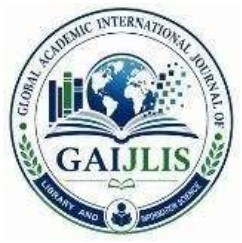
EISSN 3141-6152
GLOBAL ACADEMIC INTERNATIONAL JOURNAL OF LIBRARY AND INFORMATION SCIENCE (GAIJLIS) VOL: 2.1 (2026) PP 30-45



Received: 16.07.2026| Accepted: 30.08.2026 |Published: 10.09.2026
Citations: OMALI, T.O., AMEH, R. & EWEAMA, U.R. (2026) DIGITAL LITERACY, CYBER HYGIENE AND ETHICAL BEHAVIOUR AMONG LIBRARY STAFF AND USERS. Gaijlis vol.3.1. Pp.30-45 https://globreshub.org/index.php/gaijlis/article
DOI: https://doi.org/10.5281/zenodo.22881163

DIGITAL LITERACY, CYBER HYGIENE AND ETHICAL BEHAVIOUR AMONG LIBRARY STAFF AND USERS

OMALI, Theresa O. (Ph.D); AMEH, Rebecca; & EWEAMA, Uju Rosemary (PhD, CLN)
[1-2]**FSI Library, Joseph Sarwuan Tarka University, Makurdi,** [3]**Federal polytechnic Nekede owerri.**

[1]**tessyomali1@gmail.com,**[2]**rebeccaameh811@yahoo.com,3ujueweama@gmail.com**

Abstract

The study is on Digital Literacy, Cyber Hygiene and Ethical Behaviour among Library Staff and Users. It examined the relationship among digital literacy, cybersecurity practices and ethical use of digital resources in academic libraries. The study was guided by five objectives. The conceptual literature reviewed digital literacy, cyber hygiene, cybersecurity awareness, ethical behaviour and digital resources. The theoretical literature examined cybersecurity awareness among librarians and users, safe internet practices and password management, ethical issues of plagiarism, piracy and unauthorised downloading, training needs for cyber hygiene and the influence of digital literacy on ethical use of digital resources. It also examined privacy, protection of personal information, institutional responsibility and cybersecurity culture. Social Cognitive Theory provided the theoretical framework. A qualitative multiple case study design was adopted. The study involved 30 library staff and 200 undergraduate students from two selected tertiary institutions in Anambra and Benue States. Interviews were conducted with library staff, while focus group discussions were conducted with students. Data were analysed using thematic analysis. The findings indicated awareness of common cybersecurity threats but continuing weaknesses in practical cyber hygiene. Password management, safe internet use, plagiarism, piracy and unauthorised downloading emerged as important concerns. Participants identified continuous training as necessary and viewed digital literacy as an important foundation for ethical use of digital resources. The study concluded that digital literacy and cyber hygiene should be developed together. It recommended continuous training, stronger user education, professional development and institutional support.

Keywords: *Digital Literacy, Cyber Hygiene, Ethical Behaviour, Library Staff, Library Users*

Introduction

Digital technologies have become an important part of academic library operations and information use. Library staff and users increasingly depend on computers, mobile devices, online databases, electronic books, institutional repositories, discovery systems and internet services to support teaching, learning and research. This development makes digital literacy an important

competence because effective use of digital resources requires the ability to locate, evaluate, understand and appropriately use information and digital technologies. Agim and Azolo (2019) noted that digital literacy and job performance among twenty first century library staff can be identified internet use, electronic mail, mobile phone use, computer operations and social networking among the digital skills relevant to library work. As library services become increasingly digital, staff and users need corresponding knowledge and skills to use digital resources safely and responsibly.

The increasing use of digital library services has also created concerns about cybersecurity and cyber hygiene. Cyber hygiene refers to the routine practices individuals follow to protect devices, accounts, information and online activities from security threats. These practices include the use of strong passwords, careful handling of personal information, safe browsing, protection against suspicious messages and responsible management of digital accounts. A study by Pasipamire (2025) on cybersecurity in Nigerian university libraries found that librarians had moderately low perceived cybersecurity knowledge and that poor password management was among the challenges affecting library security. The study also found that librarians demonstrated a high level of adherence to cyber ethics and expressed interest in learning more about cybersecurity. Similar concerns have been identified internationally, where library employees have been examined in relation to cyber security awareness, cyber hygiene and actual security behaviour. (Obim & Akpokurerie, 2023)

Ethical behaviour is equally important because digital library users can access, copy, download, reproduce and distribute information with considerable ease. Without adequate understanding, users may engage in plagiarism, piracy, unauthorised downloading, copyright infringement or inappropriate sharing of electronic resources. Recent Nigerian research by Oyewole and Adetimirin (2025) found a relationship between digital literacy skills and attitudes toward plagiarism among Library and Information Science undergraduates, showing the importance of digital competence in discussions of responsible information use. Libraries therefore have responsibilities beyond providing access to digital resources. They need to develop users who can protect their accounts, recognise online risks, respect intellectual property and use electronic information appropriately. Library staff also require continuous training so that they can guide users effectively and model safe and ethical digital behavior, hence the need for this study

Statement of the Problem

Ideally, library staff and users should possess sufficient digital literacy to access digital resources safely, protect their accounts, observe cyber hygiene practices and use electronic information ethically. The current situation is that increasing dependence on digital library services is accompanied by cybersecurity risks, weak password practices, inadequate awareness of cyber threats and inappropriate use of electronic resources. These problems may expose library accounts and information systems to security incidents while also encouraging plagiarism, piracy, unauthorised downloading and copyright violations. Previous studies have examined cybersecurity awareness among Nigerian librarians, digital literacy among library staff and plagiarism among students, but much of the existing evidence has considered these issues separately. Limited qualitative evidence explains how library staff and users jointly understand cyber hygiene, ethical behaviour and the role of digital literacy within tertiary institution libraries in Anambra State. This gap provides the basis for the present study.

Objectives of the Study

The study was guided by five objectives. It sought to:

1. examine the level of cybersecurity awareness among librarians and users;
2. examine safe internet practices and password management in library use;
3. identify ethical issues relating to plagiarism, piracy and unauthorised downloading;
4. examine the training needs for cyber hygiene in academic libraries; and
5. examine the influence of digital literacy on ethical use of digital resources.

Digital Literacy

Digital literacy according to Agim and Azolo (2019) refers to the knowledge and skills required to access, understand, evaluate, create and communicate information through digital technologies. It extends beyond the ability to operate computers because competent digital users must also understand how to search for information, evaluate sources, protect personal information and communicate appropriately in digital environments. In academic libraries, digital literacy is relevant to both staff and users because library services increasingly depend on online catalogues, databases, electronic journals, repositories and digital communication platforms. Agim and Azolo further identified several digital skills among twenty first century library staff, including

internet browsing, electronic mail, mobile phone use, computer operations and social networking. Digital literacy therefore provides a foundation for effective, safe and responsible participation in the digital library environment.

Cyber Hygiene

Cyber hygiene according to Kont (2024) refers to routine behaviours that help individuals and organisations maintain the security of digital devices, accounts, networks and information. It includes creating strong and unique passwords, protecting login credentials, updating software, avoiding suspicious links, using secure networks, protecting personal information and reporting unusual digital activity. Cyber hygiene is important in libraries because staff and users often access multiple digital services through shared or individual devices. Weak cyber hygiene can expose accounts and information resources to unauthorised access. Kont further showed that although the overall cyber security behaviour of respondents was classified as good, device use and prevention and handling of incidents required additional attention. Cyber hygiene should therefore be regarded as an everyday responsibility rather than a technical duty limited to information technology personnel.

Cybersecurity Awareness

Cybersecurity awareness refers to knowledge and understanding of digital threats, protective practices and appropriate responses to security incidents. An aware library user should be able to recognise suspicious links, phishing attempts, unsafe websites, unusual account activity and requests for confidential information. Library staff also need to understand risks associated with electronic resources, shared computers, remote access systems and institutional accounts. Research by Pasipamire (2025) in university libraries found that perceived cybersecurity knowledge among librarians was moderately low and identified poor password management as one of the challenges affecting cybersecurity deployment. Cybersecurity awareness is therefore an important component of digital literacy because knowledge of digital tools without knowledge of their associated risks may leave staff and users vulnerable.

Ethical Behaviour

Ethical behaviour in digital library use according to Dunmade and Tella (2023), involves observing accepted principles governing access, use, reproduction, sharing and communication of information. Ethical users acknowledge the work of authors, respect copyright, avoid plagiarism and refrain from unauthorised access or

distribution of digital resources. ethical behaviour also includes responsible communication, protection of other users' privacy and appropriate use of library facilities. Dunmade and Tella argued that libraries and librarians have an important role in promoting cyberethical behaviour among Nigerian postgraduate students and identified awareness, training, resources and institutional policies as important requirements. Ethical behaviour is therefore not simply a personal matter. It is influenced by users' knowledge, institutional rules, professional guidance and the availability of appropriate support.

Digital Resources

Digital resources include electronic books, electronic journals, online databases, institutional repositories, digital archives, websites, multimedia materials and other electronically accessible information resources. Academic libraries provide these resources to support teaching, learning and research. However, digital resources can easily be copied, stored, shared or distributed outside the conditions under which access was granted. This creates concerns about copyright, licensing, plagiarism, piracy and unauthorised downloading. Latunde Odeku and Mabawonku (2013) reported concerns about misuse of electronic resources and highlighted the importance of access control methods, policies and regulations for protecting digital materials. Responsible use of digital resources therefore requires users to understand both the benefits of access and the obligations attached to that access.

Level of Cybersecurity Awareness among Librarians and Users

Cybersecurity awareness is essential for library staff and users because academic libraries increasingly depend on networked technologies. Library personnel may work with electronic databases, institutional repositories, library management systems, online authentication systems and digital communication platforms, while students use library computers, wireless networks, online databases and personal devices to access information. Awareness enables users to recognise common threats and take preventive action. A study by Pasipamire (2025) found that librarians possessed basic cybersecurity knowledge but that their perceived knowledge remained moderately low. It also identified exposure to several cyber threats and highlighted the need for stronger cybersecurity guidelines and education. This suggests that awareness should involve not only knowledge of cyber threats but also the ability to apply appropriate protective behaviour during everyday library activities.

Table 1: Common Cybersecurity Awareness Areas in Academic Libraries

Awareness area	Expected knowledge
Phishing	Recognising suspicious messages and links
Password security	Creating and protecting strong passwords
Malware	Understanding harmful software and unsafe downloads
Privacy	Protecting personal and account information
Secure browsing	Identifying unsafe websites and connections
Account security	Protecting usernames and authentication details
Incident reporting	Knowing what to do when a security problem occurs
Copyright security	Understanding responsible access to digital resources

Cybersecurity awareness should be shared by both staff and users. When staff understand security risks but users do not, or when users are knowledgeable while staff lack appropriate skills, weaknesses may remain within the library environment. A common understanding of basic cybersecurity responsibilities is therefore important.

Safe Internet Practices and Password Management in Library Use

Safe internet practices involve behaviours that reduce the possibility of unauthorised access, data loss and exposure to online threats. In library settings, these practices include avoiding suspicious websites, checking the legitimacy of links, logging out after using shared computers, protecting authentication details and avoiding the disclosure of passwords to other people. Password management is particularly important because one compromised account can expose electronic resources or other institutional services. The Kont (2024) identified poor password management as a significant challenge affecting the deployment of cybersecurity measures. Library staff and users therefore need practical guidance on password creation, password protection, account recovery and responsible use of shared devices.

Table 2: Safe Internet and Password Practices

Practice	Expected behavior
Password creation	Use strong and difficult to guess passwords
Password protection	Keep passwords confidential
Shared computers	Log out after use
Suspicious links	Avoid opening unverified links
Public networks	Exercise caution when accessing sensitive accounts
Software updates	Keep devices and applications updated
Personal information	Avoid unnecessary disclosure
Incident reporting	Report suspicious activity promptly

Safe internet practices should become routine behaviour rather than occasional instructions provided during library orientation. Libraries can reinforce these practices through user education, signs near public computers, online guidance and staff training.

Ethical Issues of Plagiarism, Piracy and Unauthorised Downloading

Plagiarism, piracy and unauthorised downloading are important ethical issues in digital library use because electronic resources can be copied and distributed easily. Plagiarism involves presenting another person's words, ideas or intellectual work without appropriate acknowledgement. Piracy involves unauthorised reproduction or distribution of protected materials, while unauthorised downloading occurs when users obtain digital resources in ways that violate access conditions, copyright requirements or licence agreements.

Oyewole and Adetimirin (2025) recent study of Library and Information Science undergraduates in Southwestern Nigeria examined the relationship between digital literacy and attitudes toward plagiarism and reported that digital literacy was significantly related to attitudes toward plagiarism. This indicates the importance of developing both technical competence and ethical understanding when students use digital information.

Opara and Eneh (2023) also examined strategies used by Nigerian university librarians to curb plagiarism and reported the use of referencing guidance, plagiarism checking tools and paraphrasing support. These approaches show that libraries can contribute to academic integrity by helping users understand acceptable information practices rather than relying only on punishment after misconduct has occurred.

Training Needs for Cyber Hygiene in Academic Libraries

Training is important because cyber threats and digital technologies continue to change. Library staff may acquire general digital skills through education and experience but may require additional knowledge concerning phishing, password management, privacy protection, malware, safe browsing and incident reporting. Agim, Azolo and Obi (2024) examined strategies for promoting gender inclusiveness in digital literacy programmes for female librarians in universities in Anambra State and demonstrated the continuing importance of structured digital literacy development among library personnel. Training for cyber hygiene should therefore include practical exercises rather than theoretical lectures alone. Staff should be able to identify suspicious messages, protect accounts, respond appropriately to security incidents and guide users in safe digital practices.

Training should also be extended to students. Many students acquire digital habits informally through personal internet use and may not distinguish between ordinary online activity and responsible academic information use. Dunmade and Tella (2023) identified inadequate awareness among Nigerian postgraduate students and the need for training and resources for librarians as challenges to promoting cyberethical behaviour. Academic libraries can address this through orientation programmes, workshops, online tutorials, research support sessions and information literacy programmes.

Influence of Digital Literacy on Ethical Use of Digital Resources

Digital literacy can influence ethical use of digital resources by giving users the knowledge required to understand how information should be accessed, evaluated, acknowledged and shared. A digitally literate user should be able to distinguish reliable information from questionable sources, recognise copyright restrictions, cite information appropriately and understand the consequences of unauthorised use. Research among Library and Information Science undergraduates in Southwestern Nigeria by Oyewole and Adetimirin (2025) found a significant relationship between digital literacy skills and attitudes toward plagiarism. The finding suggests that digital literacy is relevant to ethical information behaviour. However, digital literacy alone may not guarantee ethical conduct because users also need awareness of institutional rules, copyright principles, academic integrity and the consequences of misconduct.

Table 3: Digital Literacy Skills and Ethical Digital Resource Use

Digital literacy skill	Ethical application
Information searching	Finding legitimate information sources
Source evaluation	Distinguishing credible information
Citation skills	Acknowledging information sources
Copyright awareness	Respecting intellectual property
Downloading skills	Observing access conditions
Privacy awareness	Protecting personal information
Digital communication	Communicating responsibly
Information management	Storing and sharing resources appropriately

Digital literacy should therefore be developed as a combination of technical competence, information evaluation and ethical understanding.

Privacy and Protection of Personal Information

Privacy is an important part of cyber hygiene because library systems may process information relating to users, accounts, searches, borrowing activities, electronic resource access and communication. Staff and users need to understand that personal information should not be disclosed unnecessarily or handled carelessly. Privacy protection also requires responsible use of shared computers, appropriate password practices and careful management of digital records. According to Pasipamire (2025) Cybersecurity awareness should therefore include knowledge of both external threats and internal responsibilities. Libraries need to establish clear procedures for protecting user information and educating staff about confidentiality. This is particularly important in digital environments where information can be copied, transmitted and stored rapidly. Protecting privacy contributes to user trust and encourages users to interact with digital library services without unnecessary fear of exposure.

Institutional Responsibility and Cybersecurity Culture

Cybersecurity should not be treated solely as an individual responsibility. Academic libraries require institutional structures that provide secure systems, appropriate policies, staff training, incident reporting procedures and continuous awareness programmes. Pasipamire (2025) systematic review of cybersecurity awareness in libraries identified customised training, integration of cybersecurity with digital literacy, organisational culture, stakeholder participation and continuous evaluation as

important themes in building cybersecurity awareness. A strong cybersecurity culture therefore develops when management, library staff, students and technical personnel share responsibility for protecting digital resources. Such a culture encourages people to report suspicious activities and adopt safe practices instead of assuming that cybersecurity is exclusively the responsibility of information technology personnel.

Theoretical Framework

Social Cognitive Theory

The study was anchored on Social Cognitive Theory developed by Albert Bandura. The theory explains human behaviour as the result of interaction among personal factors, behaviour and the environment. It is appropriate for the study because digital literacy, cyber hygiene and ethical behaviour are learned and reinforced through observation, instruction, experience and social interaction. Library staff and users can acquire cybersecurity and ethical information practices through training, demonstrations, peer behaviour, library policies and repeated use of digital services. The theory also recognises the importance of self efficacy, meaning the individual's belief in the ability to perform a particular behaviour successfully. Applied to this study, Social Cognitive Theory suggests that users who possess appropriate digital knowledge, observe safe practices among others and receive institutional support are more likely to develop safe and ethical digital behaviour. The theory therefore provides a suitable basis for examining the relationship among digital literacy, cyber hygiene and ethical conduct in academic libraries.

Methodology

The study adopted a qualitative multiple case study design. The study was conducted in two selected tertiary institutions with one in Anambra State, namely Nnamdi Azikiwe University, Awka and Benue State University, Marurdi. The study involved 230 participants comprising 30 library staff and 200 undergraduate students. Fifteen library staff were purposively selected from each institution for semi structured interviews because of their direct involvement in library operations and digital services. The 200 students were organised into focus group discussions, with 100 students from each institution and ten students in each discussion group. Interview data were obtained from library staff, while focus group discussions were conducted with students. The data were analysed thematically according to the five objectives of the study.

Thematic Presentation of Findings

The following findings represent the proposed thematic pattern derived from the findings of the study.

Theme One: Level of Cybersecurity Awareness among Librarians and Users

The thematic analysis indicated that both library staff and students had some awareness of common cybersecurity threats, particularly phishing, account compromise, suspicious links and unauthorised access. Library staff demonstrated greater awareness of cybersecurity responsibilities associated with library systems, while students tended to focus on threats encountered during everyday internet use. However, the analysis suggested that awareness was not always accompanied by consistent protective behaviour. Some participants understood the importance of password security and safe browsing but did not always apply the practices consistently. This pattern is consistent with findings by Obim and Akpokurerie (2023) on Nigerian university libraries where librarians possessed basic cybersecurity knowledge but perceived knowledge remained moderately low and additional learning was desired.

Table 4: Theme One

Analytical category	Thematic finding
Cyber threats	Participants recognised several common online threats
Staff awareness	Staff demonstrated knowledge of library related security concerns
Student awareness	Students recognised common internet risks
Knowledge and behaviour	Awareness did not always result in consistent safe practices
Incident response	Participants identified the need for clearer reporting procedures
Further learning	Participants expressed the need for additional cybersecurity education

Theme Two: Safe Internet Practices and Password Management

The second theme showed that participants recognised password protection and safe internet use as important aspects of cyber hygiene. Participants identified strong passwords, password confidentiality, careful use of shared computers and avoidance of suspicious links as important practices. However, the analysis suggested that password management remained an area requiring continuous attention. Students in particular were more likely to discuss convenience when using passwords across different digital services, while library staff were more concerned with protecting institutional accounts. The finding is consistent with Pasipamire (2025) evidence that poor password management remains a challenge in university libraries. The analysis

therefore suggests that library cyber hygiene programmes should address practical behaviour rather than concentrating only on general awareness.

Table 5: Theme Two

Analytical category	Thematic finding
Password protection	Participants recognised the need to protect passwords
Password sharing	Sharing of passwords was regarded as unsafe
Shared computers	Participants identified logging out as important
Suspicious links	Participants recognised the need for caution
Public networks	Participants expressed concern about sensitive account use
Security reporting	Participants supported prompt reporting of suspicious activity

Theme Three: Ethical Issues of Plagiarism, Piracy and Unauthorised Downloading

The third theme revealed that participants understood plagiarism as an important ethical problem in digital resource use, although the depth of understanding differed. Students associated plagiarism primarily with copying academic materials without acknowledgement, while library staff also connected it with inappropriate use of electronic databases and digital resources. Piracy and unauthorised downloading were identified as concerns because users may attempt to obtain or distribute resources beyond the conditions established by publishers or libraries. This finding agrees with research by Oyewole and Adetimirin (2025) showing the importance of digital literacy in shaping attitudes toward plagiarism among Nigerian Library and Information Science undergraduates. It also agrees with studies recommending user education, plagiarism awareness and library guidance as mechanisms for promoting responsible information use.

Table 6: Theme Three

Ethical issue	Thematic finding
Plagiarism	Users need stronger understanding of acknowledgement and citation
Piracy	Participants recognised unauthorised reproduction as unethical
Unauthorised downloading	Participants identified access restrictions as important
Copyright	Participants recognised the need to respect creators' rights
Citation	Students required continuing guidance
User education	Libraries were viewed as important sources of ethical guidance

Theme Four: Training Needs for Cyber Hygiene in Academic Libraries

The fourth theme established that both library staff and users require continuous education on cyber hygiene. Participants identified password management, phishing awareness, privacy protection, safe browsing, incident reporting and responsible use of electronic resources as important training areas. Library staff also identified the need to understand emerging security risks so that they can provide appropriate guidance to users. This finding is supported by Agim, Azolo and Obi (2024) work on digital literacy programmes for librarians in Anambra State, which emphasised the need for strategies that support digital literacy development among library personnel. It also corresponds with the Nigerian literature on cyberethical behaviour, which identifies training and resources for librarians as important requirements for promoting responsible online behaviour.

Table 7: Theme Four

Training area	Thematic finding
Password management	Participants needed practical password security skills
Phishing	Participants needed better recognition of suspicious messages
Privacy	Participants needed guidance on protecting personal information
Safe browsing	Participants needed practical internet safety skills
Incident response	Participants needed knowledge of reporting procedures
Copyright	Students required continuing instruction
Plagiarism	Users required stronger academic integrity education

Theme Five: Influence of Digital Literacy on Ethical Use of Digital Resources

The fifth theme indicated that digital literacy was perceived as an important foundation for ethical use of digital resources. Participants associated digital literacy with the ability to locate reliable information, evaluate online sources, cite materials appropriately, understand copyright restrictions and use electronic resources within acceptable conditions. Library staff viewed digital literacy as an important means of guiding students, while students associated it with improved confidence in searching and using electronic resources. The finding is consistent with Oyewole and Adetimirin (2025) study, which reported a significant relationship between digital literacy skills and attitudes toward plagiarism among Library and Information Science undergraduates. The thematic

evidence therefore suggests that digital literacy should incorporate ethical and security competencies rather than focusing solely on technical operation of digital tools.

Table 8: Theme Five

Digital literacy area	Ethical implication
Searching	Encourages legitimate information access
Evaluation	Reduces dependence on unreliable information
Citation	Helps prevent plagiarism
Copyright awareness	Supports lawful use of digital materials
Downloading	Encourages respect for access conditions
Privacy awareness	Supports protection of personal information
Digital communication	Encourages responsible online behaviour

Summary of the Analysis

The thematic analysis produced five major findings. First, library staff and students demonstrated awareness of common cybersecurity threats, although the level of understanding and practical application differed among participants. Second, safe internet practices and password management emerged as important areas requiring continuous reinforcement, particularly in relation to account protection and use of shared digital facilities. Third, plagiarism, piracy and unauthorised downloading emerged as major ethical concerns associated with digital resource use. Fourth, participants identified continuing training in password security, phishing, privacy, safe browsing, incident reporting, plagiarism and copyright as important cyber hygiene needs. Fifth, digital literacy was perceived as an important foundation for ethical use of digital resources because it enables users to search, evaluate, cite, download and share information more responsibly. Overall, the analysis indicated that cybersecurity and ethical behaviour require a combination of individual knowledge, practical skills, institutional support and continuing library education.

Conclusion

Digital literacy, cyber hygiene and ethical behaviour are closely connected within the contemporary academic library environment. The proposed thematic findings showed that library staff and users possessed awareness of several cybersecurity and ethical concerns, but gaps remained in the consistent application of safe internet practices, password management and responsible use of digital resources. Plagiarism, piracy and unauthorised downloading were identified as important ethical challenges, while continuous training was considered necessary for both staff and

students. The study also indicated that digital literacy can support ethical use of electronic information by improving users' ability to evaluate, acknowledge, protect and appropriately share digital resources. Academic libraries should therefore treat digital literacy and cyber hygiene as continuing educational responsibilities supported by clear institutional policies, practical training and active guidance from library staff.

Recommendations

1. Academic libraries should establish regular cybersecurity awareness and cyber hygiene programmes for library staff and students.
2. Libraries should provide practical training on password management, phishing awareness, safe browsing, privacy protection and responsible use of shared digital facilities.
3. User education programmes should give greater attention to plagiarism, piracy, copyright, unauthorised downloading and appropriate citation of digital information.
4. Library management should provide continuous professional development for staff so that they can recognise emerging cybersecurity threats and provide appropriate guidance to users.
5. Digital literacy programmes in academic libraries should integrate technical skills with cybersecurity awareness, information evaluation, academic integrity, copyright knowledge and ethical digital behaviour.

References

Agim, E. C., & Azolo, E. M. (2019). Digital literacy and job performance of 21st century library staff in Imo State. *Library Research Journal, 4*, 15–26. The publication details are supported by the NAU journal record and the article PDF.

Agim, E. C., Azolo, E. M., & Obi, A. (2024). Strategies for promoting gender inclusiveness in digital literacy programs for female librarians in universities in Anambra State. *Journal of Applied Information Science and Technology, 17*(1).

Agim, E. C., Irieguna, S., & Chivuzo, C. C. (2023). Utilization of media resources for instructions among library educators in adult learning centers in Awka South LGA. *Library Philosophy and Practice*.

Dunmade, A. O., & Tella, A. (2023). Libraries and librarians' roles in ensuring cyberethical behaviour. *Library Hi Tech News, 40*(7), 7–11. https://doi.org/10.1108/LHTN-04-2023-0068

Kont, K. R. (2024). Libraries and cyber security: The importance of the human factor in preventing cyber attacks. *Library Hi Tech News, 41*(1), 11–15. https://doi.org/10.1108/LHTN-03-2023-0036

Latunde Odeku, O. E., & Mabawonku, I. (2013). Assessment of digital access control methods used by selected academic libraries in South West Nigeria. *African Journal of Library, Archives and Information Science, 23*(2). https://doi.org/10.4314/yds2jz25

Obim, I. E., & Akpokurerie, A. O. (2023). Awareness of cybersecurity and its impact on information storage in the university libraries in South East Nigeria. *Information Technology and Librarianship, 3*(2), 129–136.

Opara, V. C., & Eneh, A. C. (2023). Curbing plagiarism: Strategies adopted by librarians in universities in the age of ICT in Nigeria. *Library Philosophy and Practice*.

Oyewole, O., & Adetimirin, A. (2025). Digital literacy skills and attitude towards plagiarism by library and information science undergraduates in Southwestern Nigeria. *Alexandria: Journal of National and International Library and Information Issues*. https://doi.org/10.1177/09557490251378738

Pasipamire, E. (2025). Building a culture of cybersecurity awareness in libraries: A systematic review of best practices and frameworks. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.24.1.3608

Uzoagba, N. C., Agim, E. C., & Ezejiofor, V. O. (2024). Assessment of the implementation of information and communication technology tools among library educators in tertiary institution in Anambra State. *Library Philosophy and Practice*, 8068. The publication and authorship are confirmed through the Nnamdi Azikiwe University research profile.