Int. j. adv. multidisc. res. stud. 2024; 4(2):1102-1107

Received: 25-02-2024
Accepted: 05-04-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Junior High School Teachers' Awareness on Student Data Privacy Protection in the Conduct of Online Learning

Christian H Villegas
Polytechnic University of the Philippines, De La Salle University, Philippines

Corresponding Author: **Christian H Villegas**

Abstract
Students may become targets of cybercrime, such as fraud, cyberbullying, and theft because of the rapid increase in data collection in schools. Given the present situation, adequate data protection must be examined as the schools and the teachers may mismanage student data privacy. The study examined the level of awareness of Junior High School Teachers (JHS) on student data privacy protection in the conduct of online learning. The study examined the level of awareness of Junior High School Teachers (JHS) on student data privacy protection in the conduct of online learning. The study used the quantitative-descriptive method of research with a duly validated questionnaire as research instrument. Data were drawn from the 18 JHS Teachers of the Polytechnic University of the Philippines Laboratory High School (PUPLHS). JHS Teachers were "Extremely Aware" on data privacy protection in the conduct of online learning. There is no significant difference on the level of awareness of JHS Teachers when grouped according to profile variables such as age, years of teaching experience, educational attainment, and academic rank. The study highlighted the role of teachers in securing student data. Teachers need to be reminded of how security, privacy, and confidentiality relate to their job in the classroom. Being extremely aware of student data privacy protection would ensure safety of students, transparent, and smooth conduct of school affairs.

Keywords: Awareness, Data Privacy, Junior High School, Online Learning, Student Data Privacy Protection

1. Introduction

It is with no doubt that today's youth are growing up in a world where technology is widely available. Since the onset of the Covid-19 Pandemic, schools of today are maximizing the use of technology such as the internet, computer, and smartphones to effectively engage in the online teaching-learning process. While the fundamental goal of elementary and secondary schools is to educate all students for success in higher education, life, work, and citizenship, we also expect schools and educators to protect the safety and well-being of the students (Foundation for Excellence in Education, 2015) [10].

According to the National Association of Secondary School Principals (n.d.) [20], principals and teachers have been using technology-enhanced tools to collect data from the students. These data are then used to aid the school and teachers in creating personalized and student-centered learning experiences for the students. Student data is, in essence, any information about a student that school, colleges, universities, technology providers, and other stakeholders collect and retain. To operate virtually and physically, schools require the need for technology. But there's another need that administrators should also prioritize, the data privacy of students.

Cyberattacks and data breaches have the potential to expose and gather personal information. Students may become targets of cybercrime, such as fraud, cyberbullying, and theft when their personal data were not secured. Experts on Cyberattacks have detected a 600 percent increase in malicious emails since the coronavirus outbreak began (Miller, 2020) [18]. Human error such as the users' accidental actions or lack of action that originate, spread, or allow a security breach is the source of cyber-attacks (Ahola, 2020). This means that mishandling of data in schools may put the student's safety at risk.

The study sought to determine the awareness of JHS Teachers on student data privacy protection and answer whether there is a significant difference in the respondents' level of awareness when they are grouped according to their profile variables. Specifically, it aimed to answer the following questions: 1) What is the socio-demographic profile of the JHS Teachers in terms of Age, Years of teaching experience, Educational Attainment, and Academic Rank?; 2) What is the level of awareness of JHS Teachers on student data privacy protection in the conduct of online learning?; and 3) Is there a significant difference in

the respondents' level of awareness on student data privacy protection in the conduct of online learning when they are grouped according to profile?

1.1 Literature Review

Researchers have described privacy as a social construct that reflects people's daily beliefs and customs, yet people's perceptions of privacy and where they place it in their lives differ dramatically (Baruh *et al*., 2017; Boyd and Marwick, 2011; Nissenbaum, 2010) [3, 5, 21]. Students expose a great deal of personal and private information in class or online discussions, which may be dubious or even dangerous to our limits and ethical obligations, raising the topic of how much personal information students should share with the instructor (Booth, 2012) [4].

The study of Dunlap *et al*. (2021) [8] indicated that students had a high level of trust in their institutions to protect personal data, particularly when using well-known and branded university apps. Furthermore, the study showed that students may be apprehensive about third-party technologies and how they handle and maintain sensitive data. Learners become resistant to online learning platforms when they are uncomfortable of sharing knowledge on an online environment or social networking websites or when they do not understand the value of knowledge gained through sharing in such online platforms. By ensuring learners' privacy, a safe learning environment can be created (Anwar & Greer, 2012) [2]. Moreover, the study of Gogus and Saygin (2019) [12] suggests the importance of developing practices and techniques to overcome students' concerns about privacy risks that result from the collection and sharing of personal data.

Several countries have passed data protection legislation to safeguard their citizens. In the Philippines, the Data Privacy Act of 2012 (DPA) was enacted to protect the privacy of individuals, and it requires any personal information gathered be processed securely and confidentially. The enaction of DPA will help the schools and its teachers to ensure adequate protection in collecting and processing of student's data.

Based on the researcher's literature review, most studies were about data privacy expectations and concerns of students (Anwar & Greer, 2012; Dunlap, 2021; Gogus & Saygin, 2019) [2, 8, 12]. This study looks at this gap in the research by employing teachers as respondents and determine their awareness toward student data privacy. Given the present situation, adequate data protection must be examined as the schools and the teachers may mismanage student data privacy in the conduct of online learning and address concerns of parents, students, and other stakeholders concern about what information is being collected or shared, and what purpose might make of that data (Magid, 2017) [16].

1.2 Theoretical Framework

Communications Privacy Management (CPM) Theory (Mullen & Hamilton, 2016) [19] was used in the study. It is an evidence-based theory centered on comprehending the tension between sharing and preserving private information to govern one's personal information and design privacy rules to help impose this control.

When information is made public, common ownership of the shared data emerges. There are numerous ways to share information, and it is necessary to maintain data or personal privacy. At the same time, once data is shared with teachers, administrators, parents, or ministry of education workers, it is moved to a collective privacy boundary in school data systems. When a person shares information, status, or images on social media, their social media friends become co-owners of the information, and personal data can be disclosed on a worldwide scale. As a result, CPM theory looks into both personal self-disclosure and the management of establishing a community privacy boundary (Mullen & Hamilton, 2016) [19].

2. Methodology

2.1 Research Design

This study is quantitative descriptive method which defines the attributes of population being studied. By examining subjects as they are in reality, descriptive studies aim to provide a detailed description of people, occasions, or circumstances. Descriptive studies examine the traits of a population, pinpoint issues within a group, an organization, or a population, or investigate differences in traits or customs between institutions or even nations (Siedlecki, 2020) [23].

2.2 Respondents

Data were drawn from the 18 JHS Teachers of the Polytechnic University of the Philippines Laboratory High School (PUPLHS). Total population sampling, a type of purposive sampling was utilized in the study. Since the total population is of manageable size and has a well-defined characteristic, it is the most practical sampling technique to use.

2.3 Instruments and Validation

This study utilized a two-part researcher made survey questionnaire. The first part describes the demographic profile of the teachers, while the second part determines the teachers' level of awareness on student data privacy protection in the conduct of online learning. A series of revisions has been made to achieve the instrument's reliability and validity. The survey questionnaire was delivered to the respondents via Google Forms.

2.4 Ethical Considerations

Proper orientation was given to the respondents prior to the answering of the survey questionnaire. The researcher observed the proper research protocol in administering the survey questionnaire by acquiring ethics clearance to the office of the Research, Extension and Development. The answered survey questionnaire was kept and secured in the desktop file of the researcher. The confidentiality of the data will be maintained and will be used only for the purpose of this study.

2.5 Statistical Treatment

Descriptive statistics such as the mean and frequency counts were used to analyze data. Standard deviation was calculated to measure the dispersion of a dataset relative to its mean. Analysis of Variance was utilized to determine whether there are any statistically significant differences between the means of three or more independent groups.

3. Results

Table 1 shows the demographic profile of the junior high school teachers. 55.56% of the respondents aged between twenty-one and thirty, while 5.56% of them aged sixty and above. 72.22% of the JHS Teachers have taught from one to

ten years, 11.11% have taught from eleven to twenty years and twenty-one to thirty years, and 5.56% have taught for thirty-one to forty years. 11.11% of the respondents have earned units in master's degree program, while 22.22% of the respondents have units or currently enrolled in doctorate degree program. 72.22% of the respondents are ranked as instructors, 16.67 as assistant professors, and 11.11% as associate professors.

Table 1: Demographic Profile of the JHS Teachers

Age	Frequency	Percentage
21 – 30	10	55.56
31 – 40	1	5.56
41 – 50	4	22.22
51 – 60	2	11.11
Above 60	1	5.56
Total	18	100
Teaching Experience (in years)		
1 - 10	13	72.22
11 – 20	2	11.11
21 – 30	2	11.11
31 – 40	1	5.56
More than 40 years	0	0
Total	18	100
Educational Attainment		
Bachelor's Degree Holder	5	27.78
With Units/Currently Enrolled in a Master's Degree Program	7	38.89
Master's Degree Holder	2	11.11
With Units/Currently Enrolled in a Doctorate Degree Program	4	22.22
Doctorate Degree Holder	0	0
Total	18	100
Academic Rank		
Instructor	13	72.22
Assistant Professor	3	16.67
Associate Professor	2	11.11
Professor	0	0
University Professor	0	0
Total	18	100

Table 2 shows the level of awareness of JHS Teachers on data privacy protection in the conduct of online learning. Overall, the teachers are extremely aware of data privacy protection with means scores ranging from 4.56 to 4.83. It is also noticed that lower variability in the scores were assigned by the respondents (SD = 0.52).

Table 2: JHS Teachers Awareness on Student Data Privacy Protection in the Conduct of Online Learning

Statements	Mean	SD	Interpretation
1. When the educational institution adopts a particular Learning Management System (LMS), all activities related to online learning should be carried out on this platform to the maximum possible extent.	4.78	0.42	Extremely Aware
2. An announcement or posting containing personal data (e.g., grades, results of assignments, etc.) should be done in a way that only the intended recipient(s) may see it.	4.78	0.42	Extremely Aware
3. Personal data saved in the LMS should be downloaded as little as possible and/or limited to that which is necessary for online learning.	4.72	0.56	Extremely Aware
4. Any downloaded data should only be kept until it is necessary to have an offline copy.	4.72	0.56	Extremely Aware
5. Social media submissions are discouraged because these sites were never intended for this purpose.	4.67	0.58	Extremely Aware
6. Integrating programs, tools, and other services into an LMS should be done with caution because it may bring vulnerabilities to an otherwise secure system.	4.83	0.50	Extremely Aware
7. All personal data uploaded on social media is considered public by nature unless suitable privacy measures and settings made accessible by the platform are correctly used.	4.78	0.53	Extremely Aware
8. Posting or sharing of personal data on social media must always have a legitimate purpose. The type of personal data involved, as well as the purpose, determines whether the data subjects' consent is required prior to such posting or sharing.	4.72	0.48	Extremely Aware
9. Even if it is determined that posting of personal data is allowed, it must be carried out using the educational institutions authorized or official social media accounts.	4.72	0.56	Extremely Aware
10. When personal data is shared on social media as part of a course requirement, the data's lifespan usually matches that of the course. Once the course is over, the data's lifespan is also over. Unless there is any legal reason to keep it online, it must be removed or erased.	4.56	0.60	Extremely Aware
11. Personal data gathered by educational institution personnel in the course of their official duties and/or during official activities shall not be utilized for personal purposes or reasons.	4.94	0.23	Extremely Aware
12. To provide proper data protection measures, all personal data acquired during the conduct of an online course should be maintained in the educational institution's LMS.	4.72	0.56	Extremely Aware
13. Storing of personal data obtained over the course of class in a personal account or device should be avoided or at	4.67	0.58	Extremely

least kept to a minimum to reduce the risk of unauthorized use or access.			Aware
14. Unless there is some lawful basis for their continued retention, personal data obtained should be securely disposed of when the declared purpose for its collection and processing is no longer valid.	4.83	0.37	Extremely Aware
15. Webcams should be optional in synchronous online classes or sessions whenever possible.	4.61	0.60	Extremely Aware
16. The principles of Legitimate Purpose and Proportionality should be the primary consideration when recording these online classes or discussions. (e.g., review the lecture presentations and viewing by students who are unable to attend).	4.67	0.58	Extremely Aware
17. Where consent is necessary for the recording of these classes or sessions (as determined by attendant circumstances) and the data subject is a minor, consent must be sought from the child's parent, legal guardian, or any other person with valid parental responsibility over the child.	4.56	0.77	Extremely Aware
18. In case of posting the recorded classes or sessions or making them available on public platforms (e.g., social media, school website, etc.), Individuals present in the recording must have been informed of the school's plan to make the recording public before the recording was posted or made available on public platforms. Depending on the nature of the recording, prior approval of said individuals may also be necessary.	4.83	0.50	Extremely Aware
19. The use of webcams and the recording of online classes or sessions should be governed by a policy or guidelines established by educational institutions. Such policy should consider not only its legitimate interests, but also individual privacy rights. It should also address the possible recording and use of such classes or sessions by the participants themselves.	4.78	0.53	Extremely Aware
Overall Mean	4.73	0.52	Extremely Aware

1.00-1.79 – Not at all Aware; 1.80-2.59 – Slightly Aware; 2.60-3.39 – Somewhat Aware; 3.40-4.19 – Moderately Aware; 4.20-5.00 – Extremely Aware.

Table 3 shows that when the respondents were grouped according to age, their level of awareness on data privacy protection in the conduct of online learning were all similar.

Table 3: Significant Difference between JHS Teachers Level of Awareness on Data Privacy Protection in the Conduct of Online Learning When Grouped According to Age

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.200	4	0.050	0.547	0.704	3.179
Within Groups	1.185	13	0.091			
Total	1.384	17				

Correlation at the level of 0.05

Table 4 reveals that when the respondents were grouped according to years of teaching experience, their level of awareness on data privacy protection in the conduct of online learning did not differ.

Table 4: Significant Difference between JHS Teachers Level of Awareness on Data Privacy Protection in the Conduct of Online Learning When Grouped According to Years of Teaching Experience

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.039	4	0.010	0.095	0.982	3.179
Within Groups	1.345	13	0.103			
Total	1.384	17				

Correlation at the level of 0.05

Table 5 indicates that when the respondents were grouped according to educational attainment, their level of awareness on data privacy protection in the conduct of online learning were all the same

Table 5: Significant Difference between JHS Teachers Level of Awareness on Data Privacy Protection in the Conduct of Online Learning When Grouped According to Educational Attainment

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.037	4	0.009	0.088	0.985	3.179
Within Groups	1.348	13	0.104			
Total	1.384	17				

Correlation at the level of 0.05

Table 6 shows that when the respondents were grouped according to academic, their level of awareness on data privacy protection in the conduct of online learning were all similar.

Table 6: Significant Difference between JHS Teachers Level of Awareness on Data Privacy Protection in the Conduct of Online Learning When Grouped According to Academic Rank

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.049	4	0.012	0.120	0.973	3.179
Within Groups	1.335	13	0.103			
Total	1.384	17				

Correlation at the level of 0.05

This section summarizes the study's results and findings after carefully examining the information acquired utilizing the research instrument.

4. Discussion

According to research, instructors are not sufficiently equipped to handle the difficulties associated with privacy concerns, cyberbullying, and the evaluation of digital information (Macaulay *et al*., 2018; Shin, 2015) [17, 22]. Digital competence addressing the appropriate use of ICT and the Internet cannot be neglected in an era of harassment, cyberbullying, fake news, and vast online data exposure. Online data is simple to access and simple to change. As a result, there needs to be more knowledge of the ways in which educators and students can control and assess digital information. In addition, parents seek advice from the schools.

Furthermore, Jones *et al*. (2020) [15] reported that students trust schools and universities more than the for-profit companies in securing their personal data. Furthermore, EDUCAUSE Center for Analysis and Research (2019) [9] survey of US students found that 70 percent expressed confidence in their institution's ability to safeguard their personal data. Moreover, a three-part study of Galanek and Shulman (2019) [11] on UK students' expectations of learning analytics concluded that Students are certain that their colleges and universities should protect their academic

records, and they want assurances that their information is secure and private. This put a lot of weight on the educational institutions and teachers' job to secure students' data. Teachers have access to a lot of sensitive student information, and they play a crucial part in students' protection by keeping that information secure.

While some research revealed that teachers are not competent in handling privacy issues (Gudmundsdottir *et al*., 2020) [14], the study's finding indicates that overall, the JHS Teachers are extremely aware of data privacy protection in the conduct of online learning. Professional digital competence (PDC) is crucial for teachers because, first, they require this knowledge and expertise for their studies (Gudmundsdottir & Hatlevik, 2018) [13], and second, as future educators, they must assist their students' growth in this area (Choi *et al*., 2018; Vuorikari *et al*., 2016) [6, 24]. Both teachers and student teachers need to be digitally competent in order to use ICT in their learning and teaching processes. They also need to be digitally competent in order to sustain and participate in democracies. Democratic processes can be endangered by false information, fake news, harassment, threats, and the careless use of personal data.

The JHS Teachers level of awareness on student data privacy protection in the conduct of online learning were all similar when they are grouped according to age, years of teaching, educational attainment, and academic rank. This appears to be the case since the responsibility of teachers in handling student data is always expected from them. Every teacher is responsible for maintaining the privacy of every student's data and only disclosing it when necessary, such as to parents, other teachers, and administrators (Scheid, 2019). Teachers should think about how their duties fit into the larger picture of protecting student data privacy in the classroom once they have a basic understanding of privacy, security, and confidentiality.

5. Conclusion

This study assessed the level of awareness of JHS teachers on student data privacy protection in the conduct of online learning. The study revealed that JHS teachers were extremely aware of data privacy measures and perhaps they are already adapting it on their online teaching. The respondent's level of awareness when grouped according to profile variables did not register significant difference. The findings of the study generally imply that age, years of teaching, educational attainment, and academic rank has nothing to do on the respondent's awareness of data privacy measures in the conduct of online learning.

7. Recommendation

Since JHS teachers were found to be extremely aware of data privacy measures, they are all recommended to exercise it on their conduct of online learning. The University should also continue to provide in-service training for the teachers about handling student data privacy in a Learning Management Systems, social media, storage of data, and on the use of webcams and recorded video discussions. Likewise, the administrators and the teachers are advised to read and fully understand the implementing rules and regulations in the Data Privacy Act of 2012 to protect themselves on facing possible legal problems. The study was done on a limited scope involving only JHS Teachers at the Polytechnic University of the Philippines, in which the results may differ to other regions of the country or differ from different countries. Future studies might also explore into issues related to the entire school environment, which includes administrators and the student body.

8. Declarations

Conflicts of Interest: The author declares no conflict of interest.

9. References

1. Ahola M. The Role of Human Error in Successful Cyber Security Breaches, n.d. Retrieved May 12, 2022, from: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches
2. Anwar M, Greer J. Facilitating trust in privacy-preserving E-learning environments. IEEE Transactions on Learning Technologies. 2012; 5(1):62-73. Doi: https://doi.org/10.1109/TLT.2011.23
3. Baruh, *et al*. Online privacy concerns and privacy management: A meta-analytical review. J. Commun. 2017; 67:26-53.
4. Booth M. Boundaries and student self-disclosure in authentic, integrated learning activities and assignments. New Directions for Teaching and Learning. 2012; 2012(131):5-14. Doi: https://doi.org/10.1002/tl.20023
5. Boyd, Marwick. Social privacy in networked publics: teens' attitudes, practices, and strategies. Paper Presented at the Oxford Internet Institute's. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, 2011.
6. Choi M, Cristol D, Gimbert B. Teachers as digital citizens: The influence of individual backgrounds, internet use and psychological characteristics on teachers' levels of digital citizenship. Computers and Education. 2018; 121:143-161.
7. Data Privacy Council Education Sector Advisory No. 2020-1. Data Privacy and Online Learning. Retrieved May 12, 2022 from: https://www.privacy.gov.ph/wp-content/uploads/2020/10/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf
8. Dunlap, *et al*. Keeping Student Trust: Student Perceptions of Data Use within Higher Education, 2021. Retrieved June 16, 2022 from: https://www.newamerica.org/education-policy/reports/keeping-student-trust/
9. EDUCAUSE. Study of Undergraduate Students and Information Technology, 2019. Retrieved June 16, 2022 from: https://library.educause.edu/resources/2019/10/2019-study-of-undergraduate-students-and-information-technology
10. Foundation for Excellence in Education. Protecting K-12 Student Privacy in a Digital Age, 2015.
11. Galanek, Shulman. Not Sure If They're Invading My Privacy or Just Really Interested in Me. EDUCAUSE Review, 2019.
12. Gogus, Saygin. Privacy perception and information technology utilization of high school students, 2019.
13. Gudmundsdottir GB, Hatlevik OE. Newly qualified teachers' professional digital competence: Implications for teacher education. European Journal of Teacher Education. 2018; 41(2):214-231.
14. Gudmundsdottir GB, Gassó HH, Rubio JCC, Hatlevik

OE. Student teachers' responsible use of ICT: Examining two samples in Spain and Norway. Computers & Education. 2020; 152:103877.
15. Jones, *et al*. We're Being Tracked at All Times, 2020. Retrieved June 16, 2022 from: https://asistdl.onlinelibrary.wiley.com/doi/10.1002/asi.24358
16. Magid. The Educator's Guide to Student Data Privacy, 2017. Retrieved June 16, 2022 from: https://www.connectsafely.org/eduprivacy/
17. Macaulay PJ, Betts LR, Stiller J, Kellezi B. Perceptions and responses towards cyberbullying: A systematic review of teachers in the education system. Aggression and Violent Behavior. 2018; 43:1-12.
18. Miller M. Experts see over 600 percent spike in malicious emails during coronavirus crisis, 2020. Retrieved May 12, 2022, from: https://thehill.com/policy/cybersecurity/489692-experts-seeover-600-percent-spike-in-malicious-emails-during
19. Mullen C, Hamilton NF. Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence. Computers in Human Behavior. 2016; 60:165-172.
20. National Association of Secondary School Principals, n.d. Retrieved May 12, 2022 from: https://www.nassp.org/top-issues-in-education/position-statements/student-data-privacy/.
21. Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life Stanford University Press, Palo Alto, CA, 2010.
22. Shin SK. Teaching critical, ethical, and safe use of ICT to teachers. Language, Learning and Technology. 2015; 19(1):181-197.
23. Siedlecki SL. Understanding descriptive research designs and methods. Clinical Nurse Specialist. 2020; 34(1):8-12.
24. Vuorikari R, Punie Y, Carretero S, Van den Brande G. DigComp 2.0: The digital competence framework for citizens. Update phase 1: The conceptual reference model. Luxemburg: Luxembourg Publication Office of the European Union, 2016.
25. Zamora, *et al*. An Analysis on the Perceptions of High School Teachers in Manila, Philippines towards Student Data Privacy and Its Legal Implications, 2018.