

Research Article

Data Privacy and Information Security in Academic Libraries: A Qualitative Case Study of the Uganda Institute of Information and Communications Technology Library

Nalunkuma Elizabeth , Edward Ssali* 

Library Department, Uganda Institute of Information and Communications Technology, Kampala, Uganda

Abstract

Purpose – This study examines how data privacy and information security are understood and operationalized in the Uganda Institute of Information and Communications Technology (UICT) Library, with particular attention to the relationship between institutional safeguards, staff and user awareness, and trust in digitally mediated library services. **Design/methodology/approach** – A qualitative case study was conducted in 2025 using semi-structured interviews with five staff members (three librarians and two IT officers) and focus group discussions with ten library users (six students and four lecturers). Participants were purposively selected for their direct experience of library data handling or use of library services. Data were analysed thematically using Braun and Clarke’s six-phase approach, with staff and user accounts compared to identify convergence and divergence. **Findings** – Four interrelated themes emerged: (1) foundational safeguards without library-specific privacy governance; (2) asymmetrical privacy awareness between staff and users; (3) interacting resource, infrastructure and capability constraints; and (4) the need for an integrated governance, capacity and awareness response. Across these themes, uncertainty about data handling was closely connected to user trust. **Originality/value** – The study provides institution-level qualitative evidence from a Ugandan academic library, a context that remains underrepresented in empirical library privacy research. By examining staff and users together, it shows that privacy readiness depends not only on technical controls but also on policy localization, user awareness and institutional trust. The findings extend debates on information governance and digital transformation by showing how national data-protection requirements are translated—or fail to be translated—into everyday library practice in a resource-constrained setting.

Keywords

Data Privacy, Information Security, Academic Libraries, Information Governance, Digital Libraries, Uganda

1. Introduction

The rapid adoption of digital technologies has significantly transformed library operations worldwide, enabling improved access to information resources and more efficient service de-

livery. Academic libraries increasingly rely on integrated library management systems (ILMS), online catalogues, and networked information services to support teaching, learning, and

*Correspondence: Edward Ssali (ssalibazira@gmail.com)

Received: 17 September 2026; **Accepted:** 29 September 2026; **Published:** 31 October 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

research. While these technologies enhance efficiency and accessibility, they also introduce complex challenges related to data privacy and information security, particularly concerning the collection, storage, and processing of users' personal data [2, 3, 7].

Libraries have a long-standing ethical obligation to protect user privacy, which is closely linked to intellectual freedom and trust in information institutions. Users must be confident that their reading histories, search activities, and personal details are not subject to unauthorized access, surveillance, or misuse [1]. In digital environments, however, this responsibility is increasingly difficult to uphold due to cyber threats, weak institutional controls, and limited staff capacity, especially in developing-country contexts.

In Uganda, the enactment of the Data Protection and Privacy Act (2019) provides a national legal framework governing the lawful handling of personal data by public and private institutions. The Act outlines key principles such as data minimization, security safeguards, accountability, and user rights, which are directly applicable to library operations [12]. Despite this legal framework, studies indicate that compliance within libraries and other information institutions remains inconsistent, largely due to limited awareness, inadequate funding, obsolete infrastructure, and insufficient training of personnel responsible for managing digital systems [9, 11].

The Uganda Institute of Information and Communications Technology (UICT) Library offers a particularly informative setting in which to examine these issues. As a specialist academic institution centred on information and communication technology, UICT combines an increasingly digital library environment with the resource and governance constraints that characterize many higher-education institutions in the region. Its library uses an integrated library management system and electronic user records, thereby creating routine points at which personal, transactional and intellectual-use data are collected and managed. Yet there is limited institution-level evidence showing how Uganda's national data-protection requirements are interpreted in the everyday practices of academic libraries. This study addresses that gap by examining both sides of the privacy relationship: staff who handle or administer library data and users whose data are collected. The case therefore contributes beyond a description of security tools; it reveals how technical safeguards, policy arrangements, privacy awareness and user trust interact within a resource-constrained digital library environment.

1.1. Problem Statement

Despite the growing digitization of library services in Uganda, significant challenges persist in the effective implementation of data privacy and information security measures. At the UICT Library, the increased use of digital systems such as integrated library management systems and online catalogues has expanded the volume of personal data collected from users. However, the mechanisms for protecting this data

remain limited and largely dependent on basic technical controls and general institutional ICT policies rather than comprehensive, library-specific data protection frameworks.

Although the Data Protection and Privacy Act (2019) provides a clear legal basis for safeguarding personal information, evidence suggests that compliance at the institutional level is often weak due to low awareness, inadequate enforcement, and resource constraints [9, 12]. Previous studies in Ugandan academic libraries indicate that limited staff training, outdated ICT infrastructure, and insufficient financial resources hinder the adoption of advanced security measures such as encryption, intrusion detection systems, and multi-factor authentication [10, 11].

Furthermore, many library users remain unaware of their data privacy rights and the ways in which their personal information is collected, stored, and used. This lack of awareness increases vulnerability to data misuse and undermines confidence in libraries as safe and trusted information spaces [1, 9]. When users perceive that their personal information may not be adequately protected, they may limit their engagement with library services, thereby affecting service utilization, institutional credibility, and learning outcomes. Without a clear understanding of existing practices, awareness levels, and implementation challenges, the UICT Library risks continued exposure to data privacy breaches and erosion of user trust.

1.2. Objectives of the Study

1.2.1. General Objective

The general objective of this study is to examine data privacy and information security practices at the Uganda Institute of Information and Communications Technology (UICT) Library, with a focus on identifying existing measures, awareness levels, challenges, and opportunities for strengthening the protection of users' personal data in a digital library environment.

1.2.2. Specific Objectives

The study is guided by the following specific objectives:

- 1) To examine the current data privacy and information security measures implemented at the UICT Library in the management of users' personal and transactional data.
- 2) To assess the level of awareness and understanding of data privacy rights and information security responsibilities among library staff and users at the UICT Library.
- 3) To identify the key institutional, technical, and human resource challenges affecting the effective implementation of data privacy and information security protocols at the UICT Library.
- 4) To propose practical strategies for enhancing data privacy and information security practices in academic libraries in Uganda, in line with national legislation and international best practices.

2. Literature Review

Data privacy in libraries is both an information-governance issue and a professional obligation. Digital library systems routinely process identity data, borrowing transactions, authentication records and traces of information-seeking activity. Protecting these data supports intellectual freedom and trust because users may alter their information behaviour when they believe their reading or searching can be monitored [1, 3]. Information security provides the technical and organizational safeguards that support this obligation, while privacy additionally requires clarity about why data are collected, who may access them, how long they are retained and what rights users possess. For academic libraries, effective protection therefore requires more than cybersecurity tools; it requires governance arrangements that connect technology, policy and user rights.

Conceptually, the study uses an information-governance lens in which privacy protection depends on the alignment of legal obligations, organizational rules, technical safeguards and user-facing transparency. This lens is appropriate to libraries because confidentiality is not secured by technology alone: governance must also determine the purpose and proportionality of data collection, access authorization, retention, disclosure and accountability. The framework therefore connects professional privacy obligations with the institutional controls through which they are implemented [1, 3].

In Uganda, the Data Protection and Privacy Act (2019) provides the principal legal benchmark for the study [12]. Its requirements are used analytically to assess whether library practice reflects lawful and fair processing, purpose specification, data minimization, data quality, security safeguards, transparency and accountability, together with the rights of data subjects. These requirements are directly relevant to registration data, borrowing histories, authentication records and other personal information processed through library systems. Research on Ugandan libraries and public institutions nevertheless points to an implementation gap between formal requirements and operational practice. Kedi identifies privacy and data-protection concerns in an academic-library setting [9], while Nakaziba and Ngulube show that digital transformation in Ugandan university libraries is shaped by institutional capacity and infrastructure [10]. Odong et al. similarly report challenges in compliance with ICT standards in university libraries [11]. Taken together, this literature suggests that the existence of national rules does not by itself establish privacy-protective library practice; implementation depends on localized policies, infrastructure, staff capability and institutional accountability.

Recent library research further shows that privacy risks expand as services become more networked and data-intensive. Emerging technologies, including artificial intelligence, increase the complexity and opacity of data processing and strengthen the case for user-centred safeguards [2]. Work on cybersecurity and technology-based security in libraries likewise emphasizes the need to move beyond basic protective

tools toward integrated approaches that combine technical controls with organizational processes and staff capability [6, 7]. These developments are relevant to Ugandan academic libraries because digital transformation can increase both service capacity and exposure to privacy and security risks when governance and infrastructure develop unevenly.

Despite this growing literature, three gaps remain. First, much of the Ugandan discussion addresses digital transformation, ICT standards or institutional policy at a broad level rather than examining how privacy is enacted inside a specific academic library. Second, existing work rarely places the perspectives of data handlers (librarians and IT staff) alongside those of data subjects (library users), making it difficult to identify mismatches in privacy understanding. Third, limited empirical attention has been given to the relationship between privacy practice and users' trust in library services in resource-constrained settings. The UICT case addresses these gaps by analysing technical safeguards, policy arrangements, staff and user awareness, implementation constraints and trust within the same institutional setting. This focused case contributes to information-governance scholarship by showing how formal data-protection expectations encounter everyday library practice.

3. Methodology

3.1. Research Design

This study adopted a qualitative case study research design to explore data privacy and information security practices at the UICT Library. A qualitative approach was considered appropriate because it enables an in-depth examination of participants' experiences, perceptions, and institutional practices within their real-life context, particularly in areas where empirical evidence remains limited [5]. The case study design facilitated a detailed understanding of how data privacy and information security are operationalized within a single academic library setting.

3.2. Study Area

The study was conducted at the UICT Library, which serves students, academic staff, and administrative personnel of the Uganda Institute of Information and Communications Technology. The library relies on digital systems such as integrated library management systems and electronic user records to deliver services, making it a relevant context for examining data privacy and information security practices.

3.3. Study Population and Sampling

The study population comprised library staff and library users at UICT. A purposive sampling technique was employed to select participants with direct experience relevant to the

study: librarians and IT officers involved in handling or supporting library systems and user records, and students and lecturers who used library services and supplied personal information in doing so. The sample consisted of 15 participants, including five staff members (three librarians and two IT officers) and ten library users (six students and four lecturers). This sampling strategy ensured the inclusion of both data handlers and data subjects, enabling a balanced examination of institutional practices and user perspectives.

Table 1. Study population.

Designation	Number
Staff Members (3 Librarians & 2 IT Officers)	5
Library users (6 Students and 4 Lecturers)	10
Total	15

Source: Researcher 2025.

3.4. Data Collection Methods

Data were collected in 2025 using semi-structured interviews and focus group discussions (FGDs). Semi-structured interviews were conducted with the five staff participants to explore existing data privacy measures, security protocols, institutional policies and implementation challenges. FGDs involved the ten user participants (six students and four lecturers) and explored awareness, experiences and perceptions regarding the collection, access, storage and protection of personal data within the library environment. Interview and FGD material was documented for thematic analysis, with identifying information excluded from the analytical record. The use of multiple participant groups and data collection methods enhanced the depth and credibility of the findings through methodological and source triangulation.

3.5. Data Analysis

The qualitative data were analysed using thematic analysis following Braun and Clarke's six-phase framework [4, 5]. Analysis began with repeated familiarization with the interview and FGD material, followed by the generation of initial codes capturing recurring issues in participants' accounts. Codes relating to access controls, policy gaps, confidentiality awareness, user uncertainty, infrastructure, training, trust and proposed improvements were compared and clustered into candidate themes. These candidate themes were then reviewed against the dataset, refined for internal coherence and distinctiveness, and defined as four final themes: (1) foundational safeguards without library-specific privacy governance; (2) asymmetrical privacy awareness between staff and users; (3) interacting resource, infrastructure and capability constraints; and (4) an integrated

governance, capacity and awareness response. Staff and user accounts were compared rather than merged into a single source, enabling areas of convergence and divergence to be identified. This process created a direct analytical link between the coded data, the themes reported in the Results section and the four themes summarized in the abstract.

3.6. Trustworthiness and Rigour

To enhance the trustworthiness of the study, several strategies were employed. Credibility was ensured through triangulation of data sources (staff and users) and data collection methods (interviews and FGDs). Dependability was supported by maintaining a clear audit trail of the research process, including data collection procedures and analytical decisions. Transferability was addressed by providing a detailed description of the study context and participants, allowing readers to assess the applicability of the findings to similar library settings.

3.7. Ethical Considerations

The study adhered to established ethical research principles. Participants were informed about the purpose of the study and provided informed consent prior to participation. Confidentiality and anonymity were ensured by excluding personal identifiers from the analytical material and reporting. Participation was voluntary, and respondents were informed of their right to withdraw from the study at any stage without penalty. Participant accounts were reported in a manner intended to prevent identification of individual respondents. These measures ensured ethical integrity throughout the research process.

4. Results

The thematic analysis produced four interrelated findings: foundational safeguards without library-specific governance; an asymmetry in privacy awareness between staff and users; resource and capability constraints that limit stronger protection; and an integrated governance, capacity and awareness response. The themes draw on staff interviews and user FGDs and are presented comparatively to show where institutional practice and user experience converge or diverge. The original interview and FGD transcripts or verbatim records are no longer available to verify participants' exact wording. Accordingly, the findings below use attributed thematic summaries and paraphrases rather than reconstructed quotations. This approach preserves the evidential distinction between what can be supported by the retained study findings and wording that cannot now be verified.

4.1. Foundational Safeguards Without Library-specific Privacy Governance

Staff interview evidence indicated that day-to-day safeguards were already being used to protect library records. The

recurring practices identified in the staff accounts were password protection for the integrated library management system, antivirus protection on public-access computers, and restriction of circulation and user-registration records to authorized personnel, principally librarians and IT officers. Synthesised across the staff accounts, these practices show that privacy protection was operationally present but concentrated on access control and endpoint security rather than on a comprehensive information-governance framework.

Across the staff accounts, however, no dedicated library-specific data privacy policy was identified. Staff instead described reliance on general institutional ICT guidance. This distinction is important because general ICT rules do not necessarily specify how library-specific data—such as borrowing histories, registration details or access by third-party systems—should be minimized, retained, disclosed or deleted. The empirical pattern is therefore not an absence of security, but a gap between basic operational protection and explicit privacy governance. In practice, responsibility is concentrated among librarians and IT personnel without a library-level framework that clearly translates national data-protection principles into routine procedures.

4.2. Asymmetrical Privacy Awareness Between Staff and Users

A synthesis of staff interview accounts indicated practical awareness of confidentiality responsibilities. Librarians and IT personnel understood that login credentials and borrowing records required protection and that access to user information should be restricted. At the same time, the accounts consistently indicated that this awareness arose mainly from routine system use and general ICT training rather than dedicated privacy education. The retained findings further indicate that staff training focused more strongly on system use than on data-protection concepts. Taken together, this evidence suggests operational awareness of confidentiality, but less structured exposure to principles such as data minimization, purpose limitation, retention and data-subject rights.

The user FGD findings showed a different pattern. Across the user accounts, participants generally expected information supplied to the library to be protected, while demonstrating limited awareness of what personal data were collected, how long records were retained, who could access them, or how digital activity might be recorded within library systems and networks. The retained findings also show that awareness of digital footprints associated with networked library services was limited. The contrast between the two participant groups is analytically important: staff demonstrated practical confidentiality knowledge, whereas users had substantially less visibility into the data lifecycle. Privacy at UICT was therefore experienced more as an implicit institutional expectation than as a transparent process understood by data subjects.

4.3. Interacting Resource, Infrastructure and Capability Constraints

The staff interview findings consistently linked weak privacy implementation to three mutually reinforcing constraints: financial limitations, ageing ICT infrastructure and limited specialist privacy capability. Financial constraints restricted investment in controls such as encryption, intrusion detection and multi-factor authentication; older infrastructure reduced the institution's capacity to implement stronger contemporary controls; and limited specialist training increased the library's dependence on IT officers for security-related decisions. Considered together, these recurring accounts indicate that the implementation gap cannot be attributed to a single missing technology. Rather, resource, infrastructure and skills constraints interact and reinforce one another.

The user FGD findings further indicated that uncertainty about data handling could affect confidence in disclosing personal information. Across the retained accounts, some users were uncomfortable providing personal identifiers when they did not understand how the information would subsequently be handled. Staff accounts similarly recognized that an actual or perceived privacy failure could affect the reputation of both the library and UICT. The convergence of these two strands of evidence connects privacy governance with institutional trust: user uncertainty is not only an awareness issue but may also influence confidence in using library services.

4.4. An Integrated Governance, Capacity and Awareness Response

The proposed solutions recorded across staff and user accounts reflected the multidimensional nature of the identified problems. The recurring priorities were a library-specific data-protection policy aligned with the Data Protection and Privacy Act (2019), regular staff training in privacy and cybersecurity, user-facing awareness measures such as orientation sessions and clear privacy notices, stronger technical controls including encryption and multi-factor authentication, and collaboration with national technical and regulatory bodies such as NITA-U. Synthesised across participant groups, these proposals support an integrated approach in which governance, staff capability, user transparency and technical safeguards develop together rather than as isolated interventions.

5. Discussion

This study shows that data privacy at UICT Library is best understood as an information-governance challenge rather than solely as a cybersecurity problem. The library has recognizable technical safeguards, but these operate alongside a policy gap and uneven privacy awareness. The central finding is therefore a three-part disconnect between technical protection, formal governance and user understanding. This helps explain why the presence of passwords, antivirus software and

restricted access does not necessarily translate into a privacy environment that users can understand and trust.

The reliance on general institutional ICT policies illustrates the importance of policy localization. Using the Data Protection and Privacy Act (2019) as an analytical benchmark, the findings indicate gaps in translating requirements concerning purpose specification, data minimization, security safeguards, transparency and accountability into library-specific procedures [12]. Library systems process forms of data that have distinctive ethical significance, including borrowing and information-seeking records. Without library-specific rules, these legal principles may remain abstract rather than operational. This finding complements Odong et al., who identify broader ICT compliance challenges in Ugandan university libraries [11], but adds an institution-level account of how those challenges appear in everyday library data practice. It also supports the wider argument that infrastructure and human-resource constraints shape information security in African academic-library environments [8].

The staff–user awareness asymmetry is the study’s second major contribution. Staff possessed practical confidentiality knowledge, but users largely relied on an assumption that the institution would protect them. The issue is therefore not simply whether safeguards exist, but whether data subjects can understand the conditions under which their information is processed. This matters for informed participation and trust. ALA (2025) emphasizes that privacy and confidentiality are essential to free inquiry and user confidence; the UICT findings provide a concrete example of this relationship, as some users reported hesitation about providing personal identifiers when data-handling practices were unclear. In a resource-constrained setting, transparency measures such as privacy notices and orientation may therefore be comparatively low-cost interventions with both governance and service benefits.

The novelty of the UICT case lies in bringing technical practice, institutional governance and user experience into the same qualitative analysis. Previous Ugandan studies have documented digital transformation, privacy concerns or ICT compliance at broader levels; this case shows how these issues intersect within one library and reveals a mismatch between the perspectives of those who handle data and those whose data are handled. The findings should not be generalized statistically to all Ugandan libraries. Instead, the case offers analytically transferable insights for comparable academic libraries where digitization is advancing faster than localized privacy governance, specialist capacity and user awareness.

6. Limitations and Future Research

This study is based on a single institutional case and a purposively selected group of 15 participants; its purpose is therefore analytical depth rather than statistical generalization. The findings reflect participants’ reported experiences and perceptions and do not constitute a technical security audit of UICT systems. The study also did not compare privacy practices

across institutions. These boundaries should be considered when transferring the findings to other settings. Future multi-site research could test whether the staff–user awareness asymmetry and the gap between general ICT policy and library-specific privacy governance recur across different types of Ugandan academic libraries.

Future research should explore the impact of emerging technologies such as artificial intelligence and blockchain on data privacy in African libraries. There is also a need for longitudinal studies to assess the effectiveness of privacy education programs on user behavior and institutional compliance. Comparative studies between public and private university libraries in Uganda could also provide insights into how different funding models affect information security investments.

7. Conclusion and Recommendations

This study concludes that effective data privacy in academic libraries depends on the alignment of technical safeguards, localized governance, staff capability and user understanding. At UICT Library, password-protected access, anti-virus software and restricted records provide a basic layer of security, but they do not resolve the absence of library-specific privacy rules or the limited visibility users have into how their data are processed. The study’s principal contribution is the identification of an institutional asymmetry: staff possess practical, largely informal confidentiality knowledge, while users tend to rely on an assumption of protection without understanding the data lifecycle or their privacy rights. By examining staff and users together, the UICT case demonstrates that privacy readiness is also a question of trust and information governance. For resource-constrained academic libraries undergoing digital transformation, strengthening privacy therefore requires not only better technology but also explicit policy localization, targeted staff development and transparent communication with users.

To enhance data privacy and information security at the UICT Library and similar institutions in the region, the following strategies are recommended:

- 1) Development of a library-specific data privacy policy: The UICT Library should formulate a dedicated policy that aligns with the Data Protection and Privacy Act (2019). This policy should specifically address library-unique risks, such as the monitoring of borrowing histories and third-party access to library management systems.
- 2) Targeted capacity building for staff: Regular training sessions on data protection principles and advanced security protocols should be provided to all library staff. Training should focus on ethical data handling, emerging cyber threats, and the practical application of privacy-by-design principles.
- 3) Implementation of user awareness programmes: To bridge the identified awareness gap, the library should conduct workshops, orientation sessions, and provide

clear privacy notices. Empowering users with knowledge of their rights is essential for fostering informed consent and maintaining institutional legitimacy.

- 4) Upgrade ICT infrastructure: The library should pursue phased upgrades to its ICT infrastructure. Priority should be given to adopting modern encryption standards, multi-factor authentication, and intrusion detection systems to safeguard sensitive digital records.
- 5) Establishment of incident response mechanisms: Clear procedures for detecting, reporting and mitigating data breaches should be established to ensure compliance with national legal obligations and to minimise reputational damage.
- 6) Strategic regulatory collaboration: The library should actively engage with bodies such as the National Information Technology Authority-Uganda to access technical guidance and support for sustainable data protection implementation.

Abbreviations

ALA	American Library Association
FGD	Focus Group Discussion
ICT	Information and Communication Technology
ILMS	Integrated Library Management System
NITA-U	National Information Technology Authority-Uganda
UICT	Uganda Institute of Information and Communications Technology

Author Contributions

Nalunkuma Elizabeth: Conceptualization, Formal Analysis, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing

Edward Ssali: Data curation, Investigation, Resources, Validation, Writing – review & editing

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] American Library Association. (2025). Privacy: An interpretation of the Library Bill of Rights. <https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>

- [2] Ayinde, L., Ebiefung, R., & Oladokun, B. D. (2026). Adoption of artificial intelligence in academic libraries: A systematic review of current practices, challenges, and research opportunities. *The Journal of Academic Librarianship*, 52(1), 103185. <https://doi.org/10.1016/j.acalib.2025.103185>
- [3] Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
- [4] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- [5] Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.
- [6] Dumbiri, R., Okeke, O. C., Ukubeyinje, E. S., & Nsirim, O. (2025). Technology-based security systems and security of information resources in the university library. *Southern African Journal of Security*, 3. <https://doi.org/10.25159/3005-4222/15883>
- [7] Esh, M. (2025). Deep learning for cybersecurity in libraries: Predictive analytics, collaboration patterns, and global research trends. *Journal of Electronic Resources Librarianship*, 37(3), 252–265. <https://doi.org/10.1080/1941126X.2025.2518893>
- [8] John, D. K. S., Mohammed, H. A., Diana, M., & Ajayi, E. O. (2025). Security of information resources in Federal College of Education libraries in Northwest Nigeria. *International Journal of Contemporary Security Studies*, 1(1), 85–98. https://doi.org/10.18485/fb_ijcss.2025.1.1.7
- [9] Kedi, P. N. (2022). User privacy and data protection practices in academic libraries: A case study of Makerere University Library [Master's thesis, Makerere University]. Makerere University Institutional Repository. <http://hdl.handle.net/10570/11089>
- [10] Nakaziba, S., & Ngulube, P. (2024). Harnessing digital power for relevance: Status of digital transformation in selected university libraries in Uganda. *Collection and Curation*. <https://doi.org/10.1108/CC-11-2023-0034>
- [11] Odong, P., Magara, E., & Nabutto, C. L. (2025). Compliance with Information and Communication Technology (ICT) standards in university libraries in Uganda. *East African Journal of Information Technology*, 8(1), 310–319. <https://doi.org/10.37284/eajit.8.1.3273>
- [12] Uganda. (2019). *Data Protection and Privacy Act, 2019* (Chapter 97). Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/act/2019/9/eng@2019-05-03>