increasingly adopting information and communication technologies (ICT) to streamline administrative processes and improve educational delivery. Despite these advancements, many schools in Anambra State lack adequate cybersecurity measures to protect sensitive student data such as personal information, academic records, and examination results. This exposes students and institutions to significant security risks, including data breaches, identity theft, and privacy violations. Although Nigeria has established legal frameworks like the National Data Protection Regulation (NDPR), the level of awareness, understanding, and implementation of cybersecurity policies among secondary schools remains inconsistent and often inadequate. Consequently, students' critical data remain vulnerable to cyber threats, which can undermine trust in digital educational systems, compromise student rights, and threaten the integrity of academic records. This problem underscores the urgent need to evaluate the current cybersecurity practices in these schools, identify gaps, and develop effective policies to safeguard student data against evolving cyber risks.

Research Purposes

1. To examine the existing cybersecurity policies and practices implemented in secondary schools in Anambra State, Nigeria, for safeguarding student data.

2. To identify challenges faced by secondary schools in Anambra State in developing and implementing effective cybersecurity policies for protecting student information.

Significance of the study

This study will benefit several groups, including educational policymakers, school administrators, and teachers in Nigerian secondary schools, particularly in Anambra State. Policymakers can use the findings to develop and enforce comprehensive cybersecurity policies that effectively safeguard student data. School administrators and ICT personnel will gain insights into best practices and the importance of implementing robust security measures, enabling them to protect sensitive information better. Additionally, students and parents will benefit from increased data privacy and security, fostering a safer digital learning environment. Researchers and scholars in the field of educational technology and cybersecurity will also find the study valuable as a reference for future research on data protection in the educational sector. Ultimately, the study aims to contribute to improving the overall digital security framework within Nigerian secondary schools, ensuring the confidentiality, integrity, and privacy of student data are adequately protected.

Policy formulation: The findings will provide evidence-based insights that policymakers can use to develop or update cybersecurity regulations tailored to secondary schools in Anambra State.
Capacity building: The study will identify areas where teachers and administrators need training, guiding the development of targeted workshops and awareness programs.
Enhanced data security: Schools will be equipped with practical strategies and best practices to establish and improve their cybersecurity measures, thus reducing vulnerabilities.
Protection of students' rights: By advocating for stronger cybersecurity policies, the study helps ensure students' personal information remains confidential and protected from cyber threats.
Academic contribution: Researchers and educational institutions can use the findings as a foundation for further studies, fostering a culture of cybersecurity awareness in education.

Scope of the Study

This study focuses on the cybersecurity policies and practices related to safeguarding student data in secondary schools in **Anambra State, Nigeria**. The research is limited to **public secondary schools** within the state, encompassing both urban and rural areas. It aims to assess the current cybersecurity measures, policies, and practices being employed by school administrations. The study also examines the challenges faced in implementing effective data protection strategies and explores the level of awareness among school staff and students about cybersecurity threats. The research does not extend to private secondary schools or other levels of education such as primary or tertiary institutions. Data collection will be limited to school administrators, ICT personnel, teachers, and students from selected schools to ensure in-depth and relevant insights. The geographic focus on Anambra State helps provide contextualized findings that can inform local policy and practice improvements.

Research questions

1. To what extent are existing cybersecurity policies and practices implemented in secondary schools in Anambra State, Nigeria, for safeguarding student data.

2. What are the challenges faced by secondary schools Principals in Anambra State in developing and implementing effective cybersecurity policies for protecting student information.

Literature Review

The increasing adoption of digital technologies in educational institutions has heightened concerns regarding the security of student data (Eke & Nwachukwu, 2019). Various studies have emphasized the importance of establishing robust cybersecurity policies to protect sensitive information within schools. According to Ikechukwu and Udeh (2018), many secondary schools in Nigeria lack comprehensive cybersecurity frameworks, leaving student data vulnerable to cyber threats such as hacking, data breaches, and malware attacks. These vulnerabilities can lead to the loss of vital academic records and invasion of students' privacy rights.

Research by Obinna and Nwabueze (2020) highlights that awareness and training programs are crucial for fostering a cybersecurity culture among school staff and students. They argue that well-informed users are better equipped to identify and respond to digital threats, reducing the risk of successful cyberattacks. Conversely, Uche and Nwali (2021) found that most schools lack regular cybersecurity training sessions, which exacerbates susceptibility to cyber threats.

Furthermore, Nigeria's legal framework, including the National Data Protection Regulation (NDPR), provides guidelines for personal data protection (NITDA, 2019). However, the implementation of these policies is inconsistent across schools due to inadequate resources, lack of policy awareness, and infrastructural deficiencies, especially in secondary schools (Ojo & Akinwale, 2020). As a result, many schools have not fully integrated these policies into their data management practices.

The adaption of international best practices, such as encryption, access controls, and firewall deployment, is suggested to bolster cybersecurity defenses (Ikechukwu & Udeh, 2018). Nonetheless, challenges such as limited funding and technical expertise remain significant barriers. Consequently, there is a need for a contextualized approach to developing cybersecurity policies that suit the Nigerian secondary school environment, especially within the socio-economic realities of Anambra State.

In conclusion, existing literature underscores the critical need for comprehensive cybersecurity policies, increased awareness, and infrastructural investments to protect student data effectively. Addressing these gaps is essential for safeguarding students' privacy and maintaining the integrity of educational records in Nigerian secondary schools.

Methods

The study adopted descriptive survey research design. The population of the study comprised the entire public secondary schools in Awka South LGA with 19 principals and 495 teachers totalling 514. Simple random sampling technique was adopted to select 10 principals (50%) and 396 teachers (80%) as

participants. The respondents are principals and teachers of selected schools numbering 406. The instrument for data collection was designed by the researchers and named "Safeguarding Student Data Cybersecurity Policies, Practices Principals Questionnaire" (SSDCPPPQ). Validation of the instrument was duly certified through scholarly reviews. The reliability of the instrument was ascertained through test re-test method and the results therefrom exposed to Pearson Moment Correlation which yielded an index value of 0.82 which was adjudged adequate for this study. Four point weighting scale. The bench mark is 50% . Fill-on-the-spot technique was adopted coupled with frequent visit to the schools thus all the copies of questionnaire distributed were retrieve giving 100% return rate.

Results

To what extent are existing cybersecurity policies and practices implemented in secondary schools in Anambra State, Nigeria, for safeguarding student data.

Table 1:Mean Scores of the To what extent are existing cybersecurity policies and practices implemented in secondary schools in Anambra State, Nigeria, for safeguarding student data.

S/N	Item statement: To what extent are existing cybersecurity policies and practices implemented in secondary schools in Anambra State, Nigeria, for safeguarding student data.	VH	H	L	VL	Mean	Rmk
1	Video camera	38	49	136	183	1.85	VL
2	Surveillance camera	164	106	50	86	2.85	H
3	Electric fence	128	103	86	89	2.66	H
4	Intruder alarm	88	82	150	86	2.05	VL
5	Biometrics	71	90	155	90	2.34	VL
6	Tracking device	74	101	125	106	2.35	VL
7	Access control system	89	83	138	96	2.40	VL
8	Scan cards	90	77	132	106	2.36	VL
	Grand mean					2.10	VL

Table 1 presents school personnel level of awareness of the digital security devices in public secondary schools in Anambra State as shown on items with serial numbers 2 and 3 (awareness of surveillance and electric fence) having their mean scores above the criterion mean of 2.5. However, items with serial numbers 1, 4-8 were not aware of video camera, intruder alarms, biometrics, tracking device, access control system and scan card as digital school security devices with all their mean scores fallen below the criterion mean of 2.5. The grand mean yielded 2.10.

What are the challenges faced by secondary schools Principals in Awka South of Anambra State in developing and implementing effective cybersecurity policies for protecting student information

Table 2: Mean scores of the challenges faced by secondary schools Principals in Awka South of Anambra State in developing and implementing effective cybersecurity policies for protecting student information**.**

S/N	Item Statement: what is the availability of the following school digital security devices in your school?	Available	Not Available	%	Remark
1	Video camera	Nil	406	100	Not Available
2	Surveillance camera	Nil	406	100	Not Available
3	Electric fence	Nil	406	100	Not Available
4	Intruder alarm	Nil	406	100	Not Available
5	Biometrics	Nil	406	100	Not Available
6	Tracking device	Nil	406	100	Not Available
7	Access control system	Nil	406	100	Not Available
8	Scan cards	Nil	406	100	Not available

Table 2 indicates that none of the school digital security architecture exists in the public secondary schools in Anambra State in this digital period. This is shown in items with serial numbers 1 to 8 with the percentages of 100% which is clearly above the bench mark of 50%.

Discussions

Following the data analysis, the first finding of the study revealed that most of the school personnel are not aware of the various digital school security devices for safety school places in Awka South LGA of Anambra State. Being aware of the digital school security devices is a gate way towards being security conscious. This is imperative because sound educational delivery process and its concomitant goal achievement can only be attained in a serene and danger free school environment. This is why Team Varthana (2024) laid weight on the afore-mentioned assertion thus posited that general safety in a school is the provision of an environment that is safe from threats and dangers. UNICEF (2019) saw the essence of safe school places thus echoed that for quality education to be achieved; learning environment should be safe, healthy and stimulating.

The second finding revealed that none of the school digital security is available in the public secondary schools in Anambra State. Th e alarming increase and dimensions of insecurity in the entire State warrants digitalized security devices that could assist in curbing the insecurity ravaging the populace with school places not an exception. The need for availability of school digital security outfit is what compelled the likes of Hassard (2013) who posited that to achieve safety in school places, video camera

and other ICT devices should be installed in the classrooms as well as the entire school premises. Based on the development, Henry, Echa and Alfred (2017) stressed that the use of biometric has also been identified as a tool to providing adequate security in school places. Andrew (2016) added that Internet of Things (IoT) could also foster safety in school places through its monitoring and tracking capacities which is ICT based.

Recommendations

1. **Develop and Implement Formal Cybersecurity Policies:** School authorities and educational stakeholders should establish comprehensive cybersecurity policies tailored to the needs of secondary schools to guide data protection practices.
2. **Increase Training and Awareness:** Regular training programs should be organized for principals, teachers, and ICT staff to enhance their understanding of cybersecurity threats and best practices for safeguarding student data.
3. **Enhance Infrastructure:** Schools should invest in secure information systems, including firewalls, encryption tools, and reliable internet security measures, to prevent unauthorized access and data breaches.
4. **Establish a Data Protection Culture:** Promoting a cybersecurity-conscious environment within schools will encourage staff and students to adopt safe digital practices.
5. **Collaborate with Government and Organizations:** Schools should work closely with government agencies, such as NITDA, and private sector partners to access resources, training, and up-to-date cybersecurity standards.
6. **Periodic Audits and Monitoring:** Regular security audits should be conducted to identify vulnerabilities and ensure compliance with established data protection policies.

Implementing these recommendations will help safeguard student data effectively, fostering a secure digital learning environment in Anambra State and similar contexts.

References

Eke, O. C., & Nwachukwu, C. (2019). Digital transformation in Nigerian education: Challenges and prospects. *International Journal of Educational Technology*, 16(2), 123-134.

Ikechukwu, T., & Udeh, C. (2018). Cybersecurity in Nigerian schools: Challenges and strategies. *Journal of Information Security and Privacy*, 4(1), 45-58.

NITDA. (2019). *National data protection regulation (NDPR)*. Abuja: National Information Technology Development Agency.

Obinna, O., & Nwabueze, C. (2020). Creating cybersecurity awareness among students in Nigerian secondary schools. *African Journal of Information and Communication Technology*, 12(3), 201-215.

Ojo, O., & Akinwale, O. (2020). Cyber threats and data protection in Nigerian education sector. *Journal of Cybersecurity Research*, 8(4), 102-118.

Uche, O., & Nwali, S. (2021). Investigating cybersecurity readiness in Nigerian secondary schools. *International Journal of Educational Management*, 35(5), 888-902.

Anambra State Ministry of Education. (2020). *Annual education development report*. Awka: Anambra State Government.

Eke, O. C., & Nwachukwu, C. (2019). Digital transformation in Nigerian education: Challenges and prospects. *International Journal of Educational Technology*, 16(2), 123-134.

Ikechukwu, T., & Udeh, C. (2018). Cybersecurity in Nigerian schools: Challenges and strategies. *Journal of Information Security and Privacy*, 4(1), 45-58.

NITDA. (2019). *National data protection regulation (NDPR)*. Abuja: National Information Technology Development Agency.

Obinna, O., & Nwabueze, C. (2020). Creating cybersecurity awareness among students in Nigerian secondary schools. *African Journal of Information and Communication Technology*, 12(3), 201-215.

Ojo, O., & Akinwale, O. (2020). Cyber threats and data protection in Nigerian education sector. *Journal of Cybersecurity Research*, 8(4), 102-118.

Uche, O., & Nwali, S. (2021). Investigating cybersecurity readiness in Nigerian secondary schools. *International Journal of Educational Management*, 35(5), 888-902.

Adebayo, O. (2021). Cybersecurity challenges in Nigerian secondary schools: Implications for data protection. *Journal of Educational Technology in Africa*, 12(3), 45-59.

Okafor, E., & Nwachukwu, C. (2020). Digital transformation in Nigerian education: Ensuring data privacy and security. *International Journal of Educational Development*, 75, 102-109.