FEDERAL UNIVERSITY GUSAU (FUGUS), ZAMFARA STATE, NIGERIA
FUGUS INTERNATIONAL JOURNAL OF LIBRARY AND INFORMATION SCIENCE
(FIJLIS)VOL.2., NO.2, (DECEMBER)2025 DOI: https://doi.org/10.57233/fijlis.v2i2.08
ISSN PRINT:1595-3432
A Publication of the University Library.

# Data Privacy and Security Challenges in Digital Libraries of Tertiary Institutions in Zamfara State

By

**Husaini Musa**
College Library, Federal College of Education (Technical) Gusau
husainimzam@gmail.com
08067718884

**Aisha Sadiq Yelwa**
Inuwa Abdulkadir Library, Sokoto State University, Sokoto State
aishanbaba27@gmail.com
08068110488

**Received on:**11th Nov., 2024 **Revised and Accepted on:** 25th July, 2025 **Published on:** 1st Dec., 2025

**ABSTRACT**

*Digital libraries services have become significant services in the libraries of higher Institution; they provide users with institutional repositories and online electronic information resources based on the curriculum of the institutions. This paper discussed the data privacy and security in digital libraries of tertiary institutions in Zamfara State, two objectives, and research questions respectively were stated to guide the study. Qualitative research design was adopted for the study. Two tertiary institutions' libraries were selected for the study. The population of the study in two libraries was forty- four. The simple random sampling technique was used to sample twelve respondents for the study; the sampled respondents consisted of one staff from each of the six departments in each of the two libraries of tertiary institution. A self-structured interview was used as a means of data collection from respondents; the instrument was validated by 3 experts, who found the instrument valid for the study. All the conversations of the interview were recorded, transcribed, and analysed thematically, using the NVivo software approach, to reveal patterns and insights into the state of digital library security at these institutions. The major findings of this study revealed that adequate infrastructure, training, and financial supports are significant factors that can robust the data security in the institutions. The paper concludes that there are significant gaps that hinder the full protection of digital library resources. Staff highlighted the need for technological upgrades, improved policies, and increased funding to address security weaknesses. Some recommendations were forwarded which includes: Regular workshops on data privacy and security should be conducted for both staff and students to raise awareness and mitigate risks. Institutions should establish formal data privacy policies that align with international best practices and data protection regulations.*

**Keywords:** Data privacy, Security, Digital library, Tertiary institutions, Zamfara State

## Introduction

Digital libraries have become crucial resources for academic institutions, offering a vast range of digital assets to support learning and research. With the increasing reliance on digital platforms, the need to address issues of data privacy and security has become paramount. Institutions must safeguard users' personal data and protect library resources from cyber threats. Digital libraries provide electronic access to a wide array of resources, including e-books, journals, and databases, which has transformed how academic content is accessed, stored, and shared. As these libraries continue to expand, the importance of ensuring data privacy and security cannot be overstated, particularly in tertiary institutions where sensitive academic and personal information is frequently handled.

Data Privacy and Security are terms that are often used interchangeably but address distinct concerns in the digital ecosystem. Data privacy refers to the rights of individuals to control how their personal data is collected, used, and shared (Solove, 2024). Data security, on the other hand, focuses on protecting this data from unauthorized access, breaches, or cyber threats (Anderson, 2023). While both aspects are vital, the rapid digitization of academic libraries has brought these issues to the forefront, as educational institutions become prime targets for cyber attacks due to their vast stores of valuable intellectual property and personal information.

A digital library is defined as an organized collection of digital resources, typically accessible over the internet, which includes both digitized versions of physical resources and born-digital content (Adeyemi *et al.* 2025). Digital libraries support the academic and research missions of institutions by providing access to an array of e-resources that facilitate learning, research, and scholarship. In the context of tertiary institutions in Zamfara State, digital libraries are integral to supporting the educational needs of students and staff. However, these institutions face unique challenges in ensuring the security and privacy of their digital resources.

This research aims to explore the data privacy and security challenges in digital libraries within two teacher-training institutions in the state: The Federal College of Education (Technical), Gusau (FCET Gusau) and the College of Education, Maru (COE Maru). These institutions, like many others, rely heavily on digital systems to deliver educational services, making them vulnerable to data breaches and security lapses. This study seeks to evaluate the data privacy and security challenges faced by digital libraries in tertiary institutions in Zamfara State, with a specific focus on FCET Gusau and COE Maru. The study aims to assess current practices, identify vulnerabilities, and propose solutions to enhance data protection and security in these digital libraries.

## Statement of the Problem

Digital libraries in tertiary institutions across Zamfara State have long been providing essential services for research and education, including institutional repositories, web browsing, Wi-Fi access, and various electronic resources. However, as reliance on digital platforms grows, data privacy and security concerns have become increasingly critical. Protecting user data and safeguarding digital resources from cyber threats is essential for maintaining trust and promoting effective academic activities. While digital libraries offer valuable e-resources accessible through networks like Wi-Fi, they face significant challenges related to data privacy and resource security. Common issues include unauthorised password changes by users without administrative consent, the use of unverified external devices that may spread viruses, and unauthorized copying of resources. These vulnerabilities not only jeopardize library resources but can also disrupt research and learning for students and staff.

Given the importance of secure and reliable digital library services, understanding staff perceptions of data protection and security practices is crucial. Insights from this study could help inform improvements to outdated security protocols, thereby enhancing the quality of digital resources available for research and learning. Without an understanding of staff perceptions on data privacy and protection, institutions risk delivering substandard digital library services that may hinder academic productivity and institutional integrity.

## Scope of the Study

This study focuses on data privacy and security challenges digital libraries of two specific tertiary institutions in Zamfara State: The Federal College of Education (Technical), Gusau (FCET Gusau) and the College of Education, Maru (COE Maru). These institutions were chosen due to their specialized role in training teachers, which aligns with the study's objective of understanding data protection practices within teacher-training institutions. While there are other tertiary institutions in Zamfara State, the scope is deliberately limited to these two colleges to provide a targeted examination within the context of teacher education.

## Research Questions

The study was guided by the following research questions:

1. What measures are currently in place in your institution to protect users' data and ensure the security of digital library resources?
2. How effective do you think these measures are?
3. Have you encountered any challenges or security incidents related to data privacy in the digital library?
4. How were these issues addressed, and what improvements would you recommend enhancing data security?

## Review of Related Literature

A digital library refers to an organized collection of digital content that is accessible electronically, typically over the internet. These libraries consist of digitised versions of traditional printed materials, such as books and journals, as well as resources that are born digital, such as e-books, databases, and multimedia. Digital libraries are central to modern academic institutions, providing access to a wide range of resources that support teaching, learning, and research (Adeyemi *et al*., 2025). Digital libraries offer significant benefits by overcoming space constraints and providing features like search tools, metadata tagging, and multimedia support, which improve accessibility and usability (Harris, 2025). Their 24/7 availability from any location supports research and learning, especially in higher education, while accommodating various formats such as text, video, and audio (Adeyemi, et-al 2025). Despite these advantages, digital libraries face challenges in managing and preserving digital content. Issues like data degradation, format changes, and technology obsolescence threaten long-term access (Harris, 2025). This shift also requires updated management practices, including new metadata standards, copyright policies, and preservation strategies (Lynch, 2024).

### *Data Privacy and Security*

Data privacy and security are critical issues that have emerged with the proliferation of digital libraries and other online platforms. Data privacy refers to the protection of personal information, ensuring that individuals have control over how their data is collected, stored, and

used (Solove, 2024). It encompasses the right of individuals to determine what information is shared and with whom. Security, on the other hand, involves measures to protect data from unauthorized access, breaches, and cyber threats (Anderson, 2023). Together, data privacy and security are essential in safeguarding the integrity of digital libraries, particularly because they store a vast amount of sensitive information, including user data, academic records, and intellectual property.

The growing reliance on digital platforms has made data privacy and security increasingly challenging. Digital libraries, which collect and store a wide range of personal and academic data, are vulnerable to cyber attacks, data breaches, and unauthorized access. Hackers may target these institutions to exploit personal information or steal intellectual property, such as research data, which can be sold or misused (Anderson, 2023). Additionally, with the increasing use of cloud services and shared platforms, data privacy becomes even more complex, as institutions must trust third-party providers to ensure the protection of sensitive information. Digital libraries in educational institutions face high risks related to data privacy and security, as they manage sensitive information like personal data, academic records, and research outputs. To prevent unauthorized access, they must implement strong safeguards such as encryption, multi-factor authentication, and regular audits (Mason, 2023).

Clear policies on data ownership, access, and retention are also vital for legal compliance, including with frameworks like GDPR (Solove, 2024). Human factors like weak passwords and poor training pose additional risks, making staff education and user awareness essential. As Mason (2023) emphasized, fostering a culture of security is just as important as technical solutions.

*Security Measures in Digital Libraries*

Digital libraries are vital to academic institutions, but their growing use brings serious concern about data privacy and security. Basic tools like antivirus software and firewalls are common but often inadequate "most Nigerian university libraries rely on basic antivirus and firewall protections, though these are often insufficient against sophisticated cyber-attacks" (Okike & Adetoro, 2023, p. 63). Advanced solutions such as encryption, multi-factor authentication, and intrusion detection are essential, yet underused due to limited resources. Policies are also crucial, but many institutions "operate without formal cyber security policies, and where such policies exist, they are often outdated or poorly enforced" (Agyeman & Dzandu, 2024, p. 5).

Equally important is staff training and user awareness. Eze and Uzoigwe (2023) found that irregular and poor cyber security awareness among library staff significantly hampers the progress of digital security measures (p. 12). Without ongoing education, even strong technologies fail. Some libraries report minimal breaches thanks to "cautious administrative practices," but Tella and Olarongbe (2022) warned that such caution "cannot substitute for robust technological infrastructure" (p. 33). Sustainable security requires regular audits, policy updates, and expert support.

*Effectiveness of Data Protection Strategies in Academic Libraries*

The effectiveness of data protection strategies in academic libraries depends on the integration of technical, administrative, and human-centered measures. While many libraries use basic tools like antivirus software and firewalls, these are often inadequate. "Most university libraries in Nigeria have firewalls and antivirus programs in place, but these are reactive tools and do not offer full protection against complex threats such as phishing or ransom ware attacks" (Okike & Adetoro, 2023, p. 64). Policy implementation is also weak; as Adebayo and Bakare (2024) pointed out, "having a security policy in place is not enough its implementation,

monitoring, and regular review are what determine its impact" (p. 106). Without proper governance and enforcement, even well-written policies fail to offer real protection.

Human factors also greatly influence effectiveness. Libraries with consistent training programs report fewer data mishandling incidents than those without. (Eze & Uzoigwe, 2023, p. 14). Institutions that align technology, policy, and staff development achieve better outcomes. Tella and Olarongbe (2022) stated, "The most effective strategies are those that integrate technical tools with administrative controls and a culture of security awareness" (p. 36). Collaborating with cyber security experts further enhances preparedness "libraries that seek external expertise in data security tend to be more proactive and responsive to threats" (Alhaji & Baba, 2022, p. 79).

## Methodology

Qualitative research design was adopted for the study. Two tertiary institutions' libraries were selected for the study. The population of the study in two libraries was fortyfour. The Simple random sampling technique was used to sample twelve respondents for the study; the sampled respondents consisted of one staff from each of the six departments in each of the two libraries of tertiary institution. A Self-structured interview was used as a means of data collection from respondents; the instrument was validated by 2 experts who found the instrument valid for the study. All the conversations of the interview were recorded, transcribed, and analysed in thematic approach using the NVivo software where interview transcripts were coded and analyzed for recurring themes. Each interview focused on the following key themes: current data privacy practices, security measures in place, challenges in maintaining privacy and security, and user awareness and training on these issues.

## Data Analysis and Findings

The analysis is based on data transcribed from the interviews conducted. Themes and sub-themes were extracted using NVivo software to organize and analyse the interview conversations, and findings are presented according to the insights shared by the participants. Twelve staff members from the two libraries were interviewed, representing various departments, including the digital library section, technical services, reference services, serials section, reserves section, and the administrative department. To maintain confidentiality, all interviewees requested anonymity; thus, the data presented has been anonymised, with no identifying information about the respondents or their specific departments disclosed.

**Table 1**: Themes and Sub-Themes of the Analysis

| S/N | Themes | Sub-Themes |
|---|---|---|
| 1 | Current data privacy | 1. Security technology<br>2. Policies and procedures<br>3. User Authentication and Access Control<br>4. Training and Awareness |
| 2 | Effectiveness of Data Privacy and Security Measures | 4) Successes of Existing Measures<br>5) Gaps or Weaknesses in Measures<br>6) Risk Management<br>7) External Threats |
| 3 | User Awareness and Training | 1. Technological Enhancements<br>2. Policy and Procedure Improvements<br>3. Regular Training and Awareness Programs<br>4. Collaboration and External Support |
| 4 | Challenges in Maintaining Privacy and Security | 5. Lack of policies<br>6. Lack of fund<br>7. Lack of awareness<br>8. Poor power supply<br>9. Outdated infrastructure |

**1. Current Data Privacy**

a. Security Technology: *"At FCET Gusau, we currently rely on antivirus software and basic firewall protection for our digital library system. While these technologies help with basic protection, they are not sufficient against more sophisticated threats,"* noted a technical staff member. A counterpart at COE Maru added, *"We have similar tools, but we lack more advanced technology, such as encryption protocols, which would better protect our data."*

b. Policies and Procedures: *"Our institution has a general data protection policy,"* explained an administrator at FCET Gusau, *"but it is not very detailed when it comes to digital resources."* Meanwhile, an officer at COE Maru mentioned, *"We have procedures for data access and handling, but they have not been updated recently to keep up with current digital library standards."*

a. User Authentication and Access Control: *"We use basic password protection for user authentication,"* noted a digital librarian at COE Maru. *"However, we have not yet implemented multi-factor authentication, which would provide an extra layer of security."* Staff at FCET Gusau echoed this sentiment, emphasizing the need for enhanced access control measures to limit unauthorized access.

b. Training and Awareness: *"Regular training is limited,"* admitted a reference librarian at FCET Gusau. *"Most staff learns about data privacy informally or through on-the-job experiences."* Similarly, a staff member from COE Maru stated, *"We need structured training programs to raise awareness among staff about data security best practices."*

**2. Effectiveness of Data Privacy and Security Measures**

a. Successes of Existing Measures: *"Our basic security measures have been effective to some extent,"* said digital librarian at FCET Gusau. *"We have not had any major breaches, which I believe is due to our cautious handling of data."* COE Maru digital librarian also agreed, stating, *"While our measures are minimal, they have so far protected us from serious incidents."*

*a.* Gaps or Weaknesses in Measures: *"Our current measures are insufficient against sophisticated cyber threats,"* remarked by an administrative staff at COE Maru. *"We lack the funds for updated software and advanced security technologies."* A digital librarian at FCET Gusau noted similar challenges, *"We are doing our best with what we have, but there are clear gaps in our system."*

b. Risk Management: *"Risk management practices are mostly reactive rather than proactive,"* shared an administrative officer at FCET Gusau. *"We address issues as they arise, but we do not have a structured risk management framework."* At COE Maru, a staff member echoed this, adding, *"We could benefit from regular security audits and assessments to identify potential risks early on."*

c. External Threats: *"We have seen attempts to breach our network from external sources,"* said a COE Maru technical officer. *"We block suspicious IPs, but our defenses are limited."* A technical Staff at FCET Gusau expressed similar concerns, highlighting the need for better defenses against external cyber threats.

**3. User Awareness and Training**

a. Technological Enhancements: *"We could significantly improve our digital library's security by upgrading to more advanced technologies,"* explained a digital librarian at FCET Gusau. *"But budget constraints have limited our progress."* A technical officer at COE Maru agreed, emphasizing, *"We need technology that can provide stronger data encryption and user tracking capabilities."*

b. Policy and Procedure Improvements: *"Our policies need to be updated regularly to stay relevant"* stated an administrator at COE Maru. *"Without policy improvements, we cannot enforce the level of security required."* A staff member at FCET Gusau also noted, *"Clearer, more detailed policies would help us better protect user data and digital resources."*

c. Regular Training and Awareness Programmes: *"There is a lack of consistent training on data privacy,"* admitted a reference librarian at FCET Gusau. *"Most staff members don't know the latest security protocols."* At COE Maru, an administrative staff member highlighted the need for mandatory training sessions to maintain a high level of data security awareness among all staff.

d. Collaboration and External Support: *"We could greatly benefit from collaborating with external cyber security experts,"* mentioned by a reference librarian at COE Maru. *"Their expertise would help us strengthen our data protection."*A counterpart at FCET Gusau echoed this, saying, *"Working with outside specialists could provide us with insights into best practices and advanced security solutions."*

**4. Challenges in Maintaining Privacy and Security**

a. Lack of Policies: *"We don't have comprehensive policies specifically for digital library security,"* admitted by a serial librarian at COE Maru. *"Our guidelines are general and*

*don't address specific digital privacy concerns."* Digital librarian at FCET Gusau expressed similar views, stating that the lack of clear policies hinders effective data protection.

b. Lack of Funds: *"Funding is a major issue,"* remarked an administrator at FCET Gusau. *"Without adequate financial resources, we can't invest in the necessary security tools and training."* An administrative staff member at COE Maru also highlighted financial constraints as a barrier to improving their data security systems.
c. Lack of Awareness: *"Many staff members are not fully aware of data privacy best practices,"* explained a reference librarian at FCET Gusau. *"There's a need for more awareness initiatives."* Similarly, a technical staff at COE Maru noted, *"Increased awareness would help us ensure better data security in daily operations."*
d. Poor Power Supply: *"Frequent power outages disrupt our digital library services and compromise data security,"* mentioned a technical staff member at COE Maru. *"During outages, there is a risk of data loss or corruption."* Digital librarian at FCET Gusau also noted that unreliable power supply impacts their ability to maintain secure systems.
e. Outdated Infrastructure: *"Our infrastructure is outdated, making it challenging to keep up with modern security requirements,"* said a digital librarian at FCET Gusau. *"We need an overhaul to ensure our systems are secure."* Similarly, a technical staff member at COE Maru highlighted that older systems make their digital library vulnerable to security threats.

**Discussion of the Findings**

The findings from FCET Gusau and COE Maru reveal major weaknesses in digital library data privacy and security, especially in technological tools, policy enforcement, access control, and staff training. Both institutions rely on basic antivirus software and firewall protection, which staff admits is not sufficient against more sophisticated threats. A COE Maru staff member noted, "We lack encryption protocols," pointing to a broader issue of inadequate security systems due to limited funding and technical skills (Agyeman & Dzandu, 2024). Outdated and vague policies add to these vulnerabilities, as general guidelines fail to address the specific needs of digital libraries. Authentication is limited to basic password protection, with no multi-factor authentication in place. A common challenge is the absence of proper training, with one staff member stating, "Most staff members do not know the latest security protocols," aligning with Ogungbeni and Adeleke's (2024) observation that poor digital literacy and training hinder data protection in academic libraries.

Despite existing limitations, FCET Gusau and COE Maru have so far avoided major security breaches, mainly due to cautious handling of data rather than robust infrastructure. As one FCET Gusau staff member noted, "We have not had any major breaches," while a COE Maru counterpart added, "While our measures are minimal, they have so far protected us from serious incidents." However, staff acknowledged that this is not sustainable against evolving cyber threats. A COE Maru digital librarian explained, "We lack the funds for updated software and advanced security technologies. Risk management remains reactive, we address issues as they arise, but we don't have a structured risk management framework," said a staff at FCET Gusau. A COE Maru officer emphasized the need for regular security audits and assessments. Network breach attempts were also reported: "We block suspicious IPs, but our defenses are limited," aligning with Okike and Adetoro's (2023) view on institutional vulnerability in Nigeria.

Staff across both institutions recognises that improvement is possible with better funding, training, and collaboration. "We could significantly improve our digital library's security by upgrading to more advanced technologies, stated a digital librarian at FCET Gusau, though

another noted, "Budget constraints have limited our progress." Policy reform was also highlighted: "Without policy improvements, we cannot enforce the level of security required," said an administrator at COE Maru. Training gaps persist. "There is a lack of consistent training on data privacy," said a reference librarian at FCET Gusau. COE Maru staff stressed the need for "mandatory training sessions to maintain a high level of data security awareness." Both institutions expressed interest in expert collaboration: "We could greatly benefit from collaborating with external cyber security experts," noted a COE Maru technical officer, while one from FCET Gusau added that such partnerships could offer insights into best practices and advanced security solutions.

The institutions face key systemic issues such as weak policies as admitted by digital librarian at COE Maru "We don't have comprehensive policies specifically for digital library security, and poor enforcement, with FCET Gusau agreeing that "the lack of clear policies hinders effective data protection." Funding remains a barrier: "Without adequate financial resources, we cannot invest in the necessary security tools and training," noted a FCET administrator. Low staff awareness and weak infrastructure also pose risks. "Many staff members are not fully aware of data privacy best practices," said a FCET librarian, while others pointed to "frequent power outages" and "outdated infrastructure" affecting security. These challenges affirm Schlagwein, Currie, Leimeister and Willcocks's (2025) view that strong policies and tools are ineffective without a culture of cyber security awareness.

## Conclusion

Based on the findings from FCET Gusau and COE Maru, it is evident that while both institutions have implemented basic data privacy and security measures, there are significant gaps that hinder the full protection of digital library resources. Staff highlighted the need for technological upgrades, improved policies, and increased funding to address security weaknesses. Challenges such as outdated infrastructure, inadequate training, lack of comprehensive policies, and limited financial support hinder efforts to maintain a secure digital environment. Additionally, antivirus software is outdated on some systems, and certain computers lack antivirus protection altogether, further exposing the institutions to security risks.

## Recommendations

1. The libraries should establish clear and up-to-date data privacy and security policies that align with international best practices and data protection regulations.
2. Both institutions require increased funding to invest in critical security infrastructure.
3. Staff training on data privacy, security best practices, and cyber threat awareness is essential for a secure digital library environment. Regular awareness campaigns should also be conducted for library users to promote safe usage of digital resources and prevent inadvertent security breaches.
4. Both institutions should consider reliable backup power solutions, such as solar systems, to maintain continuous protection and minimize disruptions to their security protocols.
5. The libraries should ensure regular software updates and Antivirus Protection
6. Both institutions should invest in modern computer systems and robust infrastructure to improve overall security and support advanced data protection measures.

## REFERENCES

Adebayo, O., & Bakare, T. (2024). Policy gaps and security threats in Nigerian academic libraries: A call for institutional response. *Nigerian Journal of Library and Information Science,* 17(2), 101–110.

Adeyemi, I. O., Otaru, G. O., Fashola, O. D., Fasorati, K. K., Fatai, F. A., Bakare, A., & Omupupa, T. K. (2025). Reducing the environmental impacts of ICT adoption with library practices and collection development policies in selected university libraries in Kwara State, Nigeria. *IFLA Journal*, 03400352251342514

Agyeman, E. A., & Dzandu, M. D. (2024). Cybersecurity threats and preparedness in academic libraries in Africa: A review of challenges and prospects. *Library Philosophy and Practice*. https://digitalcommons.unl.edu/libphilprac/7158

Alhaji, I. M., & Baba, M. A. (2022). Digital libraries and data security in Nigerian academic institutions: Current practices and future directions. *Journal of Library and Information Science,* 6(2), 72–81.

Anderson, R. (2023). *Security engineering: A guide to building dependable distributed systems* (3rd Ed.). Wiley.

Eze, J. U., & Uzoigwe, C. U. (2023). Cybersecurity awareness and practices among library staff in academic libraries in Nigeria. *Library Philosophy and Practice*. https://digitalcommons.unl.edu/libphilprac/4022

Harris, M. W. (2025). What is digital library? *Journal of Digital Information*, 22(4), 123-136.

Lynch, C. A. (2024). The role of libraries in digital preservation. *Digital Preservation Review*, 15(2), 89-104.

Mason, R. (2023). Cybersecurity in academic institutions: Protecting the digital library. *International Journal of Information Security*, 29(1), 45-56.

Ogungbeni, J. I., & Adeleke, A. A. (2024). Digital literacy and data security practices among library personnel in selected Nigerian university libraries. Information Impact: *Journal of Information and Knowledge Management*, 12(1), 45–53. https://doi.org/10.4314/iijikm.v12i1.5

Okike, B. I., & Adetoro, N. (2023). Cybersecurity practices and challenges in Nigerian university libraries. *Journal of Applied Information Science and Technology*, 14(1), 59–67.

Schlagwein, D., Currie, W., Leimeister, J. M., & Willcocks L. (2025) Digital futures: definition (what), importance (why) and methods (wow). *Journal of information technology*, 40 (1), 2-8

Solove, D. J. (2024). *Understanding privacy* (2nd Ed.). Harvard University Press

Tella, A., & Olarongbe, S. A. (2022). An assessment of information security practices in academic libraries in Nigeria. *Library Philosophy and Practice*. https://digitalcommons.unl.edu/libphilprac/4330

## AUTHORS' PROFILES



**Husaini Musa** is from Zamfara State, currently pursuing his PhD in Library and Information Science at Career Point University, Kota, India. He holds an M.A. in Librarianship from the University of Sheffield (United Kingdom), a Masters in Information Management, and a Bachelors degree, all from Ahmadu Bello University, Zaria, Nigeria. He also earned a Nigeria Certificate in Education (NCE) from Shehu Shagari College of Education, Sokoto. He serves as Principal Librarian and Lecturer at the Federal College of Education (Technical) Gusau, Zamfara State, where he teaches General Studies in Library and Information Science, Media and Information Science.



**Aisha Sadiq Yelwa** is a highly motivated professional with over five years of experience in promoting literacy and fostering lifelong learning. She currently works at Sokoto State University, where she serves as a Librarian II and Lecturer. Aisha holds a Bachelor's degree in Library and Information Science (BLIS) From Umaru Musa Yar'adua University, Katsina, and earned her Diploma in Library and Information Science from Usmanu Danfodiyo University, Sokoto. In her role at Sokoto State University, Aisha contributes extensively as the Head of the Serials Section and teaches courses in general studies.