OVERCOMING FUNDING CHALLENGES IN NIGERIAN ACADEMIC LIBRARIES THROUGH 'BRING-YOUR-OWN-DEVICES' (BYOD) POLICIES

By

JULIET ONUOHA (PHD, CLN)
AND
CHUKWUEMEKA CHUKWUEKE (CLN)

Abstract

Navigating through budget deficit and problems of poor funding, have remained a major concern of academic libraries in Nigeria. On the other hand, the constant rise in the cost of acquiring ICT facilities has left these academic libraries with no other choice than to devise certain policies and strategies. Aside from the usual promotion of marketing of library and information resources and services, this paper assumes the adoption of the Bring-Your-Own-Device (BYOD) policy as a remedy to the frequent funding issues faced by academic libraries, especially, in Nigeria. In doing this, an attempt was made to reveal the BYOD concept, and the issues surrounding its adoption in Nigerian academic libraries. It also looked at the historical origin of the policy, issues surrounding the adoption of the policy, and its perceived impacts on Nigerian academic libraries. The paper concludes that the BYOD policy provides substantial benefits to academic libraries such as cost savings, flexibility, enhanced productivity and efficiency on the side of the librarians, and user satisfaction. Given the risks associated with such a policy, the paper strongly recommended the need for security strategy development and implementation alongside providing library staff and users with security, education, training and awareness.

Keywords: BYOD**,** Libraries, Policy, Technology, Devices, Library Staff, Library User

Introduction

Bring Your Own Device (BYOD) also called Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP), and Bring Your Own Personal Computer (BYOPC) is an Information Technology (IT) policy where library staff and users are allowed or encouraged to use their mobile devices and notebook PCs to access the library's data, systems, and databases. This policy is seen as a phenomenon whereby the librarians and library users bring their own computing devices to the library with them and use them in addition to or instead of library-supplied devices. According to Akande and Tran (2022), the most frequently used

personally owned devices under BYOD are mobile phones, tablets, iPads and laptops. The authors went further to submit that the practice of encouraging personally owned computing devices within professional organizations that deal with information and communication technologies, such as academic libraries, is becoming more and more acceptable, as it enables the organisation or institution to transfer the investment costs of desktop hardware into their employees and users. In this case, the academic library parent institution transfers the investment cost to the library staff and users. Additionally, preliminary observation has shown the constant decline in financing academic libraries in Nigeria coupled with the fact that most academic library staff and users in Nigeria take their personal IT devices to the library to either perform their functions or meet their information needs instead of waiting for the management and authority to provide one, which invariably, may take ages. Consequently, Adetayo (2021) believes that to increase library productivity and meet the growing technology expectations of users, many academic libraries are allowing and encouraging BYOD policies in their institutions.

Aside budget deficit ravaging Nigerian academic libraries, it is important to understand that the trend of BYOD in academic libraries, is driven by the presence of technology-savvy younger library staff and users recruited and making use of the library, respectively, popularly referred to as the GenZ or netizens. There is, therefore, the need, to meet their expectations in terms of a good working environment, regardless of the availability of funds. Based on this, BYOD has become commonplace in academic libraries, as the library alone, cannot satisfy the desire of this technology-driven generation. Adetayo (2021) submits that academic libraries, with a staff strength that runs into hundreds, and a user community that runs into thousands, cannot effectively procure and maintain devices for all. Hence, a great emphasis on BYOD policy. On the other hand, Sokolova et al. (2021) opined that while

International Journal of Information Resource Management (IJIRM)
Volume 2, Number 1 (2025)
E- ISSN: 1118-7786

celebrating the BYOD trend, it is important to note that it has not only introduced many security issues and challenges to organizations and institutions but also raised concerns about non-security issues. Similarly, Babalola (2020) noted that while some see BYOD as the answer to the migration from analogue to virtual learning commons, some leverage the dangers inherent in such a policy. Thereby, limiting the adoption of this policy in several struggling academic libraries.

However, reports have shown that institutions like Wayne State Library (Michigan), Kenneth Dike Library (University of Ibadan), Danbaba Danfulani Suntai Library (Taraba State University, Jalingo), Michael Okpara University of Agriculture, Umudike Library, among other academic libraries, are increasingly using BYOD policy because of its perceived benefits without considering the risks associated with it and compromising their networks and data protection and security. In the same vein, many librarians and institutions management are not fully aware of the benefits and risks associated with BYOD, hence the absence of precautionary measures. All these in the submission of Mohsin and Ab Hamid (2022) result in libraries not getting full benefits from BYOD and often face losses and damages due to ineffective use and application of BYOD policy.

Nonetheless, Nigerian academic libraries are faced with difficult economic times and budget cuts. However, when these libraries are devoid of adequate fund, it becomes difficult to provide effective services to the library users, and invariably to the parent body, as inadequate funding affects all its activities, as it will culminate in inadequate staff, resources, equipment, furniture, and ICT infrastructure, among others. It is on this background that this paper proposes the adoption of the BYOD policy as a means of overcoming the funding challenges prevalent among academic libraries in Nigeria.

Conceptual Clarification and Historical Overview

Bring-your-own-device is a system where employees are allowed to use their mobile devices anywhere to access privileged organization or institutional data. According to Adetayo (2021), BYOD in libraries assumes a service mobility that enables the library staff to perform their work in certain specific information delivery scenarios using their mobile devices such as laptops, tablets and Smartphones. Its benefit is that it enables such staff to leverage technologies to access the data required for work remotely, as well as allows library users to connect to the library's database with their devices in their comfort zones (Babalola, 2020). In their earlier submission, Barlettee et al. (2021) note that BYOD creates many opportunities for organizations, such as academic libraries, which are libraries located in higher institutions of learning, to improve the delivery of user services securely, improve service productivity and efficiency while providing staff with enhanced flexibility to perform their work irrespective of space and time. This is because, the sole function of the academic library according to Saibakumo et al. (2019), is information generation, organization, dissemination, preservation, and conservation. To this end, Meates (2020) notes that digital technologies and cell phones are commonly and widely used in such information generation and dissemination businesses.

On the origin of BOYD, Rosman et al. (2022) wrote that BYOD itself has its origin in the world of work as 'the policy of permitting employees to bring personally-owned mobile devices (laptops, tablets, and smartphones) to their workplace. Adetayo (2021) observed that the name and the concept have been adopted widely in librarianship and have given rise to both practice advice and research into the implications for effective service delivery. According to Shukry et al. (2023), the term was initially used by a Voice over Internet Protocol (VoIP) service provider, BroadVoice in the year, 2004. This concept as of 2004 was

initially for AstriCon, but then continued as a core part of the business model, with a service allowing businesses to bring their device for a more open service provider model. Baillette et al. (2018) believe that the phrase and the "BYOD" acronym is a take-off on "BYOB", which is a party invitation term first recorded in the 1970s, standing for "bring your own beer/booze/bottle".

Additionally, the term BYOD entered common use in 2009, courtesy of Intel when it recognized an increasing tendency among its employees to bring their own smartphones, tablets and laptop computers to work and connect them to the corporate network (Rosman et al., 2022). However, the concept and policy were not popular, until early 2011 before the term achieved prominence, when IT services provider Unisys and software vendor Citrix Systems started to share their perceptions of this emergent trend (Barlette et al., 2021). From then, Mohsin and Hamid (2022) submitted that BYOD was then characterized as a feature of the "consumer enterprise" in which enterprises blend with consumers. Finally, in 2012, the U.S. Equal Employment Opportunity Commission adopted a BYOD policy, but many employees continued to use their government-issued BlackBerrys because of concerns about billing, and the lack of alternative devices (Doargajudhur & Dell, 2020). Today, BYOD has spread to every part of the world, including several organizations and institutions, as an end to a means.

BOYD Policy Framework: A Sample

While BYOD is an innovation or initiative aimed at facilitating effectiveness and efficiency, it must be guided by a policy framework. Consequently, a policy is defined as a course of action or guidelines for achieving goals and objectives. Policies can take many forms, including written regulations or guidelines, procedures, standards to be achieved, and

general statements about priorities. However, in the case of BYOD, the policy is expected to be written with the mindset of translating the vision of the academic library into programs and activities to create a solution to the funding challenges of such a library. Such a policy is simply a roadmap or guide to BYOD operations. Furthermore, a BYOD policy is designed to balance the convenience of permitting personally-owned devices, including mobile devices, in the library against risks related to the security of confidential, personal and proprietary information. It outlines permissible and impermissible uses of such devices and cautions against any expectation of privacy while these devices are connected to the library's network and databases. Nextrio (2019) was used to design the framework for BYOD policy in the Nigerian academic library.

Policy Brief & Purpose:	Our BYOD (bring your own device) policy helps library staff and users to understand how to effectively manage personal devices (such as mobile phones, tablets, cameras, wearables, etc.) brought to the office or library whether for personal or business use.
Scope:	Our BYOD policy applies to all our staff, users, visitors, and researchers who bring Internet/network-capable devices to the library building. In addition, as staff, we are responsible for our family members, visitors and guests when we allow them to bring devices to the office. This policy addresses devices that access our company network and devices that use public networks (WiFi and cellular networks) to access the library's data and databases. Library staff and users' expectations are applicable regardless of asset location or control.
Expectations of Privacy on Personal Devices	Library staff and users choosing to use their devices to access the library's resources inherently forfeit a right to privacy on such devices. The staff agree that the library may take possession of such devices for library-related business purposes (such as a forensic investigation of a possible security breach). Furthermore, any information stored on the device, including contacts and email messages, is subject to access, retrieval and removal by the library's authorized IT staff member at any time. Notwithstanding the above waiver of privacy rights, the library will make reasonable efforts to provide advanced notice of when the device will be required and avoid access or review of personal, non-library content. The staff must realize that some incidental review of personal information is likely and there may be a risk of that personal information being lost or destroyed through the course of managing the device.

	The library staff and user agree to provide the library with access to the personal device from time to time, with or without notice, as needed at the sole discretion of the library, to perform certain security-related actions.
The Role of the Library	The Library may: • Install mobile device management software (MDM) or remote management and monitoring software (RMM) (including anti-virus/anti-malware programs where applicable) on library staff and users' devices. This software will allow authorized IT staff to access, manage, monitor and remotely delete all library-related information, including calendars, e-mails and other applications. This is particularly important when a device is lost, stolen or decommissioned from service. • Verify the device is appropriately configured to meet security standards and where necessary, reconfigure settings to meet the library security requirements. • Verify that all software/hardware updates and patches have been successfully applied. • Scan the device for unauthorized or high-risk applications, and remove them. • Verify that the library *Access Control* policy standards are being met. • Monitor the device and any library resources it connects to, at its sole discretion.
The Role of Library Staff and Users	The Library Staff and Users Must: • Monitor patches and updates for software/hardware as they become available and ensure they are downloaded/installed in a timely fashion. • Use a hardened password and automatic screensaver as per the *Access Control* policy guidelines. • Work with IT staff to ensure adequate and appropriate encryption technology is in effect on the devices and all traffic to/from the device. • Adhere carefully to the *Digital Communications* policy and use extreme caution when opening emails and/or attachments on the device. • Refrain from video or audio recording capability anywhere in the building or on library property at any time unless authorized in advance by the Librarian. • Turn off or set to silent or vibrate mode any alerting device during meetings and conferences and in other locations where incoming calls and alerts may disrupt normal workflow. • Maintain the device in its original state by not modifying its operating system or "jailbreaking" the device to bypass built-in security features and protocols. • Do not download applications or software from unauthorized sources. • Not intentionally or unintentionally download or transfer sensitive library data to the device. • Report any lost or stolen device, or unauthorized access, to the Librarian as soon as discovered.

	• Fully comply with our library's *Acceptable Technology Usage*, *Mobile Device Security* and *Access Control* policies.
Revision History:	Version: Issue Date: Issued By:

Perceived Benefits of BYOD Policy to Academic Libraries

Many authors and researchers have consistently reported the importance of BYOD policies in organizations, institutions, and the library. According to Rosman et al. (2022), the BYOD policy has proved to be one of the most successful and relevant technologies to be used in libraries facing economic hardship and budget dwindling. Additionally, the research that was conducted by Liyson (2021) found that BYOD had given positive influence on learning and academic achievements as well as stimulating and motivating the library staff. This has a positive effect on the levels of staff performance and productivity, as well as user satisfaction. In a previous study conducted by Safar (2018), it was found that BYOD had a positive impact on staff in the areas of improved job performance and satisfaction with their job. On the other hand, Adetayo (2021) reported that most of the library management is willing to introduce BYOD, as most of them are already having laptops, tablets and smartphones. This is because of the belief that BYOD increases libraries and staff productivity as it reduces the time to accomplish tasks, increases staff efficiency as they can access the institution's information, irrespective of space and time, increases the satisfaction level of staff and helps them in retaining talented staff, because they are more comfortable with their own devices, and feel empowered when they are allowed to choose their device.

However, the perceived benefits of the BYOD policy can be summarized under the listed points.

1. Productivity: The BYOD trend has stemmed from the perception that it can lead to higher productivity and improve the agility of work practices in the library among its workforce and users. This policy increases library service and staff productivity because librarians using their devices become experts using it and it makes them more comfortable. This assertion is further supported by a survey conducted by Cisco, which found that an employee saves about 37 minutes on average per week by using his device at work in the US, compared to using the organization's device (Cisco, 2013; Baillette et al., 2018).

2. Staff satisfaction: Library staff and users bringing their own devices, which they selected by themselves rather than by the IT department, gives them more satisfaction and helps them avoid carrying different devices to work. This is to say that the library staff and users can choose the technologies in the BYOD policy that suits their roles and needs, the best (Akande & Tran, 2022). Through this, they develop new ways of working and solving their information needs, respectively.

3. Cost savings*:* BYOD shifts the cost of the devices to the user as the library staff and users pay for the mobile devices. Its upgrade, repair and maintenance costs are all born by them. It is for this reason that organizations and establishments are motivated to adopt BYOD policy and move into a BYOD environment (Sokolova, et al., 2021). BYOD results in strong cost savings as the library's expenditure in hardware investment declines considerably with the implementation of the BYOD policy. Costs of lifecycle management, replacement and running of the hardware are no longer to be borne by the library which also contributes to cost savings. Corroborating this assertion, HDI research corner conducted research with 844 organizations in 35 industries and found that over 40% of them stated that employees contact

International Journal of Information Resource Management (IJIRM)
Volume 2, Number 1 (2025)
E- ISSN: 1118-7786

the vendor directly for support for their device while 35% of them operated internal support system for BYOD (Pillay et al, 2013). Cisco (2013) submitted that organizations will gain about $350 in value annually, and if comprehensive BYOD is used then it increases to about $1650.

Overall, the BYOD policy will help the library improve employee job satisfaction, facilitate flexibility and increase job efficiency. It also results in cost savings, which is necessary in overcoming the funding challenge of the library. This is because the little funds available can be deployed to other areas of the academic library operations and services.

Risks and Issues Associated with BYOD Policy

While looking at the benefits, it is also important to consider some risk factors and issues associated with the BYOD policy. According to Cho and Ip (2018), the BYOD policy gives rise to data protection and information security issues. In addition to that, Hakami (2020) reported that the issue of ownership, cropping up as to who owns the device and the data on it. This is because, if library staff get their device, it makes them the owner and the library cannot access the device. Whereas if the institution supplies, they own it, however being in the possession of the library staff or user implies that he can use it for personal purposes too. Apart from that, other issues are listed below:

1. Designing of BYOD policy: Designing the BYOD policy is also an issue as the BYOD policy of the library has to be clear, such that the library staff and users understand their responsibilities clearly. It is expected that the BYOD policy should not introduce vulnerability to the secure environments and data security should be the prime concern of the academic library (Hakami, 2020).

2. Loss of Data: This is the most important risk faced with the implementation of BYOD. Smartphones or tablets' value and size make it easy to get dropped, misplaced or stolen. Moreover, when the library staff upgrades or exchanges their device to a new one, sensitive and confidential information gets passed on to unauthorized users. Additionally, data leakage is also a major challenge that academic libraries have to cope with BYOD and detecting data leakage before it's too late is the main difficulty as staff using the device often do not understand the technology to know how the data is getting leaked (Safar, 2018).

3. Lack of library control over devices and data: In a BYOD environment, the library control over misuse and abuse of IT resources of the library decreases and most often the staff bypass the restrictions with regards to security imposed by the library intentionally for their convenience, thereby compromising the IT resources' security (Baillette et al., 2018). It is also difficult to audit who is using the device whether the authorized employee or someone else.

4. Increase of vulnerabilities due to malicious software installation: In 2012 more than 5000 malicious Android apps were found and were downloaded 700,000 times before they were detected and removed by Google. The report further shows that individuals have also downloaded these apps for personal use making the device vulnerable and increasing the risk of virus attacks (Shukry et al., 2023). Security is not the priority of the mobile device OS hence the devices are more prone to external threats (Shukry et al., 2023) and bring these threats to the network of the library, which can easily spread to the entire network of the company within a short time.

***5. Non-Security Issues*:** Mohsin and Ab Hamid (2022) have also given other non-security issues that crop up with the use of BYOD policy, such as long-range vendor plans as personal devices are meant for personal use and may not be best suited well to the needs of enterprise

technology integration and planning. The other issues are lost devices, demarcation between personal and professional use of devices and other technologies, procurement and maintenance of devices, deployment of applications, patches and updates, ruggedized devices, corporate end-user device policy and garnering support of top management for the BYOD policy.

These risks and issues, if not tackled, decrease the effectiveness of the BYOD policy in Nigerian academic libraries. However, most organizations and institutions do not consider these risks or issues while implementing the BYOD policy and as a result, suffer greatly and have to grapple with security issues. But if the academic library does not provide the newest technology to staff, which is necessary to do their job efficiently then the library staff do not hesitate to bring their device and use it if they think they need it. If they are not allowed to do so, then the library has to bear the risk of losing talented staff or a decrease in overall productivity and efficiency.

Existing Solutions

In addressing the issue of loss and security of data, Shukry et al. (2023) stated that the IT department of the institution or organization can use tools such as *Tools4ever* user management resource administrator. Such will allow the academic library to add devices to the network easily and monitor them. However, to minimize risks, Othman et al. (2021) submit that only certain devices must be allowed to be registered after evaluating the risks associated with them and also, they must ensure security at all costs. Furthermore, the Data Protection Act (DPA) suggested that the data controller should ensure that all personal data processing under their control must be in compliance with the Data Privacy Act and remain mindful of the personal usage of devices (Rosman et al., 2022). Regrettably, the DPA act

International Journal of Information Resource Management (IJIRM)
Volume 2, Number 1 (2025)
E- ISSN: 1118-7786

only protects data of the United States and such an act has not been passed in Nigeria, which makes data monitoring more challenging in Nigerian academic libraries.

Nevertheless, Sokolova et al. (2021) suggest that it is essential to control BYOD risks to derive substantial benefits from BYOD. First, the library has to identify risks associated with BYOD and then apply appropriate countermeasures to mitigate, control and prevent these risks from happening. The countermeasures suggested by Sokolova et al. (2021) are implementing security policies, fostering security culture, security strategy development and implementation and security control along with providing library staff with security, education, training and awareness (SETA). Livson et al. (2021) observe devices of staff need to be secured by evaluating the usage scenarios of the device, investing in the solution of mobile device management (MDM), enforcing standard security policies of the library as the minimum, setting a security baseline, differentiating between untrusted and trusted devise access, introducing more stringent access and authentication controls and adding mobile device risk to the awareness program of the library.

Furthermore, Akande and Tran (2022) write that mobile app risks can be countered by using anti-virus programs on mobile devices, ensuring that security processes are covered in the development of mobile apps, managing apps through the in-house app store, introducing services that enable sharing of data between BYOD devices and continually assessing the new apps' need. To enhance the security of mobile devices, Akande and Tran (2022) suggest that libraries must manage support of BYOD Devices by creating and implementing appropriate BYOD usage and support policies, revamping current support processes, creating a patch education process and introducing mechanisms of social support and implementing knowledge base that enables staff to develop as self-service support solution. In addition, the institution must also handle regulatory risk by consulting with its legal departments, and

address governance and compliance issues (Shukry et al., 2023). Notwithstanding, the most cost-effective way to ensure a secure BYOD environment is to educate and train library authority/management, the staff and users, about the risks and problems associated with BYOD and make them aware of the benefits of using BYOD securely. This will help in garnering support from and involving library staff and users in ensuring the BYOD environment is secured and used appropriately.

Conclusion

The trend of BYOD is here to stay and risks will not hinder its utility value if truly Nigerian academic libraries want to overcome their funding challenge. Therefore, there is a need to find a solution which increases the effectiveness of the BYOD policy while reducing the risk associated with it and addressing Nigerian academic libraries' concerns in introducing BYOD. Among the benefits of the BYOD policy is the fact that it can help the academic library in decreasing hardware acquisition costs, device support and maintenance costs as they are mostly born by staff and users themselves. However, there is concern as to who owns the data and devices, as well as the issue of monitoring, and harm to personal data. It is clear that to reduce, manage and mitigate the risks and problems associated with BYOD, adequate measures must be taken and agreed by all parties involved.

Recommendations

Because of the concerns exhibited by so many with regards to the issue of BYOD policy, the following measures were recommended:

1. The academic library authority and management should identify and analyse all risks and problems associated with BYOD policy and use, before adopting it.

2. There is a need to persuade top management staff about the benefits of BYOD and its risks and how they can be addressed effectively to garner their support and involvement in introducing BYOD. Such may include, seeking management support.
3. The BYOD policy should be designed in such a way that it fosters a security culture and also includes the provision of education and training that will increase library staff and users' awareness about security issues and to use of BYOD.
4. Four layers of security should be adopted including securing remote access, encryption, data loss protection and firewall.
5. There is a need to ensure that all library staff and users bringing their mobile devices to work have installed anti-virus programs.
6. There is a need to provide library staff and users with security, education, training and awareness (SETA)

References

Adetayo, A. J. (2021). Leveraging Bring Your Own Device for Mobility of Library Reference Services: The Nigerian Perspective. *The Reference Librarian*, *62*(2), 106–125. https://doi.org/10.1080/02763877.2021.1936342

Adetayo, A. J. (2021). The nexus of social media use and research productivity of lecturers in private universities in Ogun State, Nigeria. *Library Philosophy and Practice (E-journal)*, *4964*, 1-14. https://digitalcommons.unl.edu/libphilprac/4964

Akande, A. O. & Tran, V. N. (2022). A theoretical foundation for explaining and predicting the effectiveness of a bring-your-own-device program in organizations. *SN Computer Science*, 3 (5), 1-16. https://doi.org/10.1007/s42979-022-01272-0

Babalola, N. A. (2020). From library to virtual library learning commons: Alternative to school library media in Nigeria. *Canadian School Libraries Journal*, 4(2). https://journal.canadianschoollibraries.ca/from-library-to-virtual-library-learning-commons-alternative-to-school-library-media-in-nigeria/

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, 43, 76–84. https://doi.org/10.1016/j.ijinfomgt.2018.07.007

International Journal of Information Resource Management (IJIRM)
Volume 2, Number 1 (2025)
E- ISSN: 1118-7786

Barlette, Y., Jaouen, A. & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies," *International Journal of Information Management*, 56, 1-16. https://doi.org/10.1016/j.ijinfomgt.2020.102212

Chen, Y. C., Sng, F. & Kawaja, M. A. (2020). BYOD approach to blended learning in developing nations. In *International Conference on Electronic Business (ICEB)*, Singapore, 2020, pp. 240-250.

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, 12(6), 659–673. https://doi.org/10.1080/17517575.2017.1404132

Doargajudhur, M. S. & Dell, P. (2020). The effect of bring your own device (BYOD) adoption on work performance and motivation," *Journal of Computer Information Systems*, 60 (6), 518-529, 2020. https://doi.org/10.1080/08874417.2018.1543001

Fasae, J. K., Adekoya, C. O., & Adegbilero-Iwari, I. (2020). Academic libraries' response to the COVID-19 pandemic in Nigeria. *Library Hi Tech*. https://doi.org/10.1108/LHT-07-2020-0166

Hakami, M. (2020). Using Nearpod as a tool to promote active learning in higher education in a BYOD learning environment. *Journal of Education and Learning*, 9(1), 119-126. https://doi.org/10.5539/jel.v9n1p119

Livson, M., Ulanova, K. L., Pertsev, V. V., Dudynov, S. V., & Novikov, A. V. (2021). The influence of BYOD on results of students' learning. *Propósitos y representaciones*, 9 (2), 47-60. https://doi.org/10.20511/pyr2021.v9nSPE3.1265

Meates, J. (2020). Problematic digital technology use of children and adolescents: psychological impact. *Teachers and Curriculum*, 20 (1), 51-62. https://doi.org/10.15663/tandc.v20i1.349

Mohsin, M. K. A. & Ab Hamid, Z. (2022). Bring Your Own Device (BYOD): Legal protection of the employee in Malaysia," *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, 7 (7), 1-9. https://doi.org/10.47405/mjssh.v7i7.1609

Othman, N. A. A., Norman, A. A. & Kiah, M. L. M. (2021). Information system audit for mobile device security assessment, in *2021 3rd International Cyber Resilience Conference (CRC)*, 2021: IEEE, 1-6. https://doi.org/10.1109/CRC50527.2021.9392468

Rosman, M. R. M., Baharuddin, N. S., Alimin, N. A., Rosli, N. N. I. N., Shukry, A. I. M., & Razlan, N. M. (2022). Bring-Your-Own-Device (BYOD) and productivity: A conceptual framework, in *Proceedings*, 82 (1: MDPI), 1-10. https://doi.org/10.3390/proceedings2022082010

Safar, A. H. (2018). BYOD in higher education: A case study of Kuwait University. *Journal of Educators Online*, 15 (2), 1-13. https://doi.org/10.9743/jeo.2018.15.2.9

Saibakumo, W. T., Orewa, F., & Nwose, L. O. (2019). Environmental-friendly customer relation approaches to resolving low patronage in academic libraries: Perspective and preferences of student-users. *International Journal of Library Science*, 8(1), 7–17. http://article.sapub.org/10.5923.j.library.20190801.02.html

Shukry, A. I. M., Rosman, M. R. M., Rosli, N. N. I. N., Alias, N. R. & Razlan, N. M. (2023). Bring-Your-Own-Device" (BYOD) and productivity: Instrument development and validation**.** *International Journal of Interactive Mobile Technologies (iJIM)*, 17(11), 83-100

Sokolova, A. P., Gromova, L. Y. E., Tekucheva, I. V., Kocherevskaya, L. B. & Dmitrieva, E. G. (2021). The influence of BYOD concept on development of learning process in universities. *Propositos y representaciones*, 9 (2), 62-71, 2021. https://doi.org/ 10.20511/pyr2021.v9nSPE3.1271