ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

JOURNAL OF APPLIED LINGUISTICS AND TESOL

Vol.8. No.3.2025

# DATA PROTECTION AND PRIVACY IN UNIVERSITY LIBRARIES: ASSESSING THE KNOWLEDGE AND PREPAREDNESS OF UNIVERSITY CHIEF LIBRARIANS

***MUHAMMAD TARIQ LATIF***
*Sr. Librarian, Department of Libraries Govt. College University Faisalabad, Punjab, Pakistan*
***Email**: mtariqlatif@gcuf.edu.pk*
***Muhammad Asif***
*PhD Scholar, Department of Information Management, University of Sargodha, Sargodha, Punjab, Pakistan*
***Email** masif22143@gmail.com*
***Dr. SHAMSHAD AHMED***
*Professor, Department of Information Management, University of Sargodha, Sargodha, Punjab, Pakistan*
***Email** shamshad.ahmed@uos.edu.pk*
***SAKHAWAT ALI***
*(Corresponding Author)*
*Assistant Professor, Department of Information Management, Govt. College University, Faisalabad, Punjab, Pakistan*
***Email** sakhawatali@gcuf.edu.pk*

***Abstract***
***Purpose-*** *This research aimed to assess the existing knowledge and preparedness of university librarians in Pakistan regarding privacy and data protection issues.*
***Methodology-*** *Keeping in view the study's exploratory and explanatory goals, a sequential mixed methods approach was employed, combining both quantitative and qualitative methods. The study consisted of two phases, with final results derived from the integration of both data types. The questionnaire was used to collect data from University Chief Librarians (UCLs) of 105 universities of Punjab and Federal area of Pakistan.*
***Findings-*** *The findings revealed that all the participants have good level of awareness regarding privacy and data protection issues. However, a majority of participants lacked awareness of data protection laws, including the Data Protection Act 2018. The findings also illustrated that UCLs emphasized that they should educate the users regarding the importance of privacy and data protection issues, and also the consequences they may face in case of data leakage. The study found that majority of respondents emphasized the need for comprehensive training on data protection and privacy issues.*
***Limitations –*** *The population of the present study consists of only UCLs of universities, however due to the absence of these in some universities; data were collected from librarians and deputy librarians.*
***Practical Implications*** *– The study will help to understand the awareness level of UCLs about privacy and data protection issues and provide an opportunity for university authorities to arrange training programs for the UCLs to enhance their capabilities to deal the data protection issues.*
***Keywords –*** *University Chief librarians (UCLs), Data Protection, Awareness, Preparedness, Punjab (Pakistan).*
**Paper Type:** Research Paper

## 1 Introduction

The problem of user data protection and secrecy is central to the moral values, customs, and conventions of libraries (Fernandez, 2010). This is also the position of many other recognized bodies like the Federation of Library Associations and Institutions (IFLA) and the African Library and Information Associations and Institutions (AFLAI) by policies and declarations (Krueger, 2019). Even before the start of the digital era, libraries were very concerned about their users' privacy (Farkas, 2011). Libraries always try to protect the personal information of their users whether it is the revelation of borrower's personalities or short span preservation policies (Ponelis, 2013). Therefore, to protect the patron's personal data, it is important that library professionals have knowledge and awareness of relevant data protection issues and laws.

Safeguarding the privacy and confidentiality of library users has been a fundamental aspect of the library's mission for a long time. According to Caldwell-Stone (2012), information privacy for library users entails the freedom to access and explore any information without fear of judgment or retribution, a principle that applies equally to physical and digital libraries. According to Gorman (2000), privacy is one of the eight core values that are fundamental to librarianship, and

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT


it encompasses two key aspects: maintaining the confidentiality of library users' records and protecting library activities from technological intrusions that could compromise user privacy. Despite privacy being a fundamental principle of librarianship, the rapid technological advancements in the 21st century have created significant challenges for libraries to maintain the privacy of their patrons (McDonald,Greenstadt & Forte, 2023).

The importance of library privacy lies in preventing the "chilling effect", where users are aware of or suspect surveillance and amend their attitude accordingly. This effect threatens the ability of library patrons to explore sensitive, controversial, or personal topics without fear of judgment or repercussions, ultimately undermining the very purpose of libraries as safe spaces for knowledge exploration.

Libraries depend on external vendors' commercial products to deliver their services, a fact underscored by Barron and Preater (2018), who note that modern librarianship relies heavily on library systems. These technologies include integrated library systems, discovery services, and commercial products offering digital newspapers, magazines, and e-books. While libraries have contracts with vendors, they may not have direct agreements with all parties involved in the supply chain. For instance, users may access e-book content through third-party software like Adobe Digital Editions, with which the library may not have a formal contract in place.

Therefore, librarians must be proficient in fulfilling access needs as well as comprehending where security hazards exist. The secrecy and confidentiality of such records can be upheld through satisfactory awareness of present and future data protection actions, pertinent policies and measures, and decent training and development programs. Libraries and their parent organizations must be vibrant when advising users about how their information is being handled and obtain confirmatory permission to use the data for definitely intended purposes (Bailey, 2018b).

Privacy and data protection issues are policy matters and are under review by the university chief librarians (UCLs). It is the key for the UCLs to have a thorough knowledge of data protection and privacy laws so that libraries can secure the personal, circulation, and data relating to the use of the internet. Therefore, multiple studies (Affonso & Sant'Ana, 2018; Avuglah *et al.*, 2021; Corrado, 2019; Guo, 2021) are available that cover the privacy and data protection issues in libraries internationally. However, the situation in Pakistan is not encouraging, and meager (Khan, 2021) studies are available on users 'privacy issues in libraries. Consequently, the focus of the present study is to assess the knowledge and preparedness of university UCLs in terms of privacy and data protection issues.

## 2 Literature Review

The word "privacy" is diligently associated to the sanctuary of patron information. According to Bowers privacy means information about an individual that is unavailable to others (Bowers, 2006). Gorman (2001) defined privacy as the "basic values" of a library, therefore libraries must guarantee the privacy of their users. Gorman also throws light on the concepts of "spatial privacy" and "information privacy" Spatial privacy means the where and with whom you want to be, whereas information privacy is to safeguard your individual information, without being watched by outsiders. According to Mann *et al.* (2023), a privacy policy is a public statement that outlines an organization's practices and procedures for collecting, using, disclosing, and managing personally identifiable information and data related to individual activities. These written guidelines should be clear and understandable, empowering individuals to protect their online privacy by informing them how their personal data is handled.

*Goncalves,Correia and Cavique (2017)* define data protection as the act of securing personal data from unauthorized access, use, modification, recording, or destruction. Alternatively, data protection can be described as the process of preserving data integrity, preventing data loss or corruption, and ensuring data recoverability in the event of data unavailability or inaccessibility (SNIA, 2023). The primary objective of data protection is to maintain data integrity, availability, and compliance with legal and regulatory requirements, thereby enabling authorized individuals to access and utilize protected data for specific purposes.

According to the Data Protection Bill 2018, personal data refers to information that directly or indirectly relates to a person that can be identified from that information, or the information that is in possession of the data controller. The information that fall under the category of personal data include (MOITT, 2018):

- Information processed by means of machine / computers running automatically in answer to the command given for the specific purpose
- Information recorded for processing by means of computers / equipment
- Information recorded with purpose to form a part of the files

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT



In some countries, agencies are legally allowed to access the personal information of users in libraries and information centers. After the 9/11 terrorist attacks on the United States the " Patriot Act" was introduced in United States which provides legal rights to the governmental agencies to access the personal information of the users gathered by the libraries (Bowers, 2006). The data regarding a number of queries from government bodies is kept extremely confidential (Sutlieff & Chelin, 2010). This is a key problem, as Fox (2006) pointed out that we are now facing an extraordinary situation in which librarians are head to head with government agencies in a conflict over national security and users privacy. Though Neuhaus (2003) softened this risk and indicated that in the result of the attacks on September 11, 2001, restricted information showed that FBI primarily accessed e-mail records of the library patrons

However, in Pakistan so far no legislation is available regarding protection of the personal data of the library users; however, following laws are available regarding privacy and protection of the personal data of the individuals. The article 14(1) of the Constitution of Islamic Republic of Pakistan and the Prevention of Electronic Crimes act, 2016, guarantees the privacy of individuals (NA, 2023; PECA, 2016).

**2.1 Data protection/privacy and function of libraries**

During online searching from various databases library patrons use library systems, therefore there is always a possibility of transaction of personal information between libraries and library users. This transfer of information could be examined and kept by the librarians (Gorman, 2001).

Newby (2002) pointed out that during the circulation of books and other library material to library users, the personal information of the users can be accessed. Some pieces of user-related information may be very important for libraries like data on lent books by a user in a specified period; while some other information is not necessarily needed to run the library functions (e.g. Complete borrowing records of the library patrons). Gorman (2001) termed it "gathering of individual's information legitimate purposes" which can be abused. Also in the present era of automation, more private information of the users like patrons' names, website logs, addresses, and e-mail logs can be stored automatically by any library management system (Al-Suqri Waseem Afzal, 2007). Neuhaus (2003) also indicated that reference service through chat and e-mail communication can be observed on libraries or other servers providing internet services, which can cause serious privacy problems. Therefore, if more and more data about library patrons is stored, there is always a potential threat of misuse of information if the security system of the library is compromised.

Library professionals can adopt multiple measures to keep users' privacy secure that are not as drastic as going to jail or suing their governments. Macrina (2017) suggested five fairly simple ways to get started at your library. They are:

1. Teach solid password policies
2. Teach protected texting and calling
3. Upgrade software and eradicate Flash1
4. Offer online anonymity with the Tor Browser
5. Use HTTPS for all library digital services.

Threats to information security may lead to a trust deficit between the libraries and the library users. Traditionally, library users trust the libraries. Sturges,Teng and Iliffe (2003) conducted a study of library users and found that 89% of the respondents stated no concern regarding their privacy when using the library system. In libraries, confidentiality is crucial as it permits the user to select and search information without uncertainties, judgments, or penalties. The right to information can be affected if the personal privacy of the users is exposed, and a free environment in libraries needs both a diversity of materials and the guarantee that communication and selections are not being observed (ALA, 2017).

Libraries should take appropriate steps to safeguard the user's data to sustain their trust. Gorman (2001) indicated that this purpose can only be achieved by implementing an effective privacy plan. Different people suggested various recommendations for libraries regarding privacy plans. Newby (2002) offers a set of recommendations:

1. Prepare a complete list of data that can be gathered.
2. Prepare a list of risks of misuse for different types of data.
3. Form a policy for data collection and potential misuse.
4. Nominate an official responsible for certifying that privacy policies are implemented in letter and spirit, and for negotiation if needed.

**2.2 Role of librarians and personal data protection**

Sutlieff and Chelin (2010) raised a crucial question: Are librarians equipped to maintain the trust between users and libraries as they collect and utilize increasing amounts of personal digital data

to provide services? Their research revealed an inverse relationship between confidentiality and trust levels, suggesting that minimizing users' privacy concerns is essential to build trust. To achieve this, librarians, as information management experts, must take an active and accountable role in safeguarding information secrecy rights and adhering to relevant legislation, thereby upholding the trust relationship between users and librarians. OBrien *et al.* (2018) opinioned that librarians – as qualified information administrators – realize how to be ethical and obedient in dealing with personal data.

Librarians entertained requests for information that can result in the revelation of individual data of a very sensitive nature including religious beliefs, criminal proceedings, sexuality, personal interests, and political opinion. Therefore, librarians have to play a dual role, firstly, to act according to the legislation and secondly, a moral responsibility to keep the sensitive information of users confidential (Bailey, 2018b).

The professional activities of UCLs regarding confidentiality and data safety are affected by personal and professional opinions and experiences. They principally prove the value placed on discretion and confidentiality about a library patron's records and actions. Personal cognizance about confidentiality and data safety seems to imitate an understanding of lawful rights and data protection tasks regarding the use, collection, and management of private information of users. Awareness on an individual level proposes knowledge of professional duties and practices, particularly for those who have contributed to privacy and data protection related tasks. The results also showed that institutional data safety measures appear adequate in creating measures and policies but are not sufficiently communicated to library staff and patrons. Library professionals advocate privacy and data protection literacy as essential for professional growth and that libraries should arrange programs to educate the users (Cooper, 2016).

Sturges,Teng and Iliffe (2003) stated that libraries do not usually have their privacy plan. This looks conflicting to professional ethics to depend on the bigger organization for professional control. Coombs (2004) reported that supporters of privacy have the view that responsibility of user privacy protection belongs to organization, not users. This advocates the librarian's objective to certify that their service user's privacy rights are valued and helps to raise their confidence in the organization. Shuler (2004) agreed with this notion and disclosed that library professionals can play the role of instructors to raise understanding of individual and institutional privacy and data security tasks in a parallel way as other active library facilities.

Whitman (2003) indicated that education related to security, training programs, and a serious awareness campaign is the steps that can improve the capabilities of the librarians dealing with privacy issues. It is suggested that to ensure the privacy of the users in libraries, following steps must be taken: improving wakefulness; making operational policies and best practices affiliated with laws, morals, and maneuvers; instructing individuals and the organization on privacy concerns; and nonstop professional training and development (OBrien *et al.*, 2018; Sturges,Teng & Iliffe, 2003; Sutlieff & Chelin, 2010; Zimmer, 2014). After attending necessary training sessions, they can attain essential skills and understanding to successfully deal with personal information. It is also important to share the privacy plans to the outside world as a policy matter. These steps enable the users to know what type of information libraries collect and who can access the information.

## 3 Objectives and Research Questions

The main objective of the study is to determine the awareness and preparedness of UCLs regarding data protection issues and policies. To explore these phenomena, two subsequent research questions are raised.

1. What is the awareness level of UCLs regarding data protection issues?
2. What is the preparedness level of UCLs to face data protection challenges?

## 4 Research Design

The sequential explanatory design is a mixed methods research approach that leverages the strengths of both quantitative and qualitative methods to provide a deeper understanding of a research problem. Therefore, to accomplish the research objectives, the above approach was employed to gather authentic responses from the respondents. The study begins with a comprehensive survey to garner a broad perspective of the population, followed by in-depth, open-ended interviews in the second phase to collect detailed insights from the participants, thereby providing a more complete understanding of the research topic.

Initially, the study employed a survey research design to collect quantitative data (QUAN strand) with the objective of gathering insights from UCLs of HEC-recognized universities in the Punjab province and federal area regarding their awareness of data protection issues pertinent to libraries. Therefore, the study population consists of UCLs of 105 university libraries in the public and private sectors and due to small population size whole population was taken as sample. Survey

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT


method was deemed the most feasible approach to reach the target population so it was applied. A planned quantitative questionnaire was used as tool to assemble the data in QUAN strand of the research study. The questionnaire was developed by adopting and adapting the statements and ideas from previous articles (Cooper, 2016; Davies, 1997). Different variables regarding the study were merged in the first draft of instrument. Informal discussion was also made with legal experts and LIS professionals, and then it was forwarded for pretesting as it enhances the consistency, validity and reliability of the instrument. Ten university librarians pretest the instrument and made their recommendations which were incorporated. There after the survey tool was distributed to population via email. The collated quantitative data was analyzed through SPSS.

The findings from the first phase of the study (QUAN strand) guided the researcher in refining the conceptual framework and design of the second phase (QUAL strand). The first phase helped identify 23 key UCLs that were well-versed in data protection issues were recognized as the anticipated interviewees in the qualitative phase. They were approached through telephone and emails, and 20 of them agreed to be interviewed. The second phase (QUAL strand) was exploratory, explanatory, and confirmatory in nature, aiming to explore library leaders' awareness regarding data protection issues, their current status and preparedness in implementing policies and procedures, and gather expert opinions from top librarians on various study variables. This phase also sought to validate the findings from the self-completed survey form in the QUAN phase and provide a more comprehensive understanding of the research questions by integrating both quantitative and qualitative approaches.

On the basis of the findings of 1st phase QUAN strand, an interview-guide was prepared to conduct the semi- structured interview. The interview guide, instead of open-ended constructed questions, was focused to conduct interviews to elude construct biasness of the instrument as well as restate the question as per the consideration of the interviewee. The major sub themes of data protection include: importance, adoption of National/International law, data destruction policy, IT infrastructure, and orientation program. The collected data was interpreted through themes and sub themes.

## 5 Quantitative Results

### 5.1 Mean and standard deviation regarding awareness of data protection issues

The researchers requested the participants to gauge their awareness/knowledge regarding “data protection issues”. For this purpose, a five point Likert scale consisting of not at all (1), poor (2), adequate (3), good (4), and very good (5) was used. Table 1 demonstrates the mean scores about the judgments of the UCLs. The mean values present in the table confirmed that all the participants were ‘good’ regarding the successive four statements: “protection of patron’s personal data” (M = 3.83), “necessary IT skills for the protection of patrons’ data” (M = 3.80), “institutional policy regarding data protection” (M = 3.65), and “collection of patrons’ data lawfully” (M = 3.64). Conversely, the participants were ‘adequate’ about the subsequent three statements: “legal provisions regarding data protection” (M = 3.40), “legal issues regarding data protection” (M = 3.38), and “data protection act, 2018” (M = 2.96).

*Table 1*

*The mean and standard dev. regarding awareness of data protection issues (n = 85)*

| Sr. No | Statement | Mean | Std. Dev. |
|---|---|---|---|
| 1 | Protection of patrons personal data | 3.83 | 1.01 |
| 2 | Necessary IT skills for the protection of patrons data | 3.80 | 1.02 |
| 3 | Institutional policy regarding data protection | 3.65 | 1.04 |
| 4 | Collection of patrons ‘data lawfully | 3.64 | 1.08 |
| 5 | Legal provisions regarding data protection | 3.40 | 1.09 |
| 6 | Legal issues regarding data protection | 3.38 | 1.18 |
| 7 | Data Protection Act, 2018 | 2.96 | 1.13 |

### 5.2 Awareness of UCLs regarding data protection policy

The participants were requested to share their perceptions regarding data protection policy. The responses were gauged on the basis of Yes (1) and No (2). The findings (table 2) revealed that 52.9% respondents replied no while 47.1% yes regarding the statement: “Does your library has a formal policy on privacy”. In response to item: “Does your library have a formal policy on data protection”, 54.1% respondents said yes, and 45.9% said no. In the response to “Does your library have a formal policy on data retention/destruction”, most of the respondents (55.5%) replied no, and a minority (43.5%) replied yes. In the case of “Does your library have a formal policy on data breach”, the answers were 60% no and 40% yes. The responses of “Does your library have established practices/ procedures for dealing with requests for personal information about users?” most of the respondents (56.5%) replied yes and the minority (43.5%) replied no. In the case of

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT



"Does your library train staff on how to handle requests for personal information about users?" the answers were 72.9% yes and 27.1% no.

For the remaining five statements, the responses were as under: "Has your library changed any of its policies in the last 5 years regarding the management of user information in response to privacy and data protection concerns?" (Yes = 38.8%) and No = 61.2%), "Does your library communicate privacy and data protection policies to its users" (Yes = 58.8% and No = 41.2%), "Does your library have an official to deal with data protection issues?" (Yes = 43.5% and No = 56.5%), "In the past 5 years, have you participated in any information sessions, lectures, seminars, or other events related to privacy and data" (Yes = 40% and No = 60%), and "Does your institution offers Information literacy programs regarding data protection" (Yes = 37.6% and No = 62.4%).

*Table 2*

*Awareness of UCLs regarding data protection policy (n = 85)*

| Sr. No | Statement | Yes | No |
|---|---|---|---|
| 1 | Does your library has a formal policy on privacy | 40(47.1%) | 45(52.9%) |
| 2 | Does your library has a formal policy on data protection | 46(54.1%) | 39(45.9%) |
| 3 | Does your library has a formal policy on data retention/destruction | 37(43.5%) | 48(55.5%) |
| 4 | Does your library has a formal policy on data breach | 34(40%) | 51(60%) |
| 5 | Does your library has established practices/ procedures for dealing with requests for personal information about users? | 48(56.5%) | 37(43.5%) |
| 6 | Does your library train staff on how to handle requests for personal information about users? | 62(72.9%) | 23(27.1%) |
| 7 | Has your library changed any of its policies in the last 5 years regarding the management of user information in response to privacy and data protection concerns? | 33(38.8%) | 52(61.2%) |
| 8 | Does your library communicate privacy and data protection policies to its users | 50(58.8%) | 35(41.2%) |
| 9 | Does your library have an official to deal with data protection issues? | 37(43.5%) | 48(56.5%) |
| 10 | In the past 5 years, have you participated in any information sessions, lectures, seminars, or other events related to privacy and data | 34(40%) | 51(60%) |
| 11 | Does your institution offers Information literacy programs regarding data protection | 32(37.6%) | 53(62.4%) |

### 5.3 Mean and standard deviation of UCLs' preparedness regarding data protection issues

The responding UCLs were enquired to share the UCLs' preparedness regarding data protection issues. For this purpose, a five point Likert scale consisting of strongly disagree (1) to strongly agree (5) was used. The outcomes of the study shown in Table 3 exposed that the respondents were 'neutral' regarding the subsequent entire statements: "my institution encourages the library staff to attend training workshops on data protection" (M = 3.25), "my institution has provided adequate IT equipment to cope with the challenge of data protection" (M = 3.20), "my library staff has necessary skills to cope with the challenges of data protection" (M = 3.09), "my institution continuously arranges orientation programs for patrons on data protection" (M = 2.79), and "my institution frequently hosts training programs on data protection" (M = 2.70). Moreover, the respondents were 'disagree' with the statement that "my university has adopted data protection act 2018" having mean score 1.54 respectively.

*Table 3*

*The mean and standard dev. of UCLs' preparedness regarding data protection issues (n = 85)*

| Sr. No | Statement | Mean | Std. Dev. |
|---|---|---|---|
| 1 | My institution encourages the library staff to attend training workshops on data protection. | 3.25 | 1.28 |
| 2 | My institution has provided adequate IT equipment to cope with the challenge of data protection | 3.20 | 1.15 |
| 3 | My library staff has necessary skills to cope with the challenges of data protection | 3.09 | 1.17 |
| 5 | My institution continuously arranges orientation programs for patrons on data protection | 2.79 | 1.18 |
| 6 | My institution frequently hosts training programs on data protection | 2.70 | 1.2 |
| 7 | My university has adopted data protection act 2018 | 1.54 | .50 |

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT



## 6 Discussion regarding Quantitative Data

American Library Associations' (ALA) code of ethics (ALA, 2006) demand that Library professionals ensure the privacy of the library users' regarding content sought, copied, acquired, disseminated, and sources consulted. To perform his/her duties as per the code of ethics it is imperative that library professionals must have necessary knowledge of data protection/privacy issues and related laws.

In the current study when the subjects are invited to share their awareness and understanding regarding data protection issues. The findings reveal that all the participants have good level of awareness regarding data protection issues. However, they are adequately aware towards the data protection act 2018. These findings are in line with the results of Cooper (2016) who disclosed that good awareness level of data protection laws help in maintaining the trust, secrecy, and confidentiality of the users. Meanwhile, Whitman (2003) suggested that security related education, training programs, and an effective awareness campaign regarding privacy can enhance the capabilities of library staff to better address privacy issues in libraries. Conversely, contrary to these findings Sturges,Teng and Iliffe (2003) realized that librarians were not sufficiently aware how to collect data lawfully.

In order to protect the privacy of library users and their personal data, it is essential that library professionals have the essential skills to ensure privacy. For this purpose an institutional policy on privacy in any library is necessary. The present study shows that the research participants are well aware of the institutional policy regarding privacy and data protection of library users. However, the findings of Sturges,Teng and Iliffe (2003) are contradictory to these. They mentioned that only a few libraries have privacy policies and a gape exist in users' expectations and library practices and policies regarding privacy**.** Corrado (2019) also explored almost same findings and narrated that even the users were conscious regarding their privacy, majority of libraries fail to share their privacy policies on their sites. Results of the current study also indicates that majority of research participants have enough training to safeguard personal data and privacy of their users. These findings are in line with the outcomes of multiple studies according to which continuous professional training is key for ensuring the privacy of the library users (O'Brien *et al.*, 2018; Sutlieff & Chelin, 2010; Zimmer, 2014). The goal of privacy and data protection in libraries cannot be achieved unless library users are communicated about data protection policies. A user literacy program can play a pivotal role in creating awareness among library users regarding data protection policies.

University librarians have to face a variety of data protection issues in performing their duties. In order to provide the best library services to the readers, it is important that they are prepared to deal with these issues. This requires them to be familiar with the data protection issues relevant to libraries such as legal provisions to collect data, necessary IT skills, data protection policy and laws. The mean scores (M = 1.54 to 3.25) of the findings of the study regarding preparedness to deal with the data protection issues are not very encouraging. The encouragement of library staff to attend training workshops on data protection is a proactive measure to enhance their skills and knowledge in safeguarding sensitive information (Zaveri, 2015). Conversely, the outcomes of the study revealed that the institutions are neither arranging training workshops nor encouraging their patterns to attend training workshops. The staff has not the availability of IT equipment therefore; they have not the necessary skills to cope with the challenges of data protection. The study findings of Li (2019) agreed that the provision of adequate IT equipment to address the challenges of data protection is crucial. The worst thing is that majority of the institutions has not adopted data protection act 2018. The findings shows that the university librarians are not prepared to cope the challenges of data protection issues which is very alarming in this digital atmosphere. Therefore, the universities should keep this issue seriously and train their librarians for near future requirements.

The findings of the current work indicate that librarians are well aware about how to collect data lawfully, institutional policy about data protection, and use of IT skills to protect users' data. The respondents are adequately aware regarding data protection issues, and only a few respondents are aware about the data protection act 2018. It is also found that majority of the respondents have policies on data protection, established procedure to deal with the data requests, trained staff to entertain the requests of personal information about users, and have necessary arrangements to communicate users about the privacy and data protection policies.

## 7 Qualitative Results, Interpretation and Discussion

### 7.1 Importance of Knowledge/ Awareness of Data Protection Issues

Privacy has long been established as a fundamental operating principle for libraries, no library can attract its users without providing them a secured library system. When the interviewees were asked about the security of the user's data a majority of respondents (17 out of 20) perceived that

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT


security of the personal information of the library patrons is crucial, 15 opined that security of the circulation data of the patrons is important, 12 interviewees mentioned that use of the internet in the libraries be secured, and 10 considered that information regarding contents accessed by the users in the libraries needs to be secure (table 4).

*Table 4*

*Importance of Knowledge/ awareness of data protection regarding*

| Sr. No. | Contents analysis of responses | Frequency |
|---|---|---|
| 1 | Personal information | 17 |
| 2 | Information regarding circulation data | 15 |
| 3 | Information regarding use of internet | 12 |
| 4 | Information regarding contents used/accessed in the library. | 10 |

Introduction of information technology in the management of libraries has created certain threats in some aspects especially in terms of privacy and personal data protection which is generally regarded as confidential between the library and the individual. Libraries hold sensitive data of the users like, personal information, circulation data of the users, data regarding use of internet, data concerning to contents accessed by the patrons. It is fundamental responsibility of the library professionals to protect data in all aspects. On analyzing the qualitative data one of the respondent explained that user privacy is a fundamental duty of the librarian.

A librarian cannot secure sensitive personal data of students and the faculty members if he is not fully aware with data protection laws. In case of leakage of sensitive data of the library users the librarian may face legal consequences which can threaten his job, therefore a librarian must have knowledge of the data protection rules. Leakage of users' data is common problem in libraries which may cause social and financial problems for the users, one of the interviewee recognized that it is very important for a librarian to know about the data protection laws, how to launch a complaint in case of data leakage of, and how to handle the problem. Chen *et al.* (2019) also confirmed that Librarians are the custodians of users' personal data and may face legal action if users' personal data is leaked, so it is important for librarians to be familiar with data protection laws to avoid such issues.

Similarly, two participants added that it is pivotal for librarian to have knowledge of data protection laws, techniques to secure and handle users' data, as he is custodian of the personal data of the users. In this era of digital environment leakage of identity number and photographs may cause financial loss to the users. A recent study conducted by Kont (2024) also concluded that Librarians have a very key role as custodians of users' personal data.

A head librarian of private top ranked university stated that in this present era of information technology data protection is a big issue, leakage of data and its editing in the Photoshop can raise serious threats to the users. Being a professional librarian I must know the laws about data protection and the consequences in case of non-compliance. Four interviewees recognized the importance of awareness data protection laws for the library professionals to secure the privacy of the users. They added that with the introduction of information technology in the operations of library and online sources the issue of privacy of user's data has got more attention than ever. These views are similar to the Bailey (2018a) who found that Library professionals have a very crucial in safeguarding the user's personal data.

Two interview participants opined that personal data of all the students is very sensitive and must be secured. Any breach of personal data may cause moral, ethical and financial problems, therefore it is the fundamental responsibility of the librarians to take necessary measures to safeguard the personal data of the patrons, another respondent explained that personal data of the users is not public data, it should be secure, my library have multi-layer security system, and there is a very little chance of breach of personal data of the users. Mostly students use their laptops which minimize the data breach. Dresselhaus and Shrode (2012) also endorsed that the use of various types of mobile devices like laptops, android mobiles, and computers by patrons has led to data protection challenges.

A research participant from an engineering university shared that how we surrender our rights of our personal data to others and stated that when we use internet on mobiles, laptops and on personal computers, we accept cookies, actually we are giving rights to others to access our personal information, therefore there is a chance of leakage of personal information. Jones and Salo (2017) also confirm that acceptance of cookies while using the online sources means that actually we are permitting access to others to our personal data. The importance of data privacy has increased manifold in the present digital environment. An interviewee added that in the present digital environment it is fundamental for a librarian to have knowledge of data protection laws, but unfortunately it is not recognized at government level. Without recognizing the importance of data protection laws, personal data of the users cannot be secured.

ISSN E: 2709-8273
ISSN P:2709-8265
aa
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT


The analysis of the interview shows that it is consensus opinion of the participants that it is of key importance that library professionals must have knowledge how to secure personal data of the library patrons.

**7.2 Adoption of Laws by the Institution (National/International)**

When the interview participants were enquired to share their institutions' position regarding adoption of data protection laws, the situation was miserable as no university has formally adopted any National/International law, and even only (15 out 20) interviewees mentioned that their universities has institutional policies regarding privacy/data protection of the library users.

*Table 5*

*Adoption of laws by the institution (National/International)*

| Sr. No. | Contents analysis of responses | Frequency |
|---|---|---|
| 1 | National laws | 00 |
| 2 | International laws | 00 |
| 3 | Indigenous/institutional policies | 15 |

To implement the copyright laws in the libraries it is pivotal that library professionals must have adequate knowledge of copyright laws and the institutional policies about privacy/data protection of their respective universities. As universities are autonomous bodies and forms their rules and regulations through their authorities like academic council, Syndicate and Senate, therefore to implement the data protection laws it is essential that these laws be approved from respective authorities. Enquiring about the adoption of any national/international data protection laws majority of the interviewees admitted that their universities have not adopted any such law and 15 participants mentioned that they have indigenous policies regarding the privacy of the users' data. A respondent stated that his university is very sensitive towards the issues of data protection. A separate department for data protection has been established consisting of experts from various departments including the librarian. This newly established department continuously monitor the users' data and recommend various steps to make sure the privacy of the personal data of the users. Another interview participant indicated that his institution has defined protocols for the security of the personal data of the users. Our IT department monitors the digital activities in the library. Our policy regarding data protection and copyright is ISO certified.

**7.3 Availability of Data Destruction Policy About Patrons' Personal Data**

Data retention/removal policy always meant to ensure proper management of the record. Libraries are growing institutions and always face space problems. Destruction of record regarding personal data of the library users not only help to create more space but also ensure the privacy of the past personal data of the users. On enquiring about the availability of data destruction policies one of interviewee indicated that his library has a data destruction policy according to which after completion of degree the data is kept secured in the archives, where it is not accessible to anyone, but authorized official can access, when needed lawfully. Another interview participant shared his views and said there is no separate data destruction policy for library data, our university has a unified management system which is managed by Registrar office. Data destruction policy is the part of the unified management system. A head librarian of a private university stated that after completion of degree of the students their data is blocked, and can be accessed with the prior permission of the authority.

A respondent from a public sector university explained his institutions' position that previously we maintain our manual registers till the completion of the degree of the students. But after automation of the library we just use the data of the students for library operations, security of the data is the responsibility of IT department who administer the university's data management system.

On questioning about the data destruction policy an interviewee stated that at the completion of degree when security fee is refunded to the students their data becomes inactive in the software and then after one year it is deleted from the software. A research participant narrated that we are using KOHA since last ten years, personal data of the users is not deleted from the software but it is blocked after the completion of degree, and no one can access it. So far no policy has been devised for the destruction of data.

A head librarian emphasized on security of data rather than destruction of data, he reported that my library has no any data destruction policy, as my institution believes in security of data not the destruction data. We use the student's data for the weeding of the library collection. Students circulation data help the library to determine the how many times a book is issued to users in one years, and therefore from this data library collection is enriched. Space on the shelves is very crucial, a book without use on the shelf is just the misuse of the space. Therefore we cannot afford to delete the student's personal data after five or ten years. Our graduates remain the members of

our library even after the completion of their degrees. Two interviewees stated that their universities don't have any formal policies on data destruction but after the completion of degree it is practiced the data of the students is blocked and cannot be accessed by any one, but only for the authoritative use.

Qualitative data analysis also reveals that in libraries where library functions are still being performed manually, the records are discarded after completion of the students' degree, but those libraries which have been automated and all their functions have been transferred to computers where after the completion of the degree, the data of the students is blocked and deactivated and can be used only with the permission of the authority. One of the interviewee shared that my institution deletes online personal information of the students once they got clearance from the library. An interview participant mentioned that at present my library have not any policy dealing with the destruction of data, but we have prepared outlines regarding deletion of data of those students who have completed their degrees, and will be presented in the next meeting of Syndicate for approval.

A head librarian of a private sector university told that his university has integrated management system, which is maintained by their IT department. There is no data of the library users available with library in an organized form; we extract data whenever we want from the main data management system of university. A female head librarian acknowledged that data security is not in my preview, it is managed by our IT department.

**7.4 Orientation Session for Patrons**

On enquiring about the orientation session for the students on data protection awareness, a large number of the interviewee mentioned that they organize orientation session for the students on various issues concerning to library use but not specifically on the data protection while only four interviewees confirmed that their institution regularly arranges orientation session for their students that how to protect their personal data while using the library.

An interviewee stated that his university pay special attention on the user education, faculty members visits classes and educate students about how to use computes in a secured way, this practice continue throughout the year, another participant explained that institution arranges training sessions for uses on various themes including intellectual copyright, but not specifically on data protection.

Two research participants mentioned that their institutions arrange training sessions for users on various library functions. We have a regular orientation program for the fresh students about the use of the library, but specifically we have not arranged any session on data protection.

A head librarian from a private sector university shared his experience that their IT department educates users regarding network security. A smart card is issued to every student and all the transactions of books are made through this smart card. Students are asked not to hand over their smart cards to any other individual and in case of misuse of the smart card the students will be responsible. A study conducted by Baboo and Gokulraj (2010) on the use of the smart card and found that smart cards carry very sensitive information and if they are not used carefully, there is a risk of leaking very important information. Therefore, it is very important to provide the students with the necessary information about the use of smart cards to avoid its misuse.

Three participants were of the view that their institutions arrange orientation sessions for the students for the awareness of personal data security. Experts from the various departments especially from IT department are invited to deliver guest lecture on the security of data protection. One of the interviewee told that his university organized multiple programs on library automation, plagiarism and other functions of the library, but not on data protection. In future we shall arrange seminars/ workshop on the importance of the data protection for the awareness of the students and faculty. A female chief librarian of a public sector university shared that her university didn't receive any request like this, but I think it is very important subject and training session be organized for the users on data protection.

Two interviewees stated that their universities arrange regular sessions of training for students on various issues, experts from the university and from other universities are also invited to share their expertise. On request of ten or group of more than ten users, library arrange the training session. Another interviewee from an engineering university explained that his institution has not conducted any session specifically on data protection, but we conducted various seminars and workshops on plagiarism and copyright in which data protection issues were also discussed.

A head librarian of a private university confirmed that we frequently host training session for the students regarding awareness of data protection laws, we have a special department 'Institute of System Engineering for training and development', it organizes training sessions for students and staff. This institute is also responsible for web security issues. Dubois and Mouratidis (2010) also highlights the importance of the training programs on privacy and data protection laws. One of the

interview participant admitted that his library has no such program, but I think it must be the part of the curriculum to provide necessary information/knowledge to the students regarding data protection.

## 8 Conclusion

The findings of the present work disclosed that the knowledge and preparedness level of university UCLs in Pakistan regarding privacy and data protection matters was good. Though, a major portion of UCLs was not much aware regarding data protection laws, especially the Data Protection Act 2018. The results also disclosed that UCLs highlighted that they should coach the users concerning privacy and data protection issues as well as their consequences in case of data leakage. The results explored that most UCLs emphasized the need for comprehensive training on data protection and privacy issues.

It is the responsibility of library schools and library professional organizations to launch an effective awareness campaign through lectures, workshops, and seminars so that librarians can ensure the privacy of users. The university authorities should train not only the university librarians but also the librarians of their affiliated colleges on data protection and privacy issues. It is also recommended that university authorities should make laws like the Data Protection Act 2018 and Copyright Act etc. as a part of their policy by getting approval from their concerned bodies. In the future, research may be conducted to gauge the insights of users of school, college, and university libraries on what their private data is and how it can be protected.

## 9 References

Affonso, E. P., & Sant'Ana, R. C. G. (2018). Privacy awareness issues in user data collection by digital libraries. *IFLA journal, 44*(3), 170-182. doi: 10.1177/0340035218777275

Al-Suqri Waseem Afzal, M. N. (2007). Digital age: Challenges for libraries. *Information, society and justice journal, 1*(1), 43-48. doi: 10.3734/isj.2007.1105

ALA. (2006). ALA Code of Ethics. Retrieved January 11, 2024, from https://www.ala.org/tools/ethics

ALA. (2017). Privacy. Retrieved January 15, 2024, from http://www.ala.org/advocacy/privacy

Avuglah, B. K., Owusu-Ansah, C. M., Tachie-Donkor, G., & Yeboah, E. B. (2021). Privacy practices in academic libraries in Ghana: Insight into three top universities. *IFLA journal, 47*(2), 196-208. doi: 10.1177/0340035220966605

Baboo, S. S., & Gokulraj, K. (2010). A secure dynamic authentication scheme for smart card based networks. *International Journal of Computer Applications, 11*(8), 5-12.

Bailey, J. (2018a). Data Protection in UK Library and Information Services: Are We Ready for GDPR? *Legal Information Management, 18*(1), 28-34. doi: 10.1017/S1472669618000063

Bailey, J. (2018b). Data protection management in UK library and information services. *iConference 2018 Proceedings*, 1-4. https://orcid.org/0000-0002-0793-8873

Barron, S., & Preater, A. (2018). Critical systems librarianship.

Bowers, S. L. (2006). Privacy and library records. *The journal of academic librarianship, 32*(4), 377-383.

Caldwell-Stone, D. (2012). A digital dilemma: Ebooks and users' rights. *American Libraries*, 20-23.

Chen, Chen, S., Xiao, Y., Zhang, Y., Lin, Z., & Lai, T. H. (2019). *Sgxpectre: Stealing intel secrets from sgx enclaves via speculative execution.* Paper presented at the 2019 IEEE European Symposium on Security and Privacy (EuroS&P).

Coombs, K. A. (2004). Walking a tightrope: Academic libraries and privacy. *The Journal of academic librarianship, 30*(6), 493-498.

Cooper, A. (2016). *Safeguarding what's personal: privacy and data protection perspectives of Library Association of Ireland members.* (MSc), Dublin Business School, Dublin.

Corrado, E. M. (2019). Libraries and protecting patron privacy. *Technical Services Quarterly, 37*(1), 44-54. doi: 10.1080/07317131.2019.1691761

Davies, J. E. (1997). Data protection management in university libraries in the UK. *Journal of information science, 23*(1), 39-58. doi: 10.1177/016555159702300104

Dresselhaus, A., & Shrode, F. (2012). Mobile technologies & academics: do students use mobile technologies in their academic lives and are librarians ready to meet this challenge? *Information Technology and Libraries, 31*(2), 82-101.

Dubois, E., & Mouratidis, H. (2010). Guest editorial: security requirements engineering: past, present and future. *Requirements Engineering, 15*(1), 1-5. doi: 10.1007/s00766-009-0094-8

Farkas, M. G. (2011). Technology in Practice. Too Much Information? *American Libraries, 42*(5-6).

Fernandez, P. (2010). Privacy and Generation Y: Applying library values to social networking sites. *Community & Junior College Libraries, 16*(2), 100-113. doi: 10.1080/02763911003689495.

Fox, R. (2006). Digital libraries: the systems analysis perspective. *OCLC Systems & Services: International digital library perspectives, 28*(4), 170-175. doi: 10.1108/10650751211279102

Goncalves, A., Correia, A., & Cavique, L. (2017). *Data protection risk modeling into business process analysis.* Paper presented at the International Conference on Computational Science and Its Applications.

Gorman, M. (2000). *Our enduring values: Librarianship in the 21st century*: American Library Association.

Gorman, M. (2001). Privacy in the Digital Environment--Issues for Libraries.

Guo, W. (2021). *Discuss the Security Countermeasures and Data Protection of Library Computer Network.* Paper presented at the Journal of Physics: Conference Series.

Jones, K., & Salo, D. (2017). Learning analytics and the academic library: Professional ethics commitments at a crossroads. *College & Research Libraries, Forthcoming*. doi: 10.5860/crl.79.3.304

Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights. *International Journal of Information Management Data Insights, 1*(2), 1-8. doi: 10.1016/j.jjimei.2021.100015

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. doi: 10.1108/LHTN-03-2023-0036

Krueger, S. (2019). Academic librarians in Canada concerned about online and patron privacy but lack knowledge about institutional procedures and policies. *Library and Information Science Research, 40*(2), 86-97. doi: 10.18438/eblip29555

Macrina. (2017). Protecting Patron Privacy. Retrieved February 15, 2024 https://www.libraryjournal.com/story/protecting-patron-privacy

Mann, E. Z., Jacobs, S. A., Kinsley, K. M., & Spears, L. I. (2023). Tracking transparency: an exploratory review of Florida academic library privacy policies. *Information and Learning Sciences, 124*(9/10), 285-305. doi: 10.1108/ILS-04-2023-0038

McDonald, N., Greenstadt, R., & Forte, A. (2023). Intersectional thinking about PETs: A study of library privacy. *Proceedings on Privacy Enhancing Technologies*.

MOITT. (2018). Personal data protection bill 2018. Retrieved November 11, 2023

NA. (2023). THE CONSTITUTION OF THE ISLAMIC REPUBLIC OF PAKISTAN. Retrieved February, 2024, 2024, from https://na.gov.pk/uploads/documents/1333523681_951.pdf

Neuhaus, P. (2003). Privacy and confidentiality in digital reference. *Reference & User Services Quarterly, 43*(1), 26-36.

Newby, G. B. (2002). Information security for libraries *Modern Organizations in Virtual Communities* (pp. 134-144). North Carolina: IGI Global.

O'Brien, P., W.H. Young, S., Arlitsch, K., & Benedict, K. (2018). Protecting privacy on the web. *Online Information Review, 42*(6), 734-751. doi: 10.1108/OIR-02-2018-0056

OBrien, P., Young, S. W., Arlitsch, K., & Benedict, K. (2018). Protecting privacy on the web: A study of HTTPS and Google Analytics. *42*(6), 734-751. doi: 10.1108/OIR-02-2018-0056

PECA. (2016). Offences and punishments: Unauthorized access to information system or data. Retrieved March 15, 2024, from https://wpc.org.pk/wp-content/uploads/2020/02/Prevention-of-Electronic-Crime-Act-2016.pdf

Ponelis, S. (2013). Ethical risks of social media use by academic libraries. *Innovation: journal of appropriate librarianship and information work in Southern Africa, 2013*(47), 231-244. doi: 10.10520/EJC158314

Shuler, J. A. (2004). Privacy and academic libraries: Widening the frame of discussion. *The Journal of Academic Librarianship, 2*(30), 157-159.

SNIA. (2023). What is data protection. Retrieved December 11, 2024, from https://www.snia.org/education/what-is-data-protection

Sturges, P., Teng, V., & Iliffe, U. (2003). User privacy in the digital library environment: a matter of concern for information professionals. *Library Management, 22*(8/9), 364-370. doi: 10.1108/01435120110406309

Sutlieff, L., & Chelin, J. (2010). 'An absolute prerequisite': The importance of user privacy and trust in maintaining academic freedom at the library. *Journal of Librarianship and Information Science, 42*(3), 163-177. doi: 10.1177/0961000610368916

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91-95. doi: 10.1145/859670.859675

Zimmer, M. (2014). Librarians' attitudes regarding information and internet privacy. *The Library Quarterly, 84*(2), 123-151.